

|  |  |
| --- | --- |
|  | **Direction des Constructions et Patrimoine**  **Directeur : Abdelaali Gaïdi**  Secrétariat :  🕿 05 61 77 84 45  Fax : 05 61 77 84 01 |

**HÔPITAUX DE TOULOUSE**

\_\_\_\_\_\_

**X2130-**

**Fourniture et prestations de services pour le contrôle d’accès**

**C.C.T.P.**

**Fourniture et prestations de services pour le contrôle d’accès pour le CHU de Toulouse.**

**Maître d'ouvrage**

Centre Hospitalier Universitaire de Toulouse

2, rue Viguerie

TSA 80035

31059 Toulouse

|  |  |  |  |
| --- | --- | --- | --- |
| Indice | Date : | Rédacteurs : | Relecteur : |
| 0 | 29/10/2024 | Y. MOUSSACEB | F. MEZAILLES |
| 06/02/2025 | C.DARDE/ M.YOUSFI |  |
| *Première Version* | | |
| A | 30/06/2025 | Y. MOUSSACEB | Y. MOUSSACEB |
|  | | |
| B |  |  |  |
|  | | |
| C |  |  |  |
|  | | |
| D |  |  |  |
|  | | |

**SOMMAIRE**

[CHAPITRE 1. Objet du marché 5](#_Toc197939622)

[CHAPITRE 2. Généralites 6](#_Toc197939623)

[2.1 Parc existant des equipements de contrôle d’accès 6](#_Toc197939624)

[2.2 Documents à joindre à la consultation 6](#_Toc197939625)

[2.2.1 Documents à présenter 6](#_Toc197939626)

[2.2.1.1 Documents à présenter au moment de la remise des offres 6](#_Toc197939627)

[CHAPITRE 3. PRESCRIPTIONS TECHNIQUES GENERALES 8](#_Toc197939628)

[3.1 Généralités 8](#_Toc197939629)

[3.2 Badges 9](#_Toc197939630)

[3.3 Obligations diverses 10](#_Toc197939631)

[3.3.1 Garanties 10](#_Toc197939632)

[3.3.2 Processus de retour des équipements défectueux 10](#_Toc197939633)

[3.3.3 Réglementations et normes 11](#_Toc197939634)

[CHAPITRE 4. PRESCRIPTIONS TECHNIQUES PARTICULIERES 12](#_Toc197939635)

[4.1 Généralités 12](#_Toc197939636)

[4.2 Solution logicielle 13](#_Toc197939637)

[4.2.1 Généralités 13](#_Toc197939638)

[4.2.2 Logiciel d’exploitation et gestion des droits 13](#_Toc197939639)

[4.2.3 Logiciel de chiffrement des cartes 16](#_Toc197939640)

[4.2.3.1 Gestion de clés de chiffrements 17](#_Toc197939641)

[4.2.4 Logiciel de supervision des équipements de contrôle d’accès 17](#_Toc197939642)

[4.3 Equipements de contrôle d’accès 19](#_Toc197939643)

[4.3.1 Généralités 19](#_Toc197939644)

[4.3.2 Lecteur d’enrôlement et d’encodage des badges 19](#_Toc197939645)

[4.3.2.1 Lecteurs d’enrôlement et d’encodage des badges (cartes des professionnels de santé CPSX/CPE) 19](#_Toc197939646)

[4.3.2.1 Lecteurs d’enrôlement et d’encodage des badges et des étiquettes UHF 20](#_Toc197939647)

[4.3.3 Unité de Traitement Local (UTL) et Unité de de Traitement de Porte (UTP) 21](#_Toc197939648)

[4.3.3.1 Caractéristiques techniques minimales UTL : 21](#_Toc197939649)

[4.3.3.2 Caractéristiques techniques minimales UTP : 22](#_Toc197939650)

[4.3.3.3 Caractéristiques techniques minimales UTL et UTP précablées : 22](#_Toc197939651)

[4.3.4 Autres cartes et équipements d’interfaçage et de gestion 23](#_Toc197939652)

[4.3.4.1 Carte de gestion des lecteurs UHF existants 23](#_Toc197939653)

[4.3.4.2 Carte de gestion de SAS d’accès 23](#_Toc197939654)

[4.3.4.3 Carte de gestion des ascenseurs 23](#_Toc197939655)

[4.3.4.4 Coffrets et autres accessoires des UTL et autres cartes électroniques : 23](#_Toc197939656)

[4.3.5 Lecteurs de badges 24](#_Toc197939657)

[4.3.5.1 Lecteurs de badges sans contact transparent (format large) 24](#_Toc197939658)

[4.3.5.1 Lecteurs de badges sans contact transparent (format étroit) 24](#_Toc197939659)

[4.3.5.2 Lecteurs de badges doubles technologie sans contact avec digicode intégré de type transparent 25](#_Toc197939660)

[4.3.5.1 Lecteur de badge doubles technologie sans contact avec clavier tactile de type transparent 25](#_Toc197939661)

[4.3.5.2 Lecteur de badge doubles technologie sans contact avec lecteur QR code de type transparent 26](#_Toc197939662)

[4.3.5.3 Lecteur de badge doubles technologie sans contact avec lecteur biométrique de type transparent 26](#_Toc197939663)

[4.3.5.1 Lecteur de badge doubles technologie sans contact avec lecteur biométrique et afficheur, de type transparent : 27](#_Toc197939664)

[4.3.5.2 Lecteurs de badges sans contact transparent-Bluetooth (format large) 28](#_Toc197939665)

[4.3.5.3 Lecteurs de badges sans contact transparent-Bluetooth (format étroit) 29](#_Toc197939666)

[4.3.5.4 Lecteurs de badges doubles technologie sans contact avec digicode intégré de type transparent- Bluetooth 29](#_Toc197939667)

[4.3.5.5 Lecteur de badge doubles technologie sans contact avec clavier tactile de type transparent-Bluetooth 30](#_Toc197939668)

[4.3.5.6 Lecteur de badge doubles technologie sans contact avec lecteur QR code de type transparent-Bluetooth 30](#_Toc197939669)

[4.3.5.7 Accessoires des lecteurs de badges 31](#_Toc197939670)

[4.3.6 Lecteurs de badges UHF longue distance 31](#_Toc197939671)

[4.3.6.1 Lecteur de badge longue distance UHF 868 MHz (lecteur spectre 7AB-RS485) 31](#_Toc197939672)

[4.3.6.2 Lecteur de badge longue distance UHF 868 MHz (lecteur spectre Nano 7AB-RS485) 31](#_Toc197939673)

[4.3.6.3 Lecteur de badge longue distance UHF 868 MHz (lecteur spectre en Clock&Data -Configurable en Wiegand) 32](#_Toc197939674)

[4.3.6.4 Lecteur de badge longue distance UHF 868 MHz (lecteur spectre Nano en Clock&Data -Configurable en Wiegand) 32](#_Toc197939675)

[4.3.6.1 Accessoires des lecteurs de badges 32](#_Toc197939676)

[4.3.7 Lecteurs de plaques d’immatriculation 33](#_Toc197939677)

[4.3.7.1 Lecteur de plaques d’immatriculation (2m à 6m): 33](#_Toc197939678)

[4.3.7.2 Lecteur de plaques d’immatriculation (4m à 15m): 33](#_Toc197939679)

[4.3.7.3 Accessoires des lecteurs de plaques d’immatriculation 33](#_Toc197939680)

[4.3.8 Lecteurs de badges sans fils et serrures autonomes 34](#_Toc197939681)

[4.3.8.1 Ensemble de plaques béquilles électroniques 34](#_Toc197939682)

[4.3.8.2 Cylindres électroniques 35](#_Toc197939683)

[4.3.8.1 Accessoires et autres équipements 35](#_Toc197939684)

[4.3.9 Serrures et clés mécatroniques : 36](#_Toc197939685)

[4.3.9.1 Cylindres programmables 36](#_Toc197939686)

[4.3.9.1 Clés programmables 37](#_Toc197939687)

[4.3.9.2 Boitier de programmation et de transmission des droits d’accès 38](#_Toc197939688)

[4.3.9.3 Accessoires et autres équipements 38](#_Toc197939689)

[4.3.10 Badges UHF 39](#_Toc197939690)

[4.3.10.1 Teletag-TAG parebrise athermique UHF 39](#_Toc197939691)

[4.3.10.1 Etiquette adhésive UHF pour véhicule (ETA) 39](#_Toc197939692)

[4.3.10.2 Etiquette adhésive UHF pour véhicule (ETA V2) 39](#_Toc197939693)

[4.3.10.3 Badge Passif UHF ISO 40](#_Toc197939694)

[4.3.10.4 Badge Passif UHF avec technologie Mifare 40](#_Toc197939695)

[4.3.10.5 Badge UHF avec technologie DESFire EV2 40](#_Toc197939696)

[4.3.11 Badges dématérialisés sur smartphones 40](#_Toc197939697)

[4.3.12 Equipements de personnalisation des badges 40](#_Toc197939698)

[4.3.12.1 Imprimante simple face - Chargeur 50 cartes – USB : 40](#_Toc197939699)

[4.3.12.1 Rubans pour imprimante : 41](#_Toc197939700)

[4.3.13 Fourniture de matériel non listé au BPU 41](#_Toc197939701)

[4.4 Prestations d’intégration du système de contrôle d’accès 42](#_Toc197939702)

[4.4.1 Paramétrages et intégrations des solutions « logiciels/applicatifs » 42](#_Toc197939703)

[4.4.2 Préparations de préparations, études et de migrations 43](#_Toc197939704)

[4.4.2.1 Migrations entre les anciennes et la nouvelle solution de contrôle d’accès 43](#_Toc197939705)

[4.4.2.2 Migrations entre les anciennes et les nouvelles cartes de professionnels de santé (badges) 43](#_Toc197939706)

[4.4.3 Prestation d’interfaçage automatique avec la base de données AGIRH 44](#_Toc197939707)

[4.4.4 Paramétrages et intégrations des équipements de contrôle d’accès 45](#_Toc197939708)

[4.4.5 Préparations de paramétrages et programmations des badges UHF 46](#_Toc197939709)

[4.4.6 Préparations de chiffrement d’encodage et d’enrôlement des badges 46](#_Toc197939710)

[4.4.7 Préparations de paramétrages et programmations des clés mécatroniques 46](#_Toc197939711)

[4.4.8 Préparations de paramétrages et programmations badges dématérialisés sur smartphones (contrôle d’accès par smartphone) 46](#_Toc197939712)

[4.5 Prestations de formation du personnel 47](#_Toc197939713)

[4.6 Prestations de Maintenance et prestations diverses 48](#_Toc197939714)

[4.7 Continuité de service et retrocompatibilité 51](#_Toc197939715)

[4.8 Obligation de conseil 51](#_Toc197939716)

[CHAPITRE 5. PRESCRIPTIONS spécifiques informatiques/DSN 52](#_Toc197939717)

[5.1 Description du fonctionnement futur envisagé 52](#_Toc197939718)

[5.1.1 Contexte 52](#_Toc197939719)

[5.1.2 Les enjeux du Système d’Information Hospitalier 52](#_Toc197939720)

[5.1.3 Enjeux liés à la sécurité des systèmes d’information 52](#_Toc197939721)

[5.2 Besoins fonctionnels détaillés 52](#_Toc197939722)

[5.2.1 Paramétrage 52](#_Toc197939723)

[5.2.1.1 Structure de l'établissement 52](#_Toc197939724)

[5.2.1.2 Habilitations au logiciel 52](#_Toc197939725)

[5.2.1.3 Gestion des habilitations 53](#_Toc197939726)

[5.2.1.4 Gestion des droits d’accès au site 54](#_Toc197939727)

[5.2.1.5 Planification des droits d’accès 54](#_Toc197939728)

[5.2.1.6 Reporting 54](#_Toc197939729)

[5.2.1.7 Historique 54](#_Toc197939730)

[5.2.2 Procédures critiques : modes dégradés, plan de continuité de l’activité et plan de reprise de l’activité 54](#_Toc197939731)

[5.2.3 Reprise des données 55](#_Toc197939732)

[5.3 Interfaces 55](#_Toc197939733)

[5.3.1 Flux structure 55](#_Toc197939734)

[5.3.2 Flux avec le système gestion administrative RH 55](#_Toc197939735)

[5.4 Description du contexte technique 56](#_Toc197939736)

[5.4.1 Attentes et contraintes techniques 56](#_Toc197939737)

[5.4.1.1 Hébergement 56](#_Toc197939738)

[5.4.1.2 Accessibilité 56](#_Toc197939739)

[5.4.1.3 Ergonomie 56](#_Toc197939740)

[5.4.1.4 Disponibilité 56](#_Toc197939741)

[5.4.1.5 Sécurité des données 56](#_Toc197939742)

[5.4.1.6 Cloisonnement des données 56](#_Toc197939743)

[5.4.1.7 Bases de données 56](#_Toc197939744)

[5.4.1.8 Performances 56](#_Toc197939745)

[5.4.1.9 Supervision 56](#_Toc197939746)

[5.4.2 Attentes applicatives 57](#_Toc197939747)

[5.5 Organisation du pilotage INFORMATIQUE 57](#_Toc197939748)

[5.5.1 Les acteurs du pilotage 57](#_Toc197939749)

[5.5.1.1 Equipe du titulaire 57](#_Toc197939750)

[5.5.1.2 D.S.N. (Direction des Services Numériques) 57](#_Toc197939751)

[5.5.1.3 Direction des achats 57](#_Toc197939752)

[5.5.1.4 La maîtrise d’ouvrage 57](#_Toc197939753)

[5.5.2 Le pilotage du contrat 57](#_Toc197939754)

[5.5.2.1 Le comité de pilotage 58](#_Toc197939755)

[5.5.2.2 Le comité de suivi SI (mensuel) 58](#_Toc197939756)

[5.5.3 Méthodologie projet 58](#_Toc197939757)

[5.5.3.1 Phase Etude d’opportunité 59](#_Toc197939758)

[5.5.3.2 Phases d’étude. 59](#_Toc197939759)

[5.5.3.3 Phase de réalisation. 59](#_Toc197939760)

[5.5.3.4 Phase de déploiement. 59](#_Toc197939761)

[5.5.4 Vérifications 59](#_Toc197939762)

[5.6 Organisation du support et attentes 60](#_Toc197939763)

[5.6.1 Plan d’assurance qualité 60](#_Toc197939764)

[5.6.2 Maintenance et services d’assistance 60](#_Toc197939765)

[5.6.2.1 Exercice du support 61](#_Toc197939766)

[5.6.2.2 Définitions des différents niveaux de dysfonctionnement 62](#_Toc197939767)

[5.6.2.3 Evolution du système de la solution logicielle 63](#_Toc197939768)

[5.6.2.3.1. Etats techniques 63](#_Toc197939802)

[5.6.2.3.2. Mise à niveau 63](#_Toc197939803)

[5.6.2.3.3. Nouvelles versions 63](#_Toc197939804)

[5.6.2.4 Exclusion de la maintenance 64](#_Toc197939805)

[5.6.2.5 Suivi pour évolution du système d'exploitation 65](#_Toc197939806)

[5.6.2.6 Collaboration/ obligations des parties 65](#_Toc197939807)

[5.6.3 Documentation 65](#_Toc197939808)

[5.6.4 Formation 65](#_Toc197939809)

[5.7 Conditions de droit d’usage du logiciel 65](#_Toc197939810)

[5.7.1 Plateforme de test 65](#_Toc197939811)

[5.7.2 Evolution des équipements 66](#_Toc197939812)

[5.7.3 Utilisation des produits du titulaire sur des centres provisoires 66](#_Toc197939813)

[5.8 ANNEXES AU CCTP 66](#_Toc197939814)

# Objet du marché

Le présent descriptif a pour objet de décrire l’ensemble des prestations de fourniture d’une solution globale d’un système de contrôle d’accès pour les hôpitaux de Toulouse. Cette solution de contrôle d’accès sera obligatoirement certifiée et qualifiée ANSSI et reprendra aux dernières exigences ANSSI-CSPN en vigueur.

Les prestations du présent marché sont les suivantes :

* Fourniture de la solution « logiciels » de gestion et d’exploitation des équipements de contrôle d’accès,
* Fourniture d’une solution de supervision technique des équipements de contrôle d’accès,
* Fourniture des équipements centraux et terminaux de contrôle d’accès,
* Prestations d’intégrations des logiciels et des équipements de contrôle d’accès,
* Prestations des préparatifs et des reprises des bases de données existantes au sein des autres systèmes de contrôle d’accès existants, permettant l’intégration des équipements de contrôle d’accès au sein de la nouvelle solution,
* Les prestations des migrations des installations et des équipements de contrôle d’accès,
* Les prestations des migrations les anciennes cartes et futures cartes CPSx et CPEx,
* Prestations de maintenance des équipements et des logiciels de contrôle d’accès,
* Formations des personnels,
* Autres prestations d’accompagnement,
* …

Le présent marché comporte un lot unique.

**Les matériels proposés doivent en tous points être conformes aux prescriptions du présent Cahier des Clauses Techniques Particulières (CCTP), au CCAP et du Bordereau des Prix Unitaires (BPU) sous peine de rejet de l'offre.**

# Généralites

## Parc existant des equipements de contrôle d’accès

Dans le tableau ci-dessous, sont détaillés : les marques et les estimatifs des quantités des équipements de contrôle d’accès actuellement existants sur les différents sites du CHU de Toulouse :

|  |  |  |
| --- | --- | --- |
| **Marque des équipements de contrôle d’accès** | **Sites du CHU de Toulouse** | **Nombre d’UTL (estimatif)** |
| **ERO** | Hôtel Dieu | **355** |
| Chapitre |
| Purpan |
| Logipharma |
| Rangueil |
| Larrey |
| Salies |
| **NCS** | Purpan | **324** |
| **NOVADIS** | Purpan | **346** |
| Rangueil |
| Larrey |
| La Grave |
| Salies |
| Chapitre |
| **SYNCHRONIC** | IUCT-O | **165** |
| **Total** | | **1190** |

|  |  |
| --- | --- |
| **Sites CHU de Toulouse** | **Nombre de lecteurs de badges (estimatif)** |
| **PURPAN** | 1388 |
| **RANGUEIL** | 405 |
| **LARREY** | 8 |
| **CHAPITRE** | 12 |
| **SALIES DU SALAT** | 3 |
| **LA GRAVE** | 14 |
| **HOTEL DIEU** | 6 |
| **LOGIPHARMA** | 6 |
| **IUCT-O** | 350 |
| **Total** | **2192** |

Les quantités estimatives listées dans les tableaux ci-dessus sont données à titre indicatif permettant d’avoir une vision globale du parc existant des équipements de contrôle d’accès, au sein des différents sites du CHU de Toulouse et n’ont aucune valeur contractuelle.

La solution proposée dans le cadre du présent projet permettra à long terme, le remplacement des équipements de contrôle d’accès actuellement existants sur les différents sites du CHU de Toulouse et par conséquent l’uniformisation des installations de contrôle d’accès.

## Documents à joindre à la consultation

### Documents à présenter

#### Documents à présenter au moment de la remise des offres

Les documents à remettre sont listés dans le règlement de la consultation à son article 11.2.

# PRESCRIPTIONS TECHNIQUES GENERALES

## Généralités

Le présent marché prévoit la fourniture d’une solution globale (équipements et applicatifs/logiciels) de contrôle d’accès disposant **nécessairement d**’**une certification et d’une qualification ANSSI-CSPN sur l’ensemble de la chaîne (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB ») et ce conformément aux dernières exigences en vigueur ANSSI-CSPN.**

**Le titulaire doit justifier des** **qualifications et des certifications** **de l’ensemble de la chaîne de la solution de contrôle d’accès (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB ») et conformément aux sur dernières exigences en vigueur ANSSI-CSPN en transmettant cette documentation (qualifications et certifications) ou à minima :**

* **Une certification et une qualification ANSSI-CSPN en cours de validité.**
* **Ainsi que les documents justificatifs des procédures de certifications et de qualifications en cours sur l’ensemble de la chaîne de la solution de contrôle d’accès (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB ») proposée dans le cadre du présent marché et ce conformément aux dernières exigences en vigueur ANSSI-CSPN,**

Le système à mettre en place devra répondre aux spécifications détaillées, ci-dessous :

* Le système de contrôle d’accès sera de technologie IP avec un contrôleur (UTL) permettant le fonctionnement natif en POE
* Le contrôleur (UTL) permettra la gestion des équipements de contrôle d’accès (LB, BG, BP, équipements de verrouillage…)  et la communication avec les logiciels de gestion, d’exploitation, de supervision technique via un seul serveur virtualisé, cloisonné et redondé
* Le système disposera de son propre logiciel de gestion des droits d’accès et d’exploitation, ce dernier sera de type ouvert et permettra de fonctionner en temps réel avec les équipements de contrôle d’accès et les logiciels de type web service
* Le système permettra également la supervision technique des installations de contrôle d’accès et l’interfaçage avec d’autres logiciels de supervision technique et autres logiciels de type services WEB
* La solution technique proposée devra pouvoir offrir un large spectre des dispositifs de contrôle d’accès et notamment :
  + Par lecteur de badge sans contact de technologie RFID de type transparent,
  + Par lecteur de badge sans contact de technologie RFID de type transparent-Bluetooth,
  + Par lecteur de badge sans contact de technologie RFID avec digicode intégré,
  + Par lecteur d’empreintes biométriques,
  + Par des serrures autonomes et lecteurs sans fils électroniques,
  + Par serrures électriques,
  + Par gâches électriques,
  + Par des clés mécatroniques et ses serrures électroniques,
  + Par des lecteurs de plaques minéralogiques,
  + Par des lecteurs de type longue portée,
  + Par lecteur QR code,
  + Par smartphone (badge numérique dématérialisé sur smartphone)
  + …
* La solution devra également fonctionner sur un seul serveur virtualisé, redondé et cloisonné, permettant d’absorber l’ensemble des besoins en contrôle d’accès des futurs bâtiments ainsi que l’ensemble des installations de contrôle d’accès de l’ensemble des sites du CHU de Toulouse à long terme, donc en multisites avec 7 à 16 sites cloisonnés
* La solution technique devra fonctionner en ONLINE et OFFLINE et devra supporter à long terme : 5000 lecteurs de badges, 100 000 badges, l’ensemble des opérateurs pour l’ensemble des sites du CHU de Toulouse
* La solution permettra l’interfaçage automatique avec le logiciel de gestion des ressources humaines : AGIRH, permettant la prise en compte et l’actualisation des données et des droits d’accès avec le logiciel d’exploitation et de gestion du système de contrôle d’accès à mettre en place
* La solution déployée permettra de prendre en charge l’actuelle et la future carte des professionnels de santé CPSx (CPS3/CPS4)/CPE du CHU de Toulouse.
* La solution prévue permettra également l’interfaçage natif et aisé avec les installations de visiophonie actuellement existantes sur les différents sites du CHU de Toulouse
* La durée de vie minimale des équipements sera de 15 ans avec interopérabilité des équipements entre ancienne et nouvelle génération de technologies
* L’installation de contrôle d’accès à mettre en place devra être modulaire et extensible (équipements, systèmes et logiciels d’exploitation et de supervision technique)
* La solution de contrôle d’accès devra fonctionner en redondance au niveau des serveurs virtuels et cloisonnés

## Badges

Le support des autorisations d’accès pour le personnel du CHU est la carte professionnelle.

La carte professionnelle est un badge permettant l’identification de la personne (nominative avec photo). Il permet également l’accès aux différents contrôles d’accès.

Ce badge est utilisé pour des prestations diverses telles que :

* Réfectoire
* Tenue
* Réservation de véhicules mutualisés
* Etc…

La Carte Professionnelle (CP), servant de badge pour le contrôle d’accès sur le site du CHU de Toulouse, comporte entre autres une technologie de type MIFARE 1ko HICO (ISO 14443). Le format visuel du badge est de format CB (ISO 7813).

Le format de badge actuel est de technologie MIFARE Classic avec l’utilisation du CSN (Card Serial Number) pour l’identification.

Les demandes de badges initiaux sont gérées par la plateforme RH du CHUT (AGIR RH).Il est à signaler que dans le processus la création des badges extérieurs est réalisée à la base sur l’un des systèmes et le transfert vers les autres systèmes n’est pas automatisé. Si un badge doit être créé ou supprimé sur le périmètre complet du CHUT, il nécessite un transfert d’informations et autant d’opérations que de systèmes concernés.

Actuellement, la volumétrie connue au CHU est de 16 000 agents et 2000 professionnels au niveau de IUCT Oncopole. Dans les bases de données ERO, NCS et NOVADIS, la volumétrie des fiches avoisine (estimatif): 64 000 fiches sur Rangueil et 30 000 fiches sur Purpan, soit :

* 100 000 fiches agents CHU
* 10 000 fiches pour Extérieurs : INSERM, ETUDIANTS, PRESTATAIRES EXTERIEURS, etc…

Un projet d’évolution de la carte CPSx3/CPSx4/CPE est en cours d’étude côté CHUT*.* L’évolution des cartes professionnelles est pilotée au niveau national par l’Agence des Systèmes d’Informations Partagées de Santé (ASIPS) et la production des cartes est le monopole de l’Imprimerie Nationale.

Le format de badge à utiliser par le futur système de contrôle d’accès doit être celui de la carte professionnelle CPx1 ou CPx3 ou encore CPx4. Pour les usagers extérieurs, le format de badge devra donc être de même technologie MIFARE que celui de la carte professionnelle.

**Le système et la solution de contrôle d’accès proposés par le fabricant retenu dans le cadre du présent marché devront avoir la capacité d’encoder les applications des badges MIFAIRE CLASSIC, DESFIRE EV1–EV2-EV3, mais également de fonctionner uniquement avec le CSN comme autorisation. La solution de contrôle d’accès proposée devra être compatible et fonctionnelle avec l’actuelle carte professionnelle utilisée dans les différents sites du CHU de Toulouse, ainsi que la future carte de provisionnels de santé CPSx « CPS3/CPS4 »/CPE en tenant compte des dernières exigences ANSSI-CSPN en vigueur. Elle devra permettre également un fonctionnement en simultané avec l’actuelle carte professionnelle utilisée au niveau du CHU de Toulouse, ainsi que les futures cartes « CPS3/CPS4 »/CPE.**

## Obligations diverses

### Garanties

Le Fournisseur garantit au client et aux installateurs du bon fonctionnement des produits conformément à leur documentation associée ainsi qu’aux spécifications techniques et/ou contractuelles (CCAP).

A ce titre, il s’engage pendant une durée de 2 ans, à compter de la date de livraison, à réparer gratuitement dans les délais réglementaires tout défaut affectant les produits (défaut de qualité, de fonctionnement, de rendement, de disponibilité...), ou à remplacer les dits produits.

Il s’engage également au bon fonctionnement des installations et des équipements de contrôle d’accès, à compter de la fin des paramétrages, des programmations, des intégrations, des essais et des mises en service des équipements prévus à la charge du fabricant dans le cadre du présent marché et à réparer gratuitement dans les délais réglementaires tout défaut affectant le fonctionnement des installations de contrôle d’accès (défaut de qualité des équipements, de fonctionnement, de rendement, de disponibilité...), ou à remplacer lesdits produits et de reprendre les paramétrages, programmations et intégrations nécessaires assurant le bon fonctionnement des installations et des équipements de contrôle d’accès dans le cadre du présent marché.

Cette garantie contractuelle n'exclut pas la garantie légale des vices cachés. Elle prend effet au jour de l'acceptation définitive ou de la réception définitive des produits.

L’obligation de garantie comprend la totalité des prestations et fournitures nécessaires aux corrections et remises en état des éléments fournis, reconnus défectueux après examen contradictoire des défauts constatés avec le fournisseur. L’obligation de garantie s’applique à partir du moment où le produit est revenu en usine.

Tous les frais résultant de cette obligation sont à la charge du fabricant, y compris le coût du transport retour de SAV. Les frais d’expédition auprès du réparateur, y compris la reprise du matériel défectueux sur les différents sites du CHUT seront à la charge du fabricant titulaire du présent marché.

En cas de défectuosité révélée au cours de cette période, la garantie est prolongée d'une durée égale à celle de l'indisponibilité de la pièce ou de l'ensemble des pièces.

Durée de garantie de base du fabricant concernant le matériel :2 ans à compter de la livraison des équipements. Avec une garantie de bon fonctionnement des installations de contrôle d’accès après les paramétrages, les programmations, les intégrations, les essais et les mises en service des équipements prévus à la charge du fabricant titulaire du présent marché.

Durée de garantie de base du fabricant concernant le logiciel :1 an après installations, programmations, paramétrages, intégrations et essais et mises en service des applicatifs des logiciels des installations de contrôle d’accès prévus dans le cadre du présent marché.

### Processus de retour des équipements défectueux

Le titulaire du présent marché devra à sa charge la reprise de l’ensemble du matériel de contrôle d’accès défectueux sur les différents sites du CHUT. Il prévoira une fréquence de passage sur les différents sites du CHUT d’une fois par mois et ce durant toute la durée du présent marché, afin de reprendre les équipements défectueux pour réparation et leur remise en état ou leur remplacement par des produits neufs fonctionnels.

Les frais des déplacements sur sites permettant la reprise du matériel défectueux, les frais de conditionnement et d’expédition des équipements à renvoyer en réparation seront à la charge du fabricant titulaire du présent marché. Il devra également prévoir à sa charge la réexpédition et le retour de l’ensemble du matériel réparé ou à remplacer par des produits neufs fonctionnels sur les différents sites du CHUT.

Le fabricant devra également durant toute cette période de prise en charge et de réparation ou de remplacement du matériel défectueux fournir les équipements provisoires de remplacement, paramétrés et programmés permettant d’assurer la continuité de service des installations de contrôle d’accès concernées par le dysfonctionnement matériel.

Le titulaire applique la méthodologie et le processus détaillés, contenu dans son offre, de la reprise du matériel défectueux en présentiel sur les différents sites du CHUT. Il détaillera tout le processus, la méthodologie et les délais de prise en charge, depuis : la reprise sur site des équipements défectueux, passant par le conditionnement, l’expédition des équipements, leurs réparations ou leurs remplacements, la mise à disposition des équipements provisoires de remplacement, ainsi que leur réexpédition et retour sur les différents sites du CHU de Toulouse.

### Réglementations et normes

Le fabricant s’engage à ce que les produits soient conformes, à tout moment, aux textes et normes en vigueur, applicables à son domaine d’activité, et en particulier ceux relatifs à la sécurité et la protection de l’environnement.

* Les normes et lois suivantes :
  + Les directives européennes RoHS, CE, DEEE obligatoires en Europe,
  + La RGPD,
  + La CNIL,
  + ….
* **Les certifications et qualifications ANSSI, suivant les préconisations du chapitre 3.1.**
* Les **engagements RSE** (Responsabilité Sociétale et Environnementale) du client final et avoir un moindre impact environnemental se répercutent au constructeur de la solution retenue.

Les produits devront par ailleurs être conformes aux normes françaises et/ou européennes applicables sur les sites d’installation des produits.

Le fabricant informera le client de la nécessité de l’adaptation des équipements acquis à l’évolution des normes et réglementations.

Le fabricant est responsable, conformément à la réglementation en vigueur, de la fin de vie des produits commandés par le M.O. A ce titre, le fabricant s’engage à :

* Communiquer au M.O et aux installateurs les modalités de reprise des produits en fin de vie,
* Reprendre les produits en fin de vie afin de les démanteler puis de tirer les divers éléments pour les détruire dans le respect des normes en vigueur (et notamment dans le respect de la réglementation relative à l’élimination des déchets électriques et électroniques).

Le fabricant s’efforce d’agir dans le respect des lois et règlements Français ou internationaux relatifs à la protection de l’environnement qui lui sont applicables.

Dans les différentes étapes de son activité, le fabricant s’efforce de maîtriser et/ou minimiser les impacts de ses activités sur l’environnement, notamment en termes de consommations (eau, énergie et matières premières), d’émissions de gaz à effet de serre, de pollution (eau, sol, air) et de production de déchets (tri sélectif, recyclage). Il s’efforcera également à développer des technologies respectueuses de l’environnement en limitant l’impact environnemental de ses produits ou services sur l’ensemble de leur cycle de vie.

# PRESCRIPTIONS TECHNIQUES PARTICULIERES

## Généralités

Le système sera impérativement capable de centraliser la gestion de la sécurité avec un fonctionnement en temps réel, de plusieurs sites distants géographiquement, sur un seul serveur virtualisé, cloisonné et redondé commun à l’ensemble des sites du CHU de Toulouse.

Son exploitation offrira la simplicité d’un système dans l’optimisation des tâches et sera paramétrable par l’exploitant. Le système devra être particulièrement modulaire et extensible et devra aussi bien fonctionner sur une architecture de type BUS de terrain (RS485), ainsi que sur une architecture native TCP/IP.

Il sera basé sur une architecture à différents niveaux :

* Niveau 1 : Les terminaux terrain (têtes de lecture pour le contrôle d’accès/lecteurs de badges « tout type », BP, BG vert, contacts…). **Ce matériel ne pourra être propriétaire, il sera impérativement basé sur des standards du marché**
* Niveau 2 : Les Concentrateurs et/ou Centrales permettant la gestion des périphériques en local et garantissant une autonomie de fonctionnement en cas de perte de réseau d’exploitation ou de serveur
* Niveau 3 : Le logiciel d’exploitation qui se devra convivial et permettra le paramétrage du système dans sa globalité et l’exploitation temps réel des différents « métiers » de la sûreté souhaités (Contrôle d’accès, …) et l’interfaçage avec d’autres logiciels (AGIRH, Web service, logiciel de gestion technique GTC) du Maître d’ouvrage (CHUT)
* Niveau 4 : lecteur enrôleur/encodeur : permettant l’encodage et l’enrôlement des badges :cartes de professionnels de santé /badges et étiquettes UHF
* …

Les systèmes quelle que soit leur version devront être compatibles avec la suite logicielle **Air’Evolution** (**PCPass, XT Manager, Horizon Evolution**) de marque **Synchronic** ou techniquement équivalent et devront pouvoir fonctionner nativement en mode MODBUS/TCP.

Le fabricant retenu dans le cadre du présent marché devra donc proposer une véritable suite logicielle dont les interfaces systèmes partagent une ergonomie, une structure, une iconographie et une signalétique identiques. Ces interfaces seront complétées par des scénarios configurables secondant l'opérateur par des tâches automatiques et/ou planifiées.

Les événements remontant d’un équipement lié à la sûreté comme le contrôle d’accès devront avoir la capacité de générer des actions automatiques ou non avec l’ensemble des équipements de sûreté et de sécurité.

Le système de contrôle d’accès proposé devra permettre la possibilité de communiquer et s’interfacer avec les autres logiciels du maître d’ouvrage de type : AGIRH, web service ou logiciel de gestion des installations techniques (GTC) existants sur les différents sites du CHU de Toulouse. **Le système de contrôle d’accès permettra de remonter et de renvoyer une synthèse des défauts des équipements de contrôle d’accès (UTL,LB …) depuis le logiciel de supervision de contrôle d’accès « Horizon Vision » ou équivalent vers le logiciel « PCVue » de supervision GTC existant sur les sites du CHUT et cela sera réalisé nativement dans la solution de contrôle d’accès sans ajout de licences complémentaires.**

**Le système disposera impérativement d’une certification et d’une qualification ANSSI-CSPN sur l’ensemble de la chaîne (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB ») et ce conformément aux dernières exigences en vigueur ANSSI-CSPN.**

**Le titulaire transmet les documents justificatifs : les qualifications et les certifications ANSSI ou à minima :**

* **Une certification et une qualification ANSSI-CSPN en cours de validité.**
* **Ainsi que les documents justifiants des procédures de certifications et de qualifications en cours sur l’ensemble de la chaîne de la solution de contrôle d’accès (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB ») proposée dans le cadre du présent marché et ce conformément aux dernières exigences en vigueur ANSSI-CSPN.**

Ces qualifications et certifications doivent être effectives tout au long de la durée du marché.

## Solution logicielle

### Généralités

L'application de contrôle d'accès devra permettre la gestion centralisée du système de contrôle d’accès sur un seul serveur cloisonné, virtualisé et redondé (en mode On-premise). Chaque gestionnaire de chaque site respectif pourra accéder et administrer uniquement son site respectif et ne pourra accéder et administrer les autres sites du CHU de Toulouse et notamment ceux qui ne relèvent pas de son périmètre de gestion.

La solution de contrôle permettra d’absorber l’ensemble des besoins (futurs et actuels) en contrôle d’accès, ainsi que l’ensemble des installations de contrôle d’accès de l’ensemble des sites du CHU de Toulouse à long terme, donc en multisites avec **7 à 16** sites cloisonnés.

La solution technique devra fonctionner en **ONLINE et OFFLINE** et devra supporter à long terme : **5 000 lecteurs** **de badges**, **100 000 badges**, **l’ensemble des opérateurs et gestionnaires des droits d’accès** pour l’ensemble des sites du CHU de Toulouse

Les logiciels proposés devront impérativement être compatibles avec les logiciels de la suite **Air'Evolution de Synchronic** (**PCPass, XT Manager, Horizon Evolution**…)ou techniquement équivalent

Le système proposé devra répondre en tout point aux dernières préconisations en vigueur de l’ANSSI-CSPN qui précisent entre autres les éléments suivants :

* L'authentification du badge doit reposer sur une clé commune ou une clé dérivée d'une clé maîtresse .L'utilisation d'une puce Mifare, DESFire est donc la solution la plus adaptée.
* Aucune information ne doit circuler en clair sur le canal sans fil et la liaison filaire, les liaisons de type Data-Clock/Wiegand sont donc à proscrire.
* La tête de lecture ne doit contenir aucun secret (suivant les dernières exigences ANSSI-CSPN en vigueur).
* Etc.

**Le système permettra également de fonctionner simultanément avec l’actuelle carte professionnelle de santé du CHU de Toulouse et la future carte de professionnels de santé CPSx (CPS3/CPS4)/CPE**

**Les solutions logicielles disposeront impérativement d’une certification et d’une qualification ANSSI-CSPN et ce conformément aux dernières exigences en vigueur de l’ANSSI-CSPN.**

**Le titulaire transmet les documents justificatifs : les qualifications et les certifications ANSSI ou à minima :**

* **Une certification et une qualification ANSSI-CSPN en cours de validité.**
* **Ainsi que les documents justifiants des procédures de certifications et de qualifications en cours sur l’ensemble de la chaîne de la solution de contrôle d’accès (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB ») proposée dans le cadre du présent marché et ce conformément aux dernières exigences en vigueur ANSSI-CSPN.**

Ces qualifications et certifications doivent être effectives tout au long de la durée du marché.

### Logiciel d’exploitation et gestion des droits

Le système devra être administré à la fois par :

* Une application de type client lourd de série **PC PASS** de marque **Synchronic** ou techniquement équivalent à installer au niveau du serveur virtuel, cloisonné et redondé. Elle sera suffisamment dimensionnée afin d’absorber l’ensemble des besoins du CHU de Toulouse détaillés dans le chapitre 4.2.Elle disposera également de l’ensemble des licences et des fonctionnalités nécessaires suivant les préconisations du présent programme.
* Une application web client/serveur de type **XT Manager** de marque **Synchronic** ou techniquement équivalent à installer sur les postes des gestionnaires du pour chaque site respectif.

Les solutions proposées devront disposer d’une interface graphique conviviale et intuitive, en français et devront proposer une interface avec un thème clair et un thème sombre au choix de l'utilisateur.

Les applicatifs de type client lourd et léger devront s’interfacer automatiquement avec la base de données **AGIR RH (logiciel de gestion RH du CHUT)**, afin de récupérer automatiquement la base de données RH du CHU de Toulouse par Unités Fonctionnelles (UF) permettant d’attribuer les droits d’accès automatiquement par UF depuis ces applicatifs et ce pour chaque site respectif du CHU de Toulouse.

Ils devront également s’interfacer nativement et automatiquement avec le futur annuaire centralisé des futures cartes CPSx et CPE, afin de récupérer automatiquement la base de données permettant d’attribuer les droits d’accès automatiquement et ce pour chaque site respectif du CHU de Toulouse. Les applicatifs devront donc fonctionner simultanément sur plusieurs bases de données du CHUT permettant de récupérer automatiquement les données nécessaires pour attribuer automatiquement les droits d’accès aux différents profils (personnels soignants, autres professionnels du CHUT, prestataires externes, étudiants et stagiaires, flottes logistiques du CHUT…).

Les applicatifs devront être capables d’attribuer automatiquement pour un profil donné plusieurs types de badges depuis plusieurs bases de données et bloquer ou supprimer les badges sur un ou des critères spécifiques récupérés sur une des deux bases de données ou les deux bases de données simultanément.

Les applicatifs permettront également d’attribuer les droits d’accès pour chaque site respectif :

* Par personne,
* Par groupe de personne,
* Par unité fonctionnelle,
* Par mode multi-familles,
* Par métier et par code métier,
* Par accès,
* Par zone ou groupe d’accès,
* Par site,
* Par bâtiment,
* Par type de parking,
* Par grilles horaires,
* Par visiteur,
* Par plusieurs numéros de badges par personne,
* Par véhicule CHUT (ambulance, voiture de service, véhicules de logistique…)
* ….

L’encodage et l’enrôlement des badges (actuelles cartes de santé et futures cartes CPSx)/CPE) devront obligatoirement être intégrés depuis les deux applicatifs (client lourd et léger). Les bases de données centralisées devront être simultanément et automatiquement mises à jour et ce quel que soit l’applicatif utilisé (client lourd ou léger) par les différents gestionnaires des sites.

Afin de garantir une interopérabilité du système, le logiciel de contrôle d’accès devra impérativement disposer d’une **API REST** via Webservice.

Les applications devront obligatoirement intégrer une visualisation de passage et un fil de l'eau en temps réel.

Les applications permettront un fonctionnement en Online en temps réel et un fonctionnement en Offline, avec récupérations de l’historique et des différents événements archivés, lors d’un passage d’un fonctionnement du mode Offline au mode Online des équipements de contrôle d’accès.

Les applications devront obligatoirement permettre de hiérarchiser les profils exploitants pour l’administration du contrôle d’accès. Il devra être possible de définir un administrateur général, ayant un accès total à la base de données et des gestionnaires ayant un accès limité à leurs zones d’action. Ce système d’administration pourra être adapté à tous types de fonctionnements. (Administration par zone géographique, site, bâtiment, métier, service...).**Ce système de gestion sera adapté dans le cadre de notre marché au fonctionnement détaillé ci-dessus dans le chapitre 4.4.2. (Serveur, virtualisé, cloisonné et redondé, avec l’accès limité par le gestionnaire du site à son site respectif).**

les applicatifs de type client lourd et client léger devront également et nécessairement être compatibles avec :

* La technologie SSO (service d’authentification)
* La technologie IAM (règles de gestion de l’identité et des accès)

Ils permettront nativement la gestion des fonctionnalités suivantes :

* Gestion des visiteurs,
* Gestion des clés de chiffrement et enrôlements/encodages des cartes,
* Gestion des ascenseurs,
* Gestion des SAS,
* Gestion de fonctionnalités d’anti-passback / anti-timeback,
* Gestion des clés et serrures mécatroniques,
* Gestion des serrures électroniques et autonomes,
* Gestion des badges dématérialisés sur smartphone (le contrôle d’accès via smartphone),
* Gestion horaire des accès,
* Gestion des accès parking,
* etc…

les applicatifs de contrôle d'accès devront également intégrer les fonctionnalités suivantes :

* Redondance à chaud :Afin de se prémunir contre toutes défaillances du serveur d’application, et de maintenir un très haut niveau de disponibilité, la solution devra disposer d’un mécanisme de redondance à chaud permettant de basculer automatiquement vers un serveur de secours en cas de défaillance du serveur principal.
* Interfaçage base LDAP(S), AD :Le système de contrôle d’accès devra obligatoirement s’interfacer sur l’annuaire LDAP du CHUT afin de permettre une synchronisation en temps réel de la base de données du contrôle d’accès sur l’annuaire de LDAP du CHUT (et autres bases de données du CHUT)
* Encodages/enrôlement et impressions des badges (cartes de professionnels de santé), y compris la gestion des clés de chiffrement
* Extensions aisées des : applicatifs en fonction du nombre :des équipements, des badges (utilisateurs) et nombre de gestionnaires de site (opérateurs), et autres fonctionnalités liées aux gestions des droits d’accès
* S’interfacer nativement avec le système de visiophonie actuellement existant sur le CHU de Toulouse de marque CASTEL
* …

Les fonctionnalités essentielles du contrôle d’accès telles que :

* Connecteur à une base de données tierces, exemples :
  + AGIR RH, (logiciel des Ressources Humaines du CHUT)
  + Les bases de données centralisées sous forme d’annuaire,(cartes et badges :CPSR3-V4, CPSx/CPE)
  + Toutes les bases de données des prestataires extérieurs du CHUT,
  + Les bases de données des étudiants et stagiaires du CHUT,
  + Les bases de données de la logistique, y compris les parcs de véhicules du CHUT,
  + Fichiers structures de type CSV,
  + Autres bases de données,
* Comptages,
* Historiques,
* Reporting,
* Visualisation des passages en temps réel,
* Fil de l’eau en temps réel,
* Accès hiérarchisé,
* ….

**Devront être natives dans l’application (prévues et intégrées dans l’application), et non soumises à licence.**

Les applicatifs de type client lourd et léger permettront également le fonctionnement avec d’autres logiciels de type web services (portail WEB)….

**Chaque lecteur et chaque UTL ne fera pas l’objet d’une licence spécifique dépendant du niveau de sécurité, l’application intègrera nativement tous les niveaux requis.**

L’applicatif devra nativement gérer les technologies détaillées ci-dessous et il devra obligatoirement être possible pour chaque utilisateur de définir plusieurs identifiants appartenant à plusieurs technologies d’identification :

* MIFARE Classic / Ultralight C / MIFARE Plus,
* MIFARE DESFire/DESFire EV1-EV2-EV3,Bleutooth,
* Cartes de professionnels de santé de type : CPS3/CPS4/CPE, ainsi que les cartes et badges utilisés actuellement dans l’ensemble des sites du CHU de Toulouse,
* Biométrie et lecteurs biométriques,
* Lecteurs de plaques minéralogiques,
* lecteurs longue distance UHF,
* Serrures autonomes online et offline,
* Serrures électriques,
* Clés et serrures mécatroniques online et offline,
* Contrôle d’accès par smartphones (badges numériques dématérialisés sur smartphones)
* etc.

Il sera donc prévu la fourniture, l’installation et l’intégration par le fabricant titulaire du présent marché sur l’ensemble des sites du CHU de Toulouse :

* 1 applicatif de type client lourd avec toutes ses licences et ses fonctions, au sein du serveur virtuel, cloisonné et redondé commun à l’ensemble des sites du CHU de Toulouse, permettant d’absorber l’ensemble des besoins des sites des CHU de Toulouse :(tous les lecteurs de badges, tous les badges, l’ensemble des utilisateurs, l’ensemble des sites, l’ensemble des d’opérateurs). Avec un fonctionnement en multisites et un accès limité de chaque gestionnaire à son site respectif. L’applicatif lourd disposera de l’ensemble de ses licences et des fonctionnalités détaillées ci-dessus.
* Un applicatif de type client léger à prévoir au niveau des postes détaillés ci-dessous :
  + 1 applicatif de type client léger sur le poste informatique du gestionnaire principal, pour chaque site respectif
  + 2 applicatifs de type client léger sur les deux postes secondaires des gestionnaires, pour chaque site respectif
  + 2 applicatifs de type client léger sur les ordinateurs portables des gestionnaires des sites, pour les sites de Rangueil et Purpan

Les sites seront organisés et cloisonnés sur un seul serveur virtuel, comme détaillé ci-dessous :

* Site :Purpan-Garonne
* Site :Rangueil-Larrey
* Site : Chapitre
* Site : Logipharma
* Sites :Hôtel-Dieu-La Grave
* Site :Salies du salat
* Site :IUCT Oncopole

**Le fonctionnement de la solution de contrôle d’accès sera prévu en redondance au niveau des serveurs virtuels et cloisonnés. Les applicatifs seront suffisamment dimensionnés et garantiront le fonctionnement en redondance sur ces serveurs virtuels avec un basculement en automatique et sans coupure vers le serveur secondaire en cas de dysfonctionnement du serveur principal.**

**les applicatifs (client lourd/léger) disposeront obligatoirement de la certification et la qualification ANSSI-CSPN conformément aux dernières exigences en en vigueur ANSSI-CSPN.**

**Le titulaire transmet les documents justificatifs : les qualifications et les certifications ANSSI ou à minima :**

* **Une certification et une qualification ANSSI-CSPN en cours de validité.**
* **Ainsi que les documents justifiants des procédures de certifications et de qualifications en cours sur l’ensemble de la chaîne de la solution de contrôle d’accès (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB ») proposée dans le cadre du présent marché et ce conformément aux dernières exigences en vigueur ANSSI-CSPN.**

Ces qualifications et certifications doivent être effectives tout au long de la durée du marché.

### Logiciel de chiffrement des cartes

Le logiciel d'administration du contrôle d'accès devra être fourni avec un module **Secur'Evolution de marque Synchronic**, ou techniquement équivalent, ce dernier sera mis en œuvre au niveau du serveur virtuel, cloisonné et redondé avec la solution dite « client lourd » et sera accessible à l’ensemble des gestionnaires de tous les sites du CHU de Toulouse depuis l’applicatif dit « client léger » depuis chaque poste de chaque gestionnaire.

L’administration et le transfert des clés de chiffrements vers les lecteurs se feront de manière centralisée depuis le serveur virtualisé, toutes les solutions à base de badge de configuration à présenter devant chaque lecteur seront à proscrire. La solution devra permettre de gérer simultanément deux types de badges encodés différemment, soit avec deux applications distinctes (AID) soit deux fichiers différents dans la même application, et ceci afin de permettre de s’affranchir de toute compromission clé ou de renouvellement de clé.

#### Gestion de clés de chiffrements

La clé de chiffrement devra être amovible au format SE. Elle garantira une sécurité optimale par un cryptage de ses informations en EAL6+ et un confort d’utilisation dans la gestion des secrets.

L’administration des clés de chiffrement devra être centralisée via le logiciel **Secur’Evolution** de marque Synchronic ou équivalent. Le chargement des secrets dans les modules SAM peut être réalisé des deux manières suivantes :

* Téléchargé de manière sécurisée depuis le serveur vers les automates **Xsecur’Evo ou techniquement équivalent**
* Ou depuis la station d’encodage des modules SAM, raccordée sur un port USB du poste de gestion

La solution permettra également :

* Une saisie des clés en direct ou via cérémonie (plusieurs personnes apportent une partie du secret)
* Gestion des clés diversifiées (permet d’avoir des clés uniques pour chaque badge)
* Le support simultané de 2 configurations MIFARE, DESFire EV2 et EV3, par lecteur (ex: badge entreprise + badge visiteur, badge Agent + badge blanc)
* Suppression des clés et/ou identifiant sur autoprotection coffret, manuellement, à distance ou via procédure matérielle
* Le client final aura la maîtrise totale des secrets

Il sera interdit aux :fabricant/l’entreprise/intégrateur d’avoir accès ou visualiser la ou les clés de chiffrement, dont seul l’exploitant (le CHUT) en aura la connaissance.

Dans le cas, du secret corrompu ou à risque, il sera possible d’administrer la gestion du secret en local via une unité de gestion complètement détachée du réseau, localisée dans un local sécurisé ou à travers le serveur d’applications via le réseau WAN dédié pour être distribué sur bus sécurisé jusqu’aux équipements de sûreté. Cette gestion sera réservée au choix de l’exploitant. Tout secret stocké sur clé de type HSM sera refusé.

### Logiciel de supervision des équipements de contrôle d’accès

Le logiciel **Horizon Evolution** de marque **Synchronic** ou techniquement équivalent sera proposé. Il offrira une interface de gestion unique pour chaque opérateur, afin de gérer l’ensemble des informations en provenance des différents équipements de contrôle d’accès pour chaque site respectif.

Le logiciel devra impérativement permettre un nombre illimité de plans.

Il répondra aux spécifications techniques suivantes :

* Créer des vues graphiques par :
  + Site
  + Bâtiment
  + Niveau
  + Zone ou service
  + Equipement de contrôle d’accès
* Créer des vues graphiques sophistiquées pour visualiser l’état de l'installation, de chaque :
  + Site
  + Bâtiment
  + Niveau
  + Zone et ou service
  + Equipement de contrôle d’accès
* Archiver les événements dans une base de données pour pouvoir les analyser ultérieurement, par :
  + Site
  + Bâtiment
  + Niveau
  + Zone et ou service
  + Equipement de contrôle d’accès
* Visualiser et contrôler la liste des alarmes en cours, par
  + Site
  + Bâtiment
  + Niveau
  + Zone et ou service
  + Equipement de contrôle d’accès
* Visualiser l’évolution des variables de supervision sous forme de courbes, en temps réel ou à partir des données enregistrées dans l’historique des événements, par
  + Site
  + Bâtiment
  + Niveau
  + Zone et ou service
  + Equipement de contrôle d’accès
* Calculer des statistiques sur les valeurs des variables supervisées,
  + Site
  + Bâtiment
  + Niveau
  + Zone et ou service
  + Equipement de contrôle d’accès
* Importer et exporter des états et des historiques, par
  + Site
  + Bâtiment
  + Niveau
  + Zone et ou service
  + Equipement de contrôle d’accès
* S’interfacer automatiquement et renvoyer les informations au niveau de la supervision GTC (logiciel de type PC vue) de chaque site respectif
* S’interfacer nativement avec le système de visiophonie actuellement existant sur le CHU de Toulouse de marque CASTEL

Il sera donc prévu la fourniture, l’installation et l’intégration par le fabricant titulaire du présent marché :

* 1 applicatif de supervision des équipements techniques au sein du serveur virtuel, cloisonné et redondé, permettant d’absorber l’ensemble des besoins des sites des CHU de Toulouse:(tous les lecteurs de badges, tous les badges, l’ensemble des utilisateurs, l’ensemble des sites, l’ensemble des opérateurs). Avec un fonctionnement en multisites et un accès limité de chaque gestionnaire à son site respectif.

* Les applicatifs de supervision technique suivants au niveau des postes détaillés ci-dessous :
  + 1 applicatif de supervision technique sur le poste informatique du gestionnaire principal des droits d’accès, **pour chaque site respectif**
  + 2 applicatifs de supervision technique sur les deux potes pour les services d’exploitation et de maintenance, pour le site de Rangueil
  + 4 applicatifs de supervision technique sur les quatre potes pour les services d’exploitation et de maintenance, pour le site de Purpan
  + 1 applicatif de supervision technique sur un pote pour les services d’exploitation et de maintenance, pour le service de la DSN situé sur le site de l’Hôtel Dieu
  + 1 applicatif de supervision technique sur un pote pour les services d’exploitation et de maintenance, pour autres sites respectifs.

Les sites seront organisés et cloisonnés sur un seul serveur virtuel, comme détaillé ci-dessous :

* Site :Purpan-Garonne
* Sites :Rangueil-Larrey
* Site : Chapitre
* Site : Logipharma
* Sites :Hôtel-Dieu-La Grave
* Site :Salies du salat
* Site :IUCT Oncopole

Le système de contrôle d’accès proposé devra permettre la possibilité de communiquer et s’interfacer avec les autres logiciels du maître d’ouvrage de type : web service ou logiciel de gestion des installations techniques (GTC) existants sur les différents sites du CHU de Toulouse. **Le système de contrôle d’accès permettra de remonter et de renvoyer une synthèse des défauts des équipements de contrôle d’accès (UTL,LB …) depuis le logiciel de supervision de contrôle d’accès « Horizon Vision » ou techniquement équivalent vers le logiciel de supervision GTC « PCVue » existant sur les sites du CHUT et cela sera réalisé nativement dans la solution de contrôle d’accès à prévoir dans le cadre du présent marché et ce sans ajout des licences complémentaires à la licence globale de la solution de contrôle d’accès, et qui sera à prévoir dans le cadre du présent marché à la charge du fabricant.**

**Le logiciel disposera obligatoirement de la certification et de la qualification ANSSI-CSPN conformément aux dernières exigences en en vigueur ANSSI-CSPN.**

**Le titulaire transmet les documents justificatifs : les qualifications et les certifications ANSSI ou à minima :**

* **Une certification et une qualification ANSSI-CSPN en cours de validité.**
* **Ainsi que les documents justifiants des procédures de certifications et de qualifications en cours sur l’ensemble de la chaîne de la solution de contrôle d’accès (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB ») proposée dans le cadre du présent marché et ce conformément aux dernières exigences en vigueur ANSSI-CSPN.**

Ces qualifications et certifications doivent être effectives tout au long de la durée du marché.

## Equipements de contrôle d’accès

### Généralités

Les équipements de contrôle d’accès proposés par le fabricant titulaire du présent marché seront administrés, gérés et remonteront et communiqueront nativement avec les solutions applicatives (logiciels) proposées par le fabricant du contrôle d’accès (suivant le chapitre 4.2). Les équipements de contrôle d’accès seront nativement compatibles et communicants avec les applicatifs (logiciels) proposés par le fabricant du contrôle d’accès dans le cadre du présent marché. L’ensemble (les applicatifs et les équipements de contrôle d’accès) formeront une solution unique et native d’un seul système de contrôle d’accès, certifié et qualifié ANSSI-CSPN, suivant les exigences de la dernière version ANSSI-CSPN en vigueur à la date de la signature du marché.

**Les équipements de contrôle d’accès disposeront impérativement d’une certification et d’une qualification ANSSI-CSPN ce conformément aux dernières exigences en vigueur ANSSI-CSPN. D’une manière générale l’ensemble de la chaîne de la solution de contrôle d’accès (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB, etc…») disposera d’une certification et d’une qualification ANSSI-CSPN et ce conformément aux dernières exigences en vigueur ANSSI-CSPN**

**Le titulaire transmet les documents justificatifs : les qualifications et les certifications ANSSI ou à minima :**

* **Une certification et une qualification ANSSI-CSPN en cours de validité.**
* **Ainsi que les documents justifiants des procédures de certifications et de qualifications en cours sur l’ensemble de la chaîne de la solution de contrôle d’accès (serveurs, logiciels « GAC », et équipements « UTL, UCP, LB ») proposée dans le cadre du présent marché et ce conformément aux dernières exigences en vigueur ANSSI-CSPN.**

Ces qualifications et certifications doivent être effectives tout au long de la durée du marché.

### Lecteur d’enrôlement et d’encodage des badges

#### Lecteurs d’enrôlement et d’encodage des badges (cartes des professionnels de santé CPSX/CPE)

Pour chaque gestionnaire de site et pour l’ensemble des sites du CHU de Toulouse, le fabricant titulaire du présent marché devra la fourniture et la mise en place d’un lecteur USB pour l'enrôlement et l’encodage des badges utilisateurs (cartes actuelles des professionnels de santé et futures carte CPSX-V4)/CPE. Ce lecteur encodeur permettra d’encoder et d’enrôler les actuelles cartes de professionnels de santé utilisées actuellement par le CHU de Toulouse, mais également les futures cartes de professionnels de santé CPSX (CPS3/CPS4)/CPE et ce conformément aux dernières exigences ANSSI-CSPN en vigueur.

L’enrôlement et l’encodage de ces cartes de professionnels de santé (CPS3/CPS4/CPSx)/CPE se feront nativement depuis les applicatifs d’administration et de gestion des droits de la solution de contrôle d’accès proposée par le fabricant dans le cadre du présent marché.

Caractéristiques techniques minimales :

* Lecteur enrôleur USB de badge de proximité 13,56 MHz
* Lecture / écriture (encodeur)
* Protocoles :
  + T=CL, MIFARE®, iCLASS®
  + DESFire EV1 / DESFire EV2/DESFire EV3
  + ISO 14443A/B - jusqu'à 848 kbits/s (selon la carte)
  + ISO 15693 - jusqu'à 26 kbits/s (selon la carte)
  + Balise NFC Tag 1-4\*
  + Lecture/écriture avec jeton FIDO2 NFC
* Interface USB :
  + Périphérique USB 2.0 pleine vitesse (12 Mbits/s)
  + Opérabilité étendue USB 3.0, testée avec des concentrateurs/contrôleurs
* Connecteur/câble :
  + Connecteur USB de type A ; câble de 150 cm (59,1 po)
* Pilote:
  + Pilote CCID intégré au système d'exploitation (Windows/Linux/Mac)
* API prises en charge  :
  + PC/SC - API
* Voyant d’état :
  + LED blanche
* Boitier :
  + Polycarbonate
  + Corps gris clair / Cache disponible en différentes couleurs
  + Logo ou couleur spécifique au client sur demande
* Dimensions :
  + 59 x 59 x 11,4 mm
* Poids :
  + ~70 g
* Température de fonctionnement :
  + (0-70 °C)
* Température de stockage :
  + (-40 - 80 °C)
* Intervalle moyen entre défaillance :
  + 500 000 heures
* Conformité règlementaire :
  + USB 2.0
  + Certifications régionales CE, UKCA, FCC, UL, KCC, RCM
  + Caractéristiques environnementales WEEE, RoHS2, Reach
* Accessoire et kit de montage :
  + Kit d'accessoires de montage
  + Porte-carte pour l'opération de présence de carte

Série : **31-USB-XT** de marque Synchronic ou techniquement équivalent

#### Lecteurs d’enrôlement et d’encodage des badges et des étiquettes UHF

Pour chaque gestionnaire de site et pour l’ensemble des sites du CHU de Toulouse, le fabricant titulaire du présent marché devra la fourniture et la mise en place d’un lecteur USB pour l'enrôlement et l’encodage des badges et étiquettes de type UHF. Ce lecteur encodeur permettra d’encoder et d’enrôler les cartes et les étiquettes UHF conformément aux dernières exigences ANSSI-CSPN en vigueur.

L’enrôlement et l’encodage des badges et étiquettes UHF se feront nativement depuis les applicatifs d’administration et de gestion des droits de la solution de contrôle d’accès proposée par le fabricant dans le cadre du présent marché.

Le lecteur d’enrôlement et d’encodage des badges et des étiquettes UHF permettra d’enrôler et d’encoder les futures cartes et étiquettes UHF de la nouvelle solution de contrôle d’accès prévue dans le cadre du présent marché et permettra également d’enrôler et d’encoder les cartes et les étiquettes UHF de marque « TAG Master » actuellement utilisées sur les différents sites du CHUT et notamment pour le parc des véhicules du CHUT

Caractéristiques techniques minimales :

* Gabarit et/ou dimensions :126 x 80 x 30 mm
* Puce :EPC1 Gen 2 (ISO18000-6C)
* Couleurs et / ou design et / ou matière :Noir ABS
* Fonctions :Lecture
* Température de fonctionnement min / max :0°C à +50°C
* Alimentation :5VDC (câble USB)
* Distance de lecture :0 – 1m
* Consommation :100 mA
* Fréquence :125 kHz
* Réf. constructeur :
  + STR-SWEDGE-W45 (ETSI USB)
  + STR-SWEDGE-W55 (FCC USB)
* Normes :CE

Ce dernier sera fourni avec son logiciel natif du fabricant de série :STid SWedge pour l’enrôleur UHF ou techniquement équivalent.

Série : **31-SWEDGE-W45** de marque Synchronic ou techniquement équivalent

### Unité de Traitement Local (UTL) et Unité de de Traitement de Porte (UTP)

Unité de Traitement Local devra être nativement en POE et permettra de gérer 2 accès (2 portes) ou 4 accès (4 portes) suivant les préconisations détaillées ci-dessous. Elle sera certifiée et qualifiée ANSSI-CSPN (suivant les préconisations du poste 3.1) et sera de série UTL **Xsecur'-Evo de marque Synchronic** ou techniquement équivalent**.**

L’UTP sera associée à une unité de traitement de porte (UTP) permettant de gérer deux accès, elle sera également certifiée et qualifiée ANSSI-CSPN (suivant les préconisations du poste 3.1). L’ensemble (UTL et UTP) sera monté, précablé sur des borniers dans un seul coffret autoprotégé. Des borniers seront laissés en attente dans ce coffret et permettront les raccordements des équipements terminaux des installations de contrôle d’accès (LB, BG, BP…).

#### Caractéristiques techniques minimales UTL :

* UTL fonctionnant en POE nativement
* Native IEEE 802.3 af « POE » et IEEE 802.3 at « POE+ » (4 portes-4 lecteurs en POE et 6 portes 6 lecteurs en POE +)
* Nombre de bus : 1 à 3 bus
* Nombre de lecteurs de base sur carte mère : 1 ou 2 lecteurs pour 1 porte ou accès (E/S)
* Nombre max de lecteurs : 15 à 45 par le bais d’UTP
* Nombre de familles CA : 300
* Nombre de plages horaires CA : 128
* Nombre identifiants (badges/codes) maximum : 200 000
* Nombre de points d’alarmes : 0 à 360
* Transmission IP : Oui - Natif - chiffrée AES128 et AES256 - protocole TLS
* Transmission LTE/4G : Option
* Module SAM : Amovible EAL6+
* Authentification 802.1x : Oui
* Protection des firmwares : signés, chiffrés, authentifiés
* TCP / IP : Oui - Natif
* Événements mémoire : 32 000
* Lignes de programmation : 2 000
* Dialogue inter UTL : Oui
* L’ensemble sera monté et précablé au sein d’un coffret autoprotégé avec les dimensions suivantes 260x225x110mm

En plus de ces fonctionnalités le système proposé pourra également permettre :

* la gestion du contrôle d'accès pour les ascenseurs
* la gestion de SAS
* la gestion de fonctionnalités d’anti-passback / anti-timeback sur au minium 2 zones distinctes
* le raccordement de lecteur biométrique
* le raccordement de lecteur / clavier
* la transmission des alarmes via LTE/4G
* la transmission vocale des alarmes
* le secours GSM pour la transmission des alarmes

Ces UTL permettront la garantie d’un fonctionnement en mode dégradé en cas de rupture du réseau de communication avec le serveur d’exploitation.

#### Caractéristiques techniques minimales UTP :

* BUS RS-485 chiffré / 1 module = 2 lecteurs
* Gestion des secrets sur carte SAM SE (certification EAL 6+)
* 5 Entrées natives et programmées : Boutons poussoirs (entrée – sortie) - Etat du BBG - Contact de position de porte - Contact d’état de verrouillage de porte
* Possibilité de mémoriser 10 badges de secours par UTP en cas de non réponse de l’UTL
* Intégration en coffret auto protégé alimenté ou non, avec possibilité de pré-montage en atelier.
* L’ensemble sera monté et précablé au sein d’un coffret autoprotégé avec les dimensions suivantes 260x225x110mm

Série : **CN-UTP-SEC-EVO** de marque Synchronic ou techniquement équivalent

#### Caractéristiques techniques minimales UTL et UTP précablées :

Dans le cadre du présent marché, il sera prévu la fourniture d’UTL et d’UTP avec les cartes relais nécessaires d’alimentation, montés et précablés dans un coffret autoprotégé, permettant la gestion des deux portes. Ces dernières disposeront des caractéristiques minimales détaillées ci-dessus et seront raccordées entre elles et sur des borniers dûment repérés au sein de ce coffret permettant les futurs raccordements des équipements terminaux de contrôle d’accès (LB, BG vert, BP…).

Le coffret autoprotégé abritant l’UTL, l’UTP et la carte relais d’alimentation (carte relais de puissance), les borniers pour la gestion deux portes disposera des dimensions minimales suivantes : 260x225x110mm. L’ensemble sera fourni avec des schémas électriques de raccordements détaillés. Les équipements seront certifiés et qualifiés ANSSI-CSPN (suivant les préconisations du poste 3.1 du présent programme).

De la même manière, il sera prévu dans le cadre du présent marché la fourniture d’UTL et des cartes UTP avec les cartes relais nécessaires d’alimentation, montés et précablés dans un coffret autoprotégé, permettant la gestion des 4 portes. Ces dernières disposeront des caractéristiques minimales détaillées ci-dessus et seront raccordées entre elles et sur des borniers dûment repérés et suffisamment dimensionnés au sein de ce coffret permettant les futurs raccordements des équipements terminaux de contrôle d’accès (LB, BG vert, BP…).

Le coffret autoprotégé abritant l’UTL, les cartes UTP et les cartes relais d’alimentation (carte relais de puissance), les borniers pour la gestion des 4 portes disposera des dimensions suffisantes pour abriter l’ensemble de ces éléments. L’ensemble sera fourni avec des schémas électriques de raccordements détaillés. Les équipements seront certifiés et qualifiés ANSSI-CSPN (suivant les préconisations du poste 3.1 du présent programme).

Les fiches techniques des équipements détaillent les cartes, les équipements, ainsi que les éléments constitutifs de chaque coffret respectif (gestion : 2 portes ou 4 portes) en précisant les dimensions, la nature et le type d’enveloppe de chaque coffret respectif.

Chaque coffret UTL/UTP fourni par le fabricant titulaire du présent marché sera dûment repéré suivant les préconisations du poste 4.4.4. Le fabricant titulaire du présent marché fournira un tableur détaillant les informations suivantes (à fournir par le fabricant et à renseigner par les différents intervenants):

* + Le site : (à renseigner par l’entreprise intégratrice)
  + Le bâtiment : (à renseigner par l’entreprise intégratrice)
  + Le niveau du bâtiment : (à renseigner par l’entreprise intégratrice)
  + Le numéro de la pièce/ou du local : (à renseigner par l’entreprise intégratrice)
  + le numéro de prise RJ45 : (à renseigner par l’entreprise intégratrice)
  + le type d’équipement (à renseigner par le fabricant)
  + le numéro de l’UTL (à renseigner par l’entreprise intégratrice)
  + **l’adresse MAC de l’UTL (à renseigner de base par le fabricant)**
  + L’adresse IP fixe (à renseigner par le DSN et à préciser par l’entreprise)
  + Le masque (à renseigner par le DSN et à préciser par l’entreprise)
  + La passerelle réseau (à renseigner par le DSN et à préciser par l’entreprise)
  + Le DSN1 (à renseigner par le DSN et à préciser par l’entreprise)
  + Le DSN2 (à renseigner par le DSN et à préciser par l’entreprise)

**Ce tableau sera remis par le fabricant titulaire du présent marché en format informatique dématérialisé (Xlsx et en PDF) et en papier, lors de la remise des DOE par le fabricant et ne sera pas mis à l’intérieur du coffret UTL.**

### Autres cartes et équipements d’interfaçage et de gestion

#### Carte de gestion des lecteurs UHF existants

Des cartes électroniques de série : **CN-UTP-OSDP** de marque Synchronic ou techniquement équivalent permettant l’interfaçage avec les lecteurs UHF existants (de marque TAG-Master) sur les différents sites du CHU de Toulouse seront prévues et permettront la reprise de ces lecteurs longue distance UHF sur la nouvelle solution de contrôle d’accès de marque Synchronic ou techniquement équivalent.

#### Carte de gestion de SAS d’accès

Le système de contrôle d'accès devra permettre la gestion de SAS. L’effet de SAS devra être assuré sur plusieurs portes simultanément (l’ouverture d’une porte est possible que si toutes les autres sont fermées). Un minimum de 5 portes est demandé dans le cadre du présent marché. La commande d’ouverture de la porte pourra se faire suivant différentes configurations :

* + Lecteurs de Badge en entrée et sortie,
  + Lecteur de badge en entrée et bouton poussoir en sortie,
  + Boutons poussoirs en entrée et sortie.

L’effet de SAS sera assuré par l’ajout d’une carte CN-EXT-SAS ou techniquement équivalent sur chaque module de porte concerné. L’asservissement d’une porte par rapport à l’autre devra impérativement être garanti, même en cas de défaillance de l’UTL.

Pour chaque porte à effet de SAS il devra être possible de prendre en compte les informations suivantes :

* + Bouton d’appel en Entrée
  + Bouton d’appel en Sortie
  + Pilotage voyant vert
  + Pilotage voyant rouge

Outre l’asservissement entre les différentes portes, l’ouverture d’un accès pourra être conditionné à deux autre critères complémentaires :

* + La détection de présence dans le SAS,
  + L’unicité de présence dans le SAS.

Des cartes électroniques de série : **CN-EXT-SAS** de marque Synchronic ou techniquement équivalent permettant la création de fonctions de gestion de SAS seront prévues. Ces dernières seront pilotées depuis l’UTL et UTP précablées et seront mises en œuvre dans un seul coffret de protection et seront déployées au niveau des accès avec la fonction gestion de SAS.

#### Carte de gestion des ascenseurs

Le système de contrôle d'accès devra permettre la gestion d'ascenseurs (Prédestination des étages suivant le profil utilisateur) et être compatible aux ascensoristes (toutes marques d’ascenseurs) présents sur les différents sites du CHU de Toulouse avec un interfaçage direct entre l’UTL et l’automate ascenseur.

Des cartes électroniques permettant la gestion des ascenseurs seront prévues avec notamment :

* Carte de série :**CN-UTR-2R** de marque Synchronic ou techniquement équivalent : Carte interface entrées/sorties configurable : 8E/2S, 4E/6S,10S - 2 relais
* Carte de série : **CN-UI280-4R** de marque Synchronic ou techniquement équivalent  : Carte extension UTR-xx pour transformation de 4 sorties en tension en 4 sorties relais
* Carte relais d’alimentation et commande de verrouillage de série : **CN-REPLAY-P1** de marque Synchronic ou techniquement équivalent

#### Coffrets et autres accessoires des UTL et autres cartes électroniques :

Ces équipements pourront être équipés des accessoires et intégrés dans des coffrets, listés ci-dessous :

* Boitier vide pour intégration - 260x255x110mm - Type CAL06 avec autoprotection. Série : **29-BTVUG06** de marque Synchronic ou techniquement équivalent
* Boitier vide pour intégration - 420x320x175mm - Type CAL01 avec autoprotection. Série : **BTVUG01** de marque Synchronic ou techniquement équivalent
* Boitier vide pour intégration - 174x137x38mm – coffret ABS avec autoprotection. Série : **BTVU-P3** de marque Synchronic ou techniquement équivalent
* Boitier coffret métallique fermé à clé avec autoprotection-Dimensions du coffret : Grand coffret : **410 x 270 x 75 mm.**
* Mini rack pour intégration UTP et UTR (X8) - Bus RS485 et alimentation sur le fond de panier Série : **29-BTVRAC8UT3** de marque Synchronic ou techniquement équivalent
* Fiche de raccordements des cartes Série : **UI2804R** de marque Synchronic ou techniquement équivalent

### Lecteurs de badges

Les lecteurs de badges proposés seront de technologie Mifare/DESFire EV2-EV3, ils permettront la lecture des cartes/badges de professionnels de santé actuellement utilisés sur les différents sites du CHU de Toulouse mais également les futures cartes de professionnels de santé de type CPS3 et CPS4/CPE.

Ces derniers seront en lecteurs en mode « transparent » et seront qualifiés et certifiés ANSSI-CSPN.

Ils devront fonctionner en mode dit "Transparent" (le lecteur ne doit pas intervenir dans le chiffrement des données), de marque Synchronic ou techniquement équivalent. Ils seront gérés, programmés nativement et directement depuis l’applicatif de la solution de contrôle d’accès :**PC Pass, XT Manager, de Synchronic** ou techniquement équivalent.

Ils auront les caractéristiques minimales suivantes :

#### Lecteurs de badges sans contact transparent (format large)

* Fréquence 13.56MHZ
* Normes ISO 14443 types A
* Fonctionne avec les puces Mifare, Mifare DESFire EV2-EV3
* Fonctions : Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur)
* Interface : RS485
* Liaison RS485 haute sécurité avec l'UTP-SEC
* Distance de lecture : 0 - 6 cm
* Connectique Bornier débrochable : 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F -Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur sonore : Buzzer
* Consommation :130 mA/12 VDC typique
* Alimentation : 7 - 28 VDC
* Matériaux : ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
* **Dimensions : (h-l-p) : 107 x 80 x 26 mm**
* Températures de fonctionnement : - 20°C / + 70°C
* Fonction anti-arrachement : Détection arrachement par accéléromètre avec possibilité d’effacement des clefs (brevet déposé)
* Indice Protection / Résistance : IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK10
* Fixation : Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de support y compris sur métal sans spacer
* Certifications : CE

Série : **31-TPRDS-485** de marque Synchronic ou techniquement équivalent

#### Lecteurs de badges sans contact transparent (format étroit)

* Fréquence 13.56MHZ
* Normes ISO 14443 types A
* Fonctionne avec les puces Mifare, Mifare DESFire EV2-EV3
* Fonctions : Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur)
* Interface : RS485
* Liaison RS485 haute sécurité avec l'UTP-SEC
* Distance de lecture : 0 - 6 cm
* Connectique Bornier débrochable : 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F -Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur sonore : Buzzer
* Consommation :130 mA/12 VDC typique
* Alimentation : 9 – 15 VDC
* Matériaux : ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
* **Dimensions (h-l-p): 111.47x42.17x22mm**
* Températures de fonctionnement : - 20°C / + 70°C
* Fonction anti-arrachement : Détection arrachement par accéléromètre avec possibilité d’effacement des clefs (brevet déposé)
* Indice Protection / Résistance : IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK10
* Fixation : Murale en applique/sur pots électriques étroits (perçage 32 et 2 mm) Montage sur tout type de support y compris sur métal sans spacer
* Certifications : CE

Série : **31-TPRDSA1-485** de marque Synchronic ou techniquement équivalent

#### Lecteurs de badges doubles technologie sans contact avec digicode intégré de type transparent

* Fréquence 13.56MHZ
* Normes ISO 14443 types A
* Fonctionne avec les puces Mifare, Mifare DESFire EV2-EV3
* Fonctions : Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur)
* Interface : RS485
* Liaison RS485 haute sécurité avec l'UTP-SEC
* Distance de lecture : 0 - 6 cm
* Connectique Bornier débrochable : 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F -Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur sonore : Buzzer
* Consommation :130 mA/12 VDC typique
* Alimentation : 7 - 28 VDC
* Matériaux : ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
* **Dimensions : (h-l-p) : 107 x 80 x 26 mm**
* Températures de fonctionnement : - 20°C / + 70°C
* Fonction anti-arrachement : Détection arrachement par accéléromètre avec possibilité d’effacement des clefs (brevet déposé)
* Indice Protection / Résistance : IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK10
* Fixation : Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de support y compris sur métal sans spacer
* Certifications : CE

Série de type **31-TCLDS-485** de marque Synchronic ou techniquement équivalent

#### Lecteur de badge doubles technologie sans contact avec clavier tactile de type transparent

* Fréquence / Normes 13.56 MHz / ISO14443 A
* Puce : MIFARE® DESFire® EV1/EV2-EV3, MIFARE® DESFire®, MIFARE® Plus®, MIFARE® Classic, MIFARE® Ultralight®
* Fonctions :Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de
* configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur )
* Interface : RS485
* Distance de lecture : 0 - 6 cm
* Ecran :Écran tactile couleur - 2,8’’ - 240 x 320 pixels/Clavier 12 touches - Fonction clavier standard ou aléatoire (scramble pad)
* Connectique :Bornier débrochable 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur sonore : Buzzer intégré
* Consommation : 130 mA/12 VDC typique
* Alimentation : 7 - 28 VDC
* Matériaux : ABS-PC UL-V0 (noir)
* Dimensions (h x l x p) : 128 x 80 x 31 mm
* Températures de fonctionnement : - 10°C / + 50°C
* Fonction anti-arrachement :Détection arrachement par accéléromètre avec possibilité d’effacement des clefs :(brevet déposé)
* Indice Protection / Résistance :IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK08
* Fixation :Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de
* support y compris sur métal sans spacer
* Certifications : CE & FCC

Série de type **31-TCLDSE-485** de marque Synchronic ou techniquement équivalent

#### Lecteur de badge doubles technologie sans contact avec lecteur QR code de type transparent

* Fréquence : 13.56 MHz
* Normes : ISO14443 types A
* Puce :MIFARE® DESFire® EV1/EV2 et EV3, MIFARE® DESFire®, MIFARE® Plus®, MIFARE® Classic, MIFARE® Ultralight®
* Technologies de codes à barres : QR Code / Micro QR Code, Datamatrix,Aztec, Code 128
* Fonctions :Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de
* configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex:
* badge entreprise + badge blanc visiteur )
* Interface : RS485
* Distance de lecture : 0 - 6 cm / 3 cm minimum avec un QR code (selon la taille du code)
* Connectique : Bornier débrochable 10 points (5 mm) / Bornier débrochable 2 points (5 mm) : contact O/F -
* Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur : sonore Buzzer
* Consommation : 250 mA / 12 VDC typique
* Alimentation : 7 - 28 VDC
* Matériaux : ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
* Dimensions (h x l x p) : 160 x 80 x 25.70 mm
* Températures de fonctionnement : - 30°C à + 60°C / Humidité : 5 - 90%
* Fonction anti-arrachement Détection arrachement par accéléromètre avec possibilité d’effacement des clefs (brevet déposé)
* Indice Protection / Résistance : Niveau IP65 hors connectique - Résistant aux intempéries, à l’eau et aux poussières (certification CEI NF EN 61086) - Structure renforcée anti-vandale
* Fixation : Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de support y compris sur métal sans spacer
* Certifications : CE

Série de type **31-TPRDSQR-485** de marque Synchronic ou techniquement équivalent

#### Lecteur de badge doubles technologie sans contact avec lecteur biométrique de type transparent

Le système de contrôle d'accès devra permettre la mise en place d'une solution d'identification via biométrie. Cette solution devra respecter les directives de la CNIL.

* La mise en place d'un système de contrôle d’accès doit se faire en accord avec le CODE DU TRAVAIL.
* La Direction doit donc informer de son intention et demander l'avis des instances représentatives du personnel notamment le Comité d’Entreprise et le Comité d'Hygiène, de Sécurité et des Conditions du travail (CHSCT).
* La mise en place d'un système de contrôle d’accès doit aussi respecter la loi "INFORMATIQUE ET LIBERTÉ".
* La loi du 6 Janvier 1978, stipule que toute entreprise qui met en place puis gère un fichier informatisé de données nominatives est tenue de le déclarer.
* Les données personnelles recueillies doivent être accessibles par l’individu qui conserve un droit de modification sur celles-ci.
* La Direction doit donc obtenir l'accord de la Commission Nationale Informatique et Liberté (CNIL).
* De plus, la mise en place d'un contrôle d’accès ne doit pas faire obstacle au bon fonctionnement des issues de secours et d'une façon plus générale à la sécurité des personnes. Il sera donc nécessaire de tenir compte des préconisations des commissions de sécurité ou pompiers (Asservissements liés au SSI (Système de Sécurité Incendie)).
* Caractéristiques techniques minimales :
  + Fréquence / Normes :13.56 MHz / ISO14443 A
  + Puce :MIFARE® DESFire® EV1/EV2 et EV3, MIFARE® DESFire®, MIFARE® Plus®, MIFARE® Classic, MIFARE® Ultralight®
  + Fonctions :Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur ) + Empreintes digitales
  + Identification biométrique :Optique (SAGEM MorphoSmart™) / Durée d’identification ≤ 1 seconde pour une authentification 1:1 / Zone de reconnaissance 14 x 22 mm
  + Interface :RS485
  + Distance de lecture :0 - 6 cm
  + Connectique :Bornier débrochable 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F-indicateur d’état d’arrachement
  + Indicateur lumineux :2 LEDs RVB - 360 couleurs
  + Indicateur sonore :Buzzer intégré
  + Consommation :100 mA/12 VDC typique
  + Alimentation :7 - 28 VDC
  + Matériaux :ABS-PC UL-V0 (noir)
  + Dimensions (h x l x p) :167 x 80 x 62 mm
  + Températures de fonctionnement :- 10°C / + 50°C
  + Fonction anti-arrachement :Détection arrachement par accéléromètre avec possibilité d’effacement des clefs (brevet déposé)
  + Indice Protection / Résistance :IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK10
  + Fixation :Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de support y compris sur métal sans spacer
  + Certifications :CE & FCC

Série de type **31-TBIO-485** de marque Synchronic ou techniquement équivalent

#### Lecteur de badge doubles technologie sans contact avec lecteur biométrique et afficheur, de type transparent :

Le système de contrôle d'accès devra permettre la mise en place d'une solution d'identification via biométrie. Cette solution devra respecter les directives de la CNIL.

* La mise en place d'un système de contrôle d’accès doit se faire en accord avec le CODE DU TRAVAIL.
* La Direction doit donc informer de son intention et demander l'avis des instances représentatives du personnel notamment le Comité d’Entreprise et le Comité d'Hygiène, de Sécurité et des Conditions du travail (CHSCT).
* La mise en place d'un système de contrôle d’accès doit aussi respecter la loi "INFORMATIQUE ET LIBERTÉ".
* La loi du 6 Janvier 1978, stipule que toute entreprise qui met en place puis gère un fichier informatisé de données nominatives est tenue de le déclarer.
* Les données personnelles recueillies doivent être accessibles par l’individu qui conserve un droit de modification sur celles-ci.
* La Direction doit donc obtenir l'accord de la Commission Nationale Informatique et Liberté (CNIL).
* De plus, la mise en place d'un contrôle d’accès ne doit pas faire obstacle au bon fonctionnement des issues de secours et d'une façon plus générale à la sécurité des personnes. Il sera donc nécessaire de tenir compte des préconisations des commissions de sécurité ou pompiers (Asservissements liés au SSI (Système de Sécurité Incendie)).
* Caractéristiques techniques minimales :
  + Fréquences porteuses / Normes : 13,56 MHz. ISO14443 type A
  + Puces : MIFARE® Classic & Classic EV1, MIFARE Plus® & Plus® EV1, MIFARE® DESFire® 256, EV1 & EV2 et EV3
  + Fonctions: Lecture seule sécurisée (fichier, secteur) et protocole sécurisé (Secure Plus) / Lecture écriture sécurisée
  + Capteur d’empreintes digitales : Optique (SAFRAN MorphoSmart™ CBM E3) - ≤ 1 seconde pour une authentification 1:1
  + Interfaces et protocoles de communication :Sortie TTL Data Clock (ISO2) ou Wiegand (option chiffrée - S31) / Sortie RS232 (option chiffrée - S32) / Sortie RS485 (option chiffrée - S33)avec protocoles de communication sécurisés SSCP et SSCP2 ; OSDP™ V1 (communication en clair) et V2 (communication sécurisée SCP)
  + Comptabilité décodeurs : Compatible avec l’interface EasySecure
  + Ecran : Ecran tactile couleur - 2,8’’ - 240 x 320 pixels / Clavier 12 touches - Fonction clavier standard ou aléatoire (scramble pad)Modes : Badge ET Touche / Badge OU Touche Configurable par badge RFID, technologie UHF ou logiciel selon interface
  + Distances de lecture : Jusqu’à 4 cm avec un badge MIFARE® DESFire® EV2 ou Classic
  + Indicateur lumineux :2 LEDs RVB - 360 couleurs configurable par badge RFID, technologie UHF, logiciel ou piloté par commande externe (0V) selon interface
  + Indicateur sonore : Buzzer intégré, configurable par badge RFID, technologie UHF, logiciel ou piloté par commande externe (0V) selon interface
  + Consommation : 350 mA / 12 VDC typique
  + Alimentation :7 VDC à 28 VDC
  + Connectique : Bornier débrochable 10 points (5 mm) / Bornier débrochable 2 points (5 mm) : contact O/F - Indicateur d’état d’arrachement ou de lecture d’un identifiant
  + Matériaux : ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
  + Dimensions : (h x l x p) 166,2x 80 x 30,2/71 mm (tolérance générale suivant standard ISO NFT 58-000)
  + Températures de fonctionnement : - 10°C à + 50°C / Humidité : 0 - 95%
  + Fonction anti-arrachement : Détection arrachement par accéléromètre avec possibilité d’effacement des clés (solution brevetée)
  + Protection Niveau : IP65 - Résistant aux intempéries, à l’eau et aux poussières (certification CEI NF EN 61086)
  + Fixation Montage sur tout type de support y compris sur métal sans spacer - Murale en applique / sur pots électriques :Européen 60 & 62 mm
  + Certifications : CE, FCC et UL

Série de type **31-TBIOE-485** de marque Synchronic ou techniquement équivalent

#### Lecteurs de badges sans contact transparent-Bluetooth (format large)

* Fréquence 13.56MHZ
* Normes ISO 14443 types A
* Fonctionne avec les puces Mifare, Mifare DESFire EV2-EV3
* Fonctions : Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur)-**Intègre le mode Bluetooth**
* Interface : RS485
* Liaison RS485 haute sécurité avec l'UTP-SEC
* Distance de lecture : 0 - 6 cm
* Connectique Bornier débrochable : 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F -Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur sonore : Buzzer
* Consommation :130 mA/12 VDC typique
* Alimentation : 7 - 28 VDC
* Matériaux : ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
* **Dimensions : (h-l-p) : 107 x 80 x 26 mm**
* Températures de fonctionnement : - 20°C / + 70°C
* Fonction anti-arrachement : Détection arrachement par accéléromètre avec possibilité d’effacement des clefs (brevet déposé)
* Indice Protection / Résistance : IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK10
* Fixation : Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de support y compris sur métal sans spacer
* Certifications : CE

Série : **31-TPRDS-BL-485** de marque Synchronic ou techniquement équivalent

#### Lecteurs de badges sans contact transparent-Bluetooth (format étroit)

* Fréquence 13.56MHZ
* Normes ISO 14443 types A
* Fonctionne avec les puces Mifare, Mifare DESFire EV2-EV3
* Fonctions : Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur) -**Intègre le mode Bluetooth**
* Interface : RS485
* Liaison RS485 haute sécurité avec l'UTP-SEC
* Distance de lecture : 0 - 6 cm
* Connectique Bornier débrochable : 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F -Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur sonore : Buzzer
* Consommation :130 mA/12 VDC typique
* Alimentation : 9 – 15 VDC
* Matériaux : ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
* **Dimensions (h-l-p): 111.47x42.17x22mm**
* Températures de fonctionnement : - 20°C / + 70°C
* Fonction anti-arrachement : Détection arrachement par accéléromètre avec possibilité d’effacement des clefs (brevet déposé)
* Indice Protection / Résistance : IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK10
* Fixation : Murale en applique/sur pots électriques étroits (perçage 32 et 2 mm) Montage sur tout type de support y compris sur métal sans spacer
* Certifications : CE

Série : **31-TPRDSA1-BL-485** de marque Synchronic ou techniquement équivalent

#### Lecteurs de badges doubles technologie sans contact avec digicode intégré de type transparent- Bluetooth

* Fréquence 13.56MHZ
* Normes ISO 14443 types A
* Fonctionne avec les puces Mifare, Mifare DESFire EV2-EV3
* Fonctions : Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur) -**Intègre le mode Bluetooth**
* Interface : RS485
* Liaison RS485 haute sécurité avec l'UTP-SEC
* Distance de lecture : 0 - 6 cm
* Connectique Bornier débrochable : 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F -Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur sonore : Buzzer
* Consommation :130 mA/12 VDC typique
* Alimentation : 7 - 28 VDC
* Matériaux : ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
* **Dimensions : (h-l-p) : 107 x 80 x 26 mm**
* Températures de fonctionnement : - 20°C / + 70°C
* Fonction anti-arrachement : Détection arrachement par accéléromètre avec possibilité d’effacement des clefs (brevet déposé)
* Indice Protection / Résistance : IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK10
* Fixation : Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de support y compris sur métal sans spacer
* Certifications : CE

Série de type **31-TCLDS-BL-485** de marque Synchronic ou techniquement équivalent

#### Lecteur de badge doubles technologie sans contact avec clavier tactile de type transparent-Bluetooth

* Fréquence / Normes 13.56 MHz / ISO14443 A
* Puce : MIFARE® DESFire® EV1/EV2-EV3, MIFARE® DESFire®, MIFARE® Plus®, MIFARE® Classic, MIFARE® Ultralight®
* Fonctions :Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de
* configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex: badge entreprise + badge blanc visiteur )- **Intègre le mode Bluetooth**
* Interface : RS485
* Distance de lecture : 0 - 6 cm
* Ecran :Écran tactile couleur - 2,8’’ - 240 x 320 pixels/Clavier 12 touches - Fonction clavier standard ou aléatoire (scramble pad)
* Connectique :Bornier débrochable 10 points (5mm) Bornier débrochable 2 points (5mm) : contact O/F Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur sonore : Buzzer intégré
* Consommation : 130 mA/12 VDC typique
* Alimentation : 7 - 28 VDC
* Matériaux : ABS-PC UL-V0 (noir)
* Dimensions (h x l x p) : 128 x 80 x 31 mm
* Températures de fonctionnement : - 10°C / + 50°C
* Fonction anti-arrachement :Détection arrachement par accéléromètre avec possibilité d’effacement des clefs :(brevet déposé)
* Indice Protection / Résistance :IP65 hors connectique et carte électronique tropicalisée / Structure renforcée anti-vandale IK08
* Fixation :Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de
* support y compris sur métal sans spacer
* Certifications : CE & FCC

Série de type **31-TCLDSE-BL-485** de marque Synchronic ou techniquement équivalent

#### Lecteur de badge doubles technologie sans contact avec lecteur QR code de type transparent-Bluetooth

* Fréquence : 13.56 MHz
* Normes : ISO14443 types A
* Puce :MIFARE® DESFire® EV1/EV2 et EV3, MIFARE® DESFire®, MIFARE® Plus®, MIFARE® Classic, MIFARE® Ultralight®
* Technologies de codes à barres : QR Code / Micro QR Code, Datamatrix,Aztec, Code 128
* Fonctions :Lecture numéro de série et/ou sécurisée : Gestion de clés centralisée (aucun badge de
* configuration), le lecteur supporte simultanément 2 configurations DESFire différentes (ex:
* badge entreprise + badge blanc visiteur )- **Intègre le mode Bluetooth**
* Interface : RS485
* Distance de lecture : 0 - 6 cm / 3 cm minimum avec un QR code (selon la taille du code)
* Connectique : Bornier débrochable 10 points (5 mm) / Bornier débrochable 2 points (5 mm) : contact O/F -
* Indicateur d’état d’arrachement
* Indicateur lumineux : 2 LEDs RVB - 360 couleurs
* Indicateur : sonore Buzzer
* Consommation : 250 mA / 12 VDC typique
* Alimentation : 7 - 28 VDC
* Matériaux : ABS-PC UL-V0 (noir) / ASA-PC-UL-V0 UV (blanc)
* Dimensions (h x l x p) : 160 x 80 x 25.70 mm
* Températures de fonctionnement : - 30°C à + 60°C / Humidité : 5 - 90%
* Fonction anti-arrachement Détection arrachement par accéléromètre avec possibilité d’effacement des clefs (brevet déposé)
* Indice Protection / Résistance : Niveau IP65 hors connectique - Résistant aux intempéries, à l’eau et aux poussières (certification CEI NF EN 61086) - Structure renforcée anti-vandale
* Fixation : Murale en applique/sur pots électriques (entre-axes 60 et 62 mm) Montage sur tout type de support y compris sur métal sans spacer
* Certifications : CE

Série de type **31-TPRDSQR-BL-485** de marque Synchronic ou techniquement équivalent

#### Accessoires des lecteurs de badges

Ces électeurs de badges pourront être équipés des accessoires listés, ci-dessous :

* Bouclier équipé pour lecteur standard Architect® & Architect® Blue - Joint adhésif + vis inviolables. Série :**31-SHIELD-ARC** de marque Synchronic ou techniquement équivalent
* Bouclier équipé pour lecteur étroit Architect® One & Architect® One Blue - Joint adhésif + vis inviolables. Série :**31-SHIELD-ARC1** de marque Synchronic ou techniquement équivalent
* Casquette de protection environnements extrêmes Architect. Série : **31-COVER-ARC** de marque Synchronic ou techniquement équivalent

### Lecteurs de badges UHF longue distance

Les lecteurs de badges proposés seront de technologie UHF, ils permettront la lecture des cartes UHF, les TAG et Télé-TAG UHF ainsi que les étiquettes pare-brise UHF de marque « TAG Master » actuellement utilisées sur les différents sites du CHU de Toulouse mais également les futurs équipements détaillés ci-dessous, de la nouvelle solution de contrôle d’accès à prévoir dans le cadre du présent marché.

Ces derniers devront être compatibles et fonctionnels avec la solution de contrôle d’accès proposée dans le cadre du présent marché. Ils seront gérés, programmés directement et nativement depuis les applicatifs de la solution de contrôle d’accès **PC Pass, XT Manager, de Synchronic** ou techniquement équivalent.

#### Lecteur de badge longue distance UHF 868 MHz (lecteur spectre 7AB-RS485)

* Fréquences: UHF
* Gabarit et/ou dimensions: (l x h x p)348,7 x 279,2 x 45,1 mm (Spectre)
* Boitier: Gris/Antenne Noire
* Température de stockage min/max: -25°C à + 60°C
* Température de fonctionnement min/max: -25°C à + 60°C
* Tension et consommation utiles: 12 Vdc 1,5 A (2 A max) (Spectre)
* Puissance nominale en Watt : 15 W
* Indice IP : IP 66
* Normes : ISO18000-63 / EPC1 Gen 2 - 2 versions : bande

basse 865 - 868 MHz / bande haute 902 - 928 MHz/ Certifications : CE, ETSI, FCC Part 15

* Distance de lecture : de 14m à 20m suivant le type et la nature du badge UHF

Série de type **31-TMU-ST4-RS** de marque Synchronic ou techniquement équivalent

#### Lecteur de badge longue distance UHF 868 MHz (lecteur spectre Nano 7AB-RS485)

* Fréquences: UHF
* Gabarit et/ou dimensions: (l x h x p)185x230x35 mm (Spectre Nano)
* Boitier: Gris/Antenne Noire
* Température de stockage min/max: -25°C à + 60°C
* Température de fonctionnement min/max: -25°C à + 60°C
* Tension et consommation utiles: 12 Vdc 0.9A (Spectre Nano)
* Puissance nominale en Watt : 15 W
* Indice IP : IP 66
* Normes : ISO18000-63 / EPC1 Gen 2 - 2 versions : bande

basse 865 - 868 MHz / bande haute 902 - 928 MHz/ Certifications : CE, ETSI, FCC Part 15

* Distance de lecture : de 6m à 20m suivant le type et la nature du badge UHF

Série de type **31-TMU-ST5-RS** de marque Synchronic ou techniquement équivalent

#### Lecteur de badge longue distance UHF 868 MHz (lecteur spectre en Clock&Data -Configurable en Wiegand)

* Fréquences: UHF
* Gabarit et/ou dimensions: (l x h x p)348,7 x 279,2 x 45,1 mm (Spectre)
* Boitier: Gris/Antenne Noire
* Température de stockage min/max: -25°C à + 60°C
* Température de fonctionnement min/max: -25°C à + 60°C
* Tension et consommation utiles: 12 Vdc 1,5 A (2 A max) (Spectre)
* Puissance nominale en Watt : 15 W
* Indice IP : IP 66
* Normes : ISO18000-63 / EPC1 Gen 2 - 2 versions : bande

basse 865 - 868 MHz / bande haute 902 - 928 MHz/ Certifications : CE, ETSI, FCC Part 15

Série de type **31-TMU-ST4** de marque Synchronic ou techniquement équivalent

#### Lecteur de badge longue distance UHF 868 MHz (lecteur spectre Nano en Clock&Data -Configurable en Wiegand)

* Fréquences: UHF
* Gabarit et/ou dimensions: (l x h x p)185x230x35 mm (Spectre Nano)
* Boitier: Gris/Antenne Noire
* Température de stockage min/max: -25°C à + 60°C
* Température de fonctionnement min/max: -25°C à + 60°C
* Tension et consommation utiles: 12 Vdc 0.9A (Spectre Nano)
* Puissance nominale en Watt : 15 W
* Indice IP : IP 66
* Normes : ISO18000-63 / EPC1 Gen 2 - 2 versions : bande

basse 865 - 868 MHz / bande haute 902 - 928 MHz/ Certifications : CE, ETSI, FCC Part 15

Série de type **31-TMU-ST5** de marque Synchronic ou techniquement équivalent

#### Accessoires des lecteurs de badges

Ces électeurs de badges pourront être équipés des accessoires, listés ci-dessous :

* Kit de fixation sur mur pour lecteur UHF. Série : **31-TMU-STKIT08** de marque Synchronic ou techniquement équivalent
* Kit de fixation sur mât pour lecteur UHF. Série : **31-TMU-STKIT09** de marque Synchronic ou techniquement équivalent

### Lecteurs de plaques d’immatriculation

Les lecteurs de plaque d’immatriculation seront compatibles et fonctionnels avec la nouvelle solution de contrôle d’accès certifiée et qualifiée ANSSI, ces derniers seront gérés, programmés et pilotés nativement depuis les applicatifs de la solution de contrôle d’accès **PCPass, XT Manager, de Synchronic** ou techniquement équivalent. Les logiciels natifs des fabricants de ces produits seront également fournis avec ces équipements

#### Lecteur de plaques d’immatriculation (2m à 6m):

* Versions produit / logiciel / firmware :FirmwareMicropak3Update-1.1.1.0-Build4519-Platform2.01
* Gabarit et/ou dimensions avec casquette :L : 1750 mm x l : 950 mm x H : 1550 mm
* Poids :1640 grammes
* Couleurs et / ou design et / ou matière :Boitier Aluminium gris
* Température de stockage/fonctionnement min / max :- 40°C à + 55°C
* Tensions utiles :24 Vdc
* Puissance en Watt :12 W
* Caractéristiques vidéo :
  + Caméra HD : 1,3 Mégapixels Analyse d’image : 60 images/seconde
  + Portée : 2m à 6m
  + Eclairage : IR 850nm ; Compression : H264
  + Réglages : Bitrate, fréquence, cadrage dynamique
  + Vitesse maximale 250km/h
* Indice IP :IP 67
* Normes :CEM EN 55032, sécurité photobiologique IEC62471, Marquage CE, FCC Part 15, CB Scheme, CEI 61 000 - 4, RoHs
* Références associées :CN-UTP-TLPV ; VSS7Setup-7.6.8.x-Buildxxx

Série de type **31-TLPV-06-RS** de marque Synchronic ou techniquement équivalent

#### Lecteur de plaques d’immatriculation (4m à 15m):

* Versions produit / logiciel / firmware :FirmwareMicropak3Update-1.1.1.0-Build4519-Platform2.01
* Gabarit et/ou dimensions avec casquette :L : 1750 mm x l : 950 mm x H : 1550 mm
* Poids :1640 grammes
* Couleurs et / ou design et / ou matière :Boitier Aluminium gris
* Température de stockage/fonctionnement min / max :- 40°C à + 55°C
* Tensions utiles :24 Vdc
* Puissance en Watt :12 W
* Caractéristiques vidéo :
* Caméra HD : 1,3 Mégapixels Analyse d’image : 60 images/seconde
  + Eclairage : IR 850nm ; Compression : H264
  + Portée : 4m à 15m
  + Réglages : Bitrate, fréquence, cadrage dynamique
  + Vitesse maximale 250km/h
* Indice IP :IP 67
* Normes :CEM EN 55032, sécurité photobiologique IEC62471, Marquage CE, FCC Part 15, CB Scheme, CEI 61 000 - 4, RoHs
* Références associées :CN-UTP-TLPV ; VSS7Setup-7.6.8.x-Buildxxx

Série de type **31-TLPV-15-RS** de marque **Synchronic** ou techniquement équivalent

#### Accessoires des lecteurs de plaques d’immatriculation

Ces lecteurs de plaques d’immatriculation pourront être équipés des accessoires, listés ci-dessous :

* Kit de fixation sur mur pour lecteur de plaque d’immatriculation. Série : **31-TLP-BRAS** de marque Synchronic ou techniquement équivalent
* Adaptateur montage sur mât pour lecteur de plaque d’immatriculation. Série **31-TLP-MAT** de marque Synchronic ou techniquement équivalent
* Logiciel de programmation des lecteurs des plaques d’immatriculation
* Le logiciel de programmation des plaques d’immatriculation devra être nativement intégré au logiciel de control d’accès : **PCPass, XT manager** **de Synchronic** ou techniquement équivalent

### Lecteurs de badges sans fils et serrures autonomes

Il sera prévu des lecteurs de la gamme **Aperio® de ASSA Abloy** ou techniquement équivalent, cylindres et/ou béquilles sans fil, selon les accès. Cette technologie devra être nativement intégrée dans les équipements et directement gérée par le logiciel de gestion de contrôle d'accès, type **PC Pass de Synchronic ou techniquement équivalent.** Les logiciels natifs de ces produits seront également fournis avec ces équipements

L'intégration de la solution devra impérativement respecter les prérequis suivants :

* Le lecteur devra communiquer en temps réel via une liaison sans fil dans un rayon de 5/25 mètres et suivant la norme IEEE 802.15.4 vers son hub. Pour optimiser le coût de l’installation et simplifier l’architecture, ce hub devra être capable de communiquer avec plusieurs lecteurs sans fil (jusqu’à 5 lecteurs).
* Afin d’assurer une maintenance efficace sur les portes équipées de lecteurs de contrôle d’accès sans fil, les événements suivants devront être pilotés en temps réel :
  + niveau batterie,
  + perte de la liaison sans fil entre le hub et le lecteur,
  + lecteur absent (ou endommagé),
  + problème de communication entre le contrôleur de porte et le hub de communication.
* Les hubs radio seront raccordés sur un bus de communication non-dédié.
* UTP et Hubs radio devront cohabiter sur un même bus RS485.
* Il sera prévu dans la gamme du fabricant la gestion Offline via le Protocol OSS ou techniquement équivalent
* …

#### Ensemble de plaques béquilles électroniques

* Les ensembles proposés doivent pouvoir être installés sur différents types de portes et seront compatibles avec l’utilisation traditionnelle d’un cylindre de serrure européen et l’ensemble des cylindres et serrures existants dans les différents bâtiments de l’ensemble des sites du CHU de Toulouse.
* 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 portes ;
* Béquille extérieure libre : elle s’enclenche pour actionner la serrure lorsque l’autorisation d’ouverture est donnée par le contrôle d’accès.
* LED de signalisation sur la plaque extérieure :
  + Vert : accès autorisé
  + Rouge : accès refusé
  + Clignotement rouge : signale une défaillance.
* Béquille intérieure toujours active : sortie libre.
* Système d’alerte batteries faibles ;
* Têtes de lecture RFID, NFC et Bluetooth équipées de signalisation couleur (accès autorisé, accès refusé au minimum),
* 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 événements 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.

Ci-dessous sont détaillées les références des équipements :

* Série :**A1-BQB1-S/Béquille Aperio®** ou techniquement équivalent - **Porte standard de 40 à 50mm**–Autre taille prévoir **A1-BQ-EXT-B10** ou techniquement équivalent
* Série : **A1-BQP1-S/Béquille** **Aperio**® Premium ou techniquement équivalent - **Porte standard de 40 à 50mm** - Carré de 9mm - Autre taille prévoir **A1-BQ-EXT-B10** ou techniquement équivalent
* Série : **A1-BQB1-C/Béquille Aperio® + Clavier** ou techniquement équivalent - **Porte standard de 40 à 50mm** - Autre taille prévoir **A1-BQ-EXT-B10** ou techniquement équivalent.
* Série :**A1-POB1-XX/Poignée Aperio® 1 lecteur** - carré de 7/8mm ou techniquement équivalent **- Pour porte de 35 à 80mm**
* Série :**A1-PO-ROSACE/Aperio® H100** Rosaces cylindre européen (par ensemble de deux) ou techniquement équivalent.
* Série :**A1-KS100/Fermeture Aperio KS100** ou techniquement équivalent **pour baie informatique**
* Série **A1-KL100-Serrure Aperio KL100** ou techniquement équivalent **pour casiers et armoires** - Diamètre 19 ou 22 mm selon référence
* …

**La liste ci-dessus n’est pas exhaustive, les autres références des serrures électroniques (béquilles) seront prévues dans le cadre du présent marché et seront détaillées suivant les préconisations du paragraphe 4.3.13 du présent programme.**

#### Cylindres électroniques

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 plaques béquilles. Le processus d'identification est confirmé par une information visuelle du cylindre électronique. Aucun câblage n'est nécessaire sur la porte.

* Les ensembles proposés doivent pouvoir être installés sur différents types de portes et seront compatibles avec l’utilisation traditionnelle d’un cylindre de serrure européen et l’ensemble des cylindres et serrures existants dans les différents bâtiments de l’ensemble des sites du CHU de Toulouse.
* Cylindre composé d’un corps central et de deux boutons de manœuvre :
  + Bouton extérieur libre : il s’enclenche pour actionner la serrure lorsque l’autorisation d’ouverture est donnée par le contrôle d’accès.
  + LED de signalisation sur le bouton extérieur sur le même principe que la béquille.
  + Bouton intérieur toujours actif : sortie libre.
* Ensemble des composants électroniques sensibles dans le corps du cylindre
* Pile positionnée dans la tête de lecteur remplaçable à l’aide d’un outil spécifique.
* Alerte batterie.
* Têtes de lecture RFID, NFC et Bluetooth équipées de signalisation couleur (accès autorisé, accès refusé au minimum) ;
* Indice IPxx suffisant pour un montage en extérieur ;
* Communication en temps réel permettant les ouvertures à distance, la remontée des événements et la mise à jour des badges ;
* En cas de défaillance : sauvegarde des derniers événements ayant lieu hors liaison (badges validés, badges refusés, défaut liaison sans fil).

Ci-dessous sont détaillées les références des équipements :

* Série :**A1-CYB0-I/Demi-Cylindre Aperio®** ou techniquement équivalent- **Porte 30x0** - Autres tailles prévoir **A1-CY-EXT-B05 ou techniquement équivalent**
* **A1-CYB1-I/Cylindre Aperio® 1 lecteur** ou techniquement équivalent- **Porte 30x30** - Autres tailles prévoir **A1-CY-EXT-B05** ou techniquement équivalent
* **A1-CYB2-I/Cylindre Aperio® 2 lecteurs** - **Porte 30x30** Autres tailles prévoir **A1-CY-EXT-B05** ou techniquement équivalent
* Rallonges des : demi-cylindre, cylindre, cylindre double, **par pas de 5 mm** de série : **Aperio®, de marque ASSA ABLOY** ou techniquement équivalent
* …

**La liste ci-dessus n’est pas exhaustive, les autres références des serrures électroniques (cylindres) seront prévues dans le cadre du présent marché et seront détaillées suivant les préconisations du paragraphe 4.3.13 du présent programme.**

#### Accessoires et autres équipements

Il sera prévu avec l’ensemble de ces équipements l’ensemble des accessoires et outils nécessaires pour le bon fonctionnement des installations de contrôle d’accès par serrures électroniques (cylindres, béquilles) et notamment :

* Hub radio pour 5 cylindres ou béquilles Distance max 20m. Série : **A1-HUB5**, **marque Aperio®** ou techniquement équivalent
* Antenne externe pour hub 5 : Série :**A1-ANT, marque APERIO** ou techniquement équivalent
* Logiciel de programmation des Béquilles/Cylindres de **marque APERIO ,** série : **A1-PAP ou** techniquement équivalent
* Le logiciel de programmation des béquilles et cylindres devra être nativement intégré au logiciel de control d’accès **PCPass, XT manager** **de Synchronic** ou techniquement équivalent
* …

**La liste ci-dessus n’est pas exhaustive, les autres références des accessoires des serrures électroniques (béquilles et cylindres) seront prévues dans le cadre du présent marché et seront détaillées suivant les préconisations du paragraphe 4.3.13 du présent programme.**

### Serrures et clés mécatroniques :

Il sera prévu des éléments de verrouillage mécatronique de marque **ASSA ABLOY Protec2 CLIQ ou** techniquement équivalent. Cette technologie devra être nativement intégrée dans les équipements et directement gérée par le logiciel de gestion de contrôle d'accès, type :**PCPass, XT manager de Synchronic**, ou techniquement équivalent**.** Les logiciels natifs de ces produits seront également fournis avec ces équipements

L'intégration de la solution devra impérativement respecter les prérequis suivants :

#### Cylindres programmables

* Cylindre à disques
* La communication entre les clés et les cylindres sera effectuée par contact électrique. La technologie à induction est à proscrire pour éviter les perturbations magnétiques.
* Pour faciliter l’installation et la maintenance, le fonctionnement des éléments de verrouillage ne nécessitera aucun câblage ou pile au niveau de la porte.
* Pour supprimer tout risque lié aux clés perdues pendant toute la durée de vie du système, il sera possible d’interdire au moins 3 000 clés dans chaque cylindre.
* Le cylindre électronique pourra contenir au minimum les 2 000 derniers événements pour assurer la traçabilité des accès et des tentatives d’accès.
* Pour les accès les plus sensibles, certains cylindres pourront être programmés de façon à ce que le déverrouillage du cylindre nécessite l’insertion de deux clés autorisées dans le cylindre.
* Pour s’adapter aux environnements d’installation, la plage de température de fonctionnement des cylindres devra couvrir de - 40°C à + 70°C
* Les identifiants seront à double sécurité, mécanique et électronique. Ils seront de **marque ABLOY** **Protec² (cylindres programmables) et ABLOY Protec² CLIQ (clés programmables)** ou techniquement équivalent.

**Les variures des cylindres des clés mécatroniques seront à définir au moment de la commande. Elles seront définies en fonction : des sites, des bâtiments, des locaux et des zones à contrôler (type d’activité ou par corps de métier par exemple pour les locaux techniques :CVC, ELEC, VDI…)**

Ci-dessous sont détaillées les références des équipements :

* Demi-cylindres, série : **ABLOY PROTECT² CLIQ, référence :** **CYL331T128060** ou techniquement équivalent
* Cylindre à bouton, série : **ABLOY PROTECT² CLIQ, référence :** **CYL333T128060** ou techniquement équivalent
* Cylindre double, série : **ABLOY PROTECT² CLIQ, référence :** **CYL332T128060** ou techniquement équivalent
* Cylindre double électronique série : **ABLOY PROTECT² CLIQ, référence :** **CYL342T128060** ou techniquement équivalent
* Cylindre double pour usage extérieur série : **ABLOY PROTECT² CLIQ, référence :** **CYLP322T128060** ou techniquement équivalent
* Rallongement de cylindre par tranche de 5mm série : **ABLOY PROTECT² CLIQ, référence :** SA00008 ou techniquement équivalent
* Adaptation Deny Cylindre **PROTEC CLIQ** adaptable à embase ordinaire usage extérieur L56, **référence :** **CYLP843T128060** ou techniquement équivalent
* Adaptation Deny Cylindre **PROTEC CLIQ** adaptable à embase ordinaire usage extérieur L51, **référence :** **CYLP844T126060** ou techniquement équivalent
* Cache entrée cylindre PE, Capot de protection cylindre PE pour utilisation en extérieur protégé série : **ABLOY PROTECT² CLIQ, référence :** **CH103900000** ou techniquement équivalent
* Serrure batteuse, série : **ABLOY PROTECT² CLIQ, référence :CLL130T128060** ou techniquement équivalent
* Serrure batteuse profil européen, série : **ABLOY PROTECT² CLIQ, référence :** **CLL715T128060** ou techniquement équivalent
* …

**La liste ci-dessus n’est pas exhaustive, les autres références des cylindres mécatroniques seront prévues dans le cadre du présent marché et seront détaillées suivant les préconisations du paragraphe 4.3.13 du présent programme.**

#### Clés programmables

Pour des raisons de sécurité, le titulaire du marché garantira la mise à disposition d’une variure mécanique spécifique. Pour s’assurer qu’aucun autre client n’aura jamais de produits mécaniquement identiques, le système mécanique fourni disposera d’une puissance combinatoire de l’ordre d’un milliard de combinaisons possibles.

L’administrateur du système pourra programmer les clés localement, depuis le logiciel de contrôle d’accès, via un boitier de programmation local banché en USB sur son ordinateur.

La solution doit permettre la programmation des clés à distance, c’est-à-dire que l’administrateur n’aura pas à récupérer les clés des agents pour les programmer.

La mise à jour des clés utilisateurs consistera à modifier les autorisations d’accès aux cylindres, les paramètres de validité et les plannings hebdomadaires le cas échéant, à revalider les droits pour la durée configurée. Pour les clés de programmation, il s’agira de leur assigner des tâches de programmation pour les cylindres, comme la récupération d’historique ou l’ajout d’une clé à la liste noire. Les événements contenus dans la clé seront transmis à l’occasion de la mise à jour des clés.

Pour faire face à un environnement réseau perturbé, le système devra permettre la revalidation des droits en offline.

Le fabricant titulaire du présent lot prévoira :

* Une clé de programmation par administrateur de site et par site
* Une superclé de programmation par administrateur de site et par site

**Les variures des clés mécatroniques seront à définir au moment de la commande. Elles seront définies en fonction : des sites, des bâtiments, des locaux et des zones à contrôler (type d’activité ou par corps de métier par exemple pour les locaux techniques :CVC, ELEC, VDI…)**

**Caractéristiques techniques minimales :**

Les clés **PROTEC² CLIQ ou techniquement équivalent** comportent une tige métallique taillée et un corps en plastique moulé isolant contenant l’électronique et la pile. Toutes les clés **PROTEC² CLIQ ou techniquement équivalent** sont équipées d’une horloge interne temps réel et d’une mémoire qui permet d’enregistrer les événements et de récupérer les historiques.

Les clés **PROTEC² CLIQ ou techniquement équivalent** seront également disponibles en version **CLIQ™ Connect ou techniquement équivalent**. Les clés CLIQ Connect ou techniquement équivalent peuvent être mises à jour en Bluetooth via l’application smartphone **CLIQ™ Connect ou techniquement équivalent.**

* La durée de vie de la pile est de 10 ans et il est très facile de changer la pile en ouvrant le capot plastique de la clé
* Pour les clés Bluetooth CLIQ Connect ou techniquement équivalent, la durée de vie de la pile est de 1 an
* Pile CR2450N ou techniquement équivalent
* Indication sonore et lumineuse bicolore sur chaque côté de la clé
* Capot plastique optionnel pour ajouter un tag RFID sur la clé et l’utiliser avec d’autres lecteurs sur site
* Plusieurs capots de couleur disponibles en option
* Certification IP57
* Utilisation possible de -20°C à +50°C
* Fonctionnalités horaires disponibles dans toutes les clés utilisateurs : paramétrages de validité, planning & horaire des événements
* ….

Ci-dessous sont détaillées les références des équipements :

* Clé standard, série : **PROTEC² CLIQ**, référence : **TQ406/TQG406** ou techniquement équivalent
* Clé Dynamique, série : **PROTEC² CLIQ**, référence : **TQ407/TQG407** ou techniquement équivalent
* Clé de programmation, série : **PROTEC² CLIQ**, référence : **TQ403/TQG403** ou techniquement équivalent
* Clé utilisateur à fonction horaire certifiée ATEX, **CLIQ Connect**, **référence :TQ406EX0000**
* Clé utilisateur dynamique certifiée ATEX, **CLIQ Connect**, **référence : TQ407EX0000**
* Clé de programmation, certifiée ATEX, **CLIQ Connect**, **référence :TQ403EX0000**
* Clé standard, série : clés **CLIQ Connect**, référence : **TQB406/TQBG406** ou techniquement équivalent
* Clé Dynamique, série : **CLIQ Connect**, référence : **TQB407/TQBG407** ou techniquement équivalent
* Clé de programmation, série : **CLIQ Connect**, référence : **TQB403/TQBG403** ou techniquement équivalent
* Clé temps réel, série : **CLIQ Connect**, référence : **TQC407/TQGC407** ou techniquement équivalent
* …

**La liste ci-dessus n’est pas exhaustive, les autres références des clés mécatroniques seront prévues dans le cadre du présent marché et seront détaillées suivant les préconisations du paragraphe 4.3.13 du présent programme.**

#### Boitier de programmation et de transmission des droits d’accès

Les droits pourront être mis à jour par différents moyens, adaptés à l’environnement et au besoin des sites. La solution proposée permettra les moyens d’actualisation suivants :

* Borne murale intérieure avec option de compatibilité avec le protocole de sécurité IEEE 802.1X pour qu’elle puisse se connecter au réseau local.
* Borne murale extérieure et protégée contre le vandalisme, minimum IP 57 et IK9.
* Borne mobile permettant la mise à jour des clés non-Bluetooth en mobilité.

Ci-dessous sont détaillées les références des équipements :

* Boitier de programmation local, série**: ABLOY CLIQ PDA500** ou techniquement équivalent
* Borne murale intérieure, série : **ABLOY PDA100**, ou techniquement équivalent
* Borne murale intérieure avec écusson extérieur, série : **ABLOY PDA110**, ou techniquement équivalent
* Borne murale extérieure et protégée contre le vandalisme, série : **ABLOY PDA120**, ou techniquement équivalent
* Lecteur CLIQ série : **ABLOY TQ124**, ou techniquement équivalent
* Borne mobile permettant la mise à jour des clés non-Bluetooth en mobilité, série : **ABLOY PDA200**, ou techniquement équivalent

#### Accessoires et autres équipements

* Support de mise en applique pour borne murale, série : **813738,ABLOY PROTECT² CLIQ** ou techniquement équivalent
* Outil spécifique de démontage de la borne murale, série : **813858,ABLOY PROTECT² CLIQ** ou techniquement équivalent
* Adaptateur USB pour connexion de la borne murale, série **7911056**, **ABLOY PROTECT² CLIQ** ou techniquement équivalent
* Adaptateur PoE pour connexion de la borne murale, série **7370001**, **ABLOY PROTECT² CLIQ** ou techniquement équivalent
* Alimentation 12 VDC, série :**EA700**, **ABLOY PROTECT² CLIQ** ou techniquement équivalent
* Logiciel de programmation des serrures et clés mécatroniques (web manager CLIQ) de PROTECT² CLIQ ou techniquement équivalent, permettant de fonctionner en multisites et absorber l’ensemble des besoins, des utilisateurs et des opérateurs du CHUT et devra respecter les exigences détaillées dans les chapitres ci-dessus et notamment chapitres :3 et 4 (fonctionnement en multisites, sur un seul serveur virtuel, cloisonné et redondé, avec l’accès limité et exclusif de chaque administrateur à son site respectif dont il a la gestion…)
* Le logiciel de programmation serrures et clés mécatroniques devra être nativement intégré au logiciel de contrôle d’accès : **PCPass, XT manager** **de Synchronic** ou techniquement équivalent
* Le fabricant détaillera dans son BPU les abonnements nécessaires spécifiques aux clés **CLIQ Connect ou techniquement équivalent** par tranche de nombre d’équipement
* ….

### Badges UHF

Les badges proposés seront de technologie UHF RFID, ils permettront la communication et le fonctionnement avec les lecteurs de badges UHF de la solution de contrôle d’accès proposée :**PCPass, XT manager de Synchronic**, ou techniquement équivalentet seront gérés et programmés par ces applicatifs : **PCPass, XT manager de Synchronic.**

L’ensemble des badges fournis seront paramétrés et programmés par le titulaire du présent marché.

ci-dessous sont détaillées les caractéristiques minimales de ces équipements :

#### Teletag-TAG parebrise athermique UHF

* Teletag – Tag pare-brise athermique UHF. Puce UHF GEN2 programmé, fourni avec porte-tag.
* Fréquence porteuse / Puce :UHF / IMPINJ Monza R6-P
* Matériaux :ABS
* Dimensions (h x l x p) : 70 x 30 x 11 mm
* Couleur Gris RAL7035 / Support de fixation : noir

Série de type **31-BMU-ST3** de marque **Synchronic** ou techniquement équivalent

#### Etiquette adhésive UHF pour véhicule (ETA)

* Etiquettes adhésives parebrises UHF
* Fréquence : UHF
* Puce : EPC1 Gen 2 Alien Higgs-3
* Distance de lecture : 0 - 10 m
* Dimensions (h x l x p) : 96,5 x 23,2 x 0,36 mm
* Température de fonctionnement : -40ºC to +70ºC
* Résistance : Résistant aux intempéries, à l’eau, au soleil et aux poussières / Humidité : 5 - 95%
* Normes : ISO18000-63 / EPC1 Gen 2 Versions ETSI 302-208 : 866 MHz (Europe), FCC Part 15 : 915 MHz (USA), Certifications : CE

Marque **Synchronic** ou techniquement équivalent

#### Etiquette adhésive UHF pour véhicule (ETA V2)

* Etiquettes adhésives parebrises UHF ETAV2
* Fréquence : UHF
* Puce : IMPINJ Monza R6-P
* Distance de lecture : 0 - 13 m
* Dimensions (h x l x p) : 100x30 mm
* Température de fonctionnement : -40ºC to +85ºC
* Résistance : Résistant à l’eau, aux produits d’entretien, aux UV nocifs et aux poussières / Humidité : 5 - 95%
* Normes : Normes : ISO18000-63 / EPC1 Gen 2 Broadband - Certifications : CE, FCC

Marque **Synchronic** ou techniquement équivalent

#### Badge Passif UHF ISO

* Badge Passif UHF ISO
* Distance de lecture Max 3.5m, fourni avec porte-tag.
* Fréquence porteuse / Puce :UHF ISO

Série de type **31-BMU-ST1** de marque **Synchronic** ou techniquement équivalent

#### Badge Passif UHF avec technologie Mifare

* Badge Passif UHF + MIFARE® 1K ISO
* Distance lecture Max 2M

Série de type **31-BMUMF-ST1** de marque **Synchronic** ou techniquement équivalent

#### Badge UHF avec technologie DESFire EV2

* Badge DESFire® EV2 2K + UHF de la puce UHF avec le n° de série de la puce DESFire®

Série de type **31-BMUDS2-EV2** de marque **Synchronic** ou techniquement équivalent

### Badges dématérialisés sur smartphones

Les badges proposés seront dématérialisés et sous format numérique sur les smartphones des professionnels de santé (via l’application spécifique sur smartphone du fabricant).Ils permettront la communication et le fonctionnement avec les lecteurs de badges transparents équipés de Bluetooth de la solution de contrôle d’accès proposée et fonctionneront avec les logiciels de contrôle d’accès de la solution :**PC Pass, XT manager de Synchronic**, ou techniquement équivalent. Ils seront gérés et programmés par ces applicatifs : **PC Pass, XT manager de Synchronic.**

Il sera prévu les trois niveaux de fonctionnalités suivantes :

* Badge vert : fonctionnant sur lecture CSN = 0 crédit
* Badge Orange : 3 crédits / sécurisable au même titre qu’un badge DESfire/ fonctionnalité SLIDE, Tap, Main libre (badge bloqué sur le téléphone)
* Badge Bleu : 5 crédits / sécurisable au même titre qu’un badge DESfire / fonctionnalité SLIDE, Tap, Main libre + Télécommande (badge non bloqué = révocable sur le téléphone)

Les badges dématérialisés n'auront pas de durée de vie limitée, ils ne seront donc pas à renouveler et sont en achat définitif.

Le fabricanttitulaire du présent marchéprévoira l’ensemble des licences et des crédits nécessaires par badge dématérialisé sur smartphone, pour le bon fonctionnement des installations de contrôle d’accès via smartphone par badge dématérialisé.

### Equipements de personnalisation des badges

Le titulaire du présent marché proposera également l’ensemble des outils (équipements et logiciels) permettant la personnalisation des badges. Ils fonctionneront nativement avec la solution globale de contrôle d’accès de série : **XT Print** de marque **Synchronic** ou techniquement équivalent.

L’ensemble des équipements de personnalisation des badges fournis par le fabricant seront paramétrés et programmés par le titulaire du présent marché.

ci-dessous sont détaillées les caractéristiques minimales de ces équipements :

#### Imprimante simple face - Chargeur 50 cartes – USB :

* Sublimation couleur directement
* sur la carte / Transfert thermique résine
* Impression simple face, bord à bord
* Tête d’impression 300 dpi (11,8 points/mm)
* 16 millions de couleurs
* 16 Mo de mémoire (RAM),
* 32 Mo pour la version Expert
* Couleurs disponibles : rouge flamme et brun taupe
* Couleur (YMCKO) : 120 - 150 cartes/heure1
* Monochrome : 400 - 500 cartes/heure
* USB (1.0, 1.1, 2.0, 3.0) , câble fourni
* Ethernet TCP-IP 10BaseT, 100BaseT
* (Trafic Led) sur la version Expert
* Chargeur automatique ou manuel
* Capacité du chargeur : 50 cartes(0,76mm– 30 mil)
* Capacité du réceptacle : 20 cartes(0,76mm– 30 mil)
* Épaisseur des cartes :0,25 à 0,76mm(10 à 30 mil),ajustement à l’aide de la jauge
* Types de cartes : cartes PVC, cartes PVC composite, cartes PET, cartes ABS1, vernis spéciaux1
* Format des cartes : ISO CR80 – ISO 7810 (53,98mmx 85,60 mm)
* Modules disponibles sur la version Expert :
  + Encodeur piste magnétique ISO7811 HiCo/LoCo, JIS2
  + Station de contact puce ISO 7816-2
  + Encodeur carte à puce contact -PC/SC, EMV 2000-1
  + Encodeur carte à puce sans contact - ISO 14443A, B,ISO15693, MIFARE, DESFire, HIDiCLASS
* Connexions USB interne
* Options combinables entre elles
* Montage usine ou sur site
* Emplacement pour verrou de sécurité Kensington®
* Cryptage des données pour encodage magnétique
* Mode veille prolongée et consommation électrique réduite
* CE, FCC, IEC, VCCI, CCC, KC, BIS, EAC ,RoHS
* Dimensions (H x l x P) :195 x 205 x 315mm
* Poids : 3,3 kg

Série de type **31-** **31-EIL00061-E de** marque **Synchronic** ou techniquement équivalent

#### Rubans pour imprimante :

L’imprimante sera fournie avec ses accessoires et notamment :

* Raban couleurs YMCKO 300 faces , série **31-ERC063-E300** marque **Synchronic** ou techniquement équivalent
* Raban monochrome noir KO 600 impressions, série **31-ERN063-E600** marque **Synchronic** ou techniquement équivalent

### Fourniture de matériel non listé au BPU

A la demande du CHU de Toulouse, le titulaire fournira un devis des équipements complémentaires et accessoires non listés au BPU et entrant dans l’intitulé du marché, à savoir notamment :

* Ensembles plaques béquilles pour portes en verre ou autres portes spécifiques;
* Autres dimensions des plaques béquilles;
* Autres longueurs de cylindres ou demi-cylindres ;
* Autres longueurs de cylindres ou demi-cylindres des serrures électroniques et des clés mécatroniques (solution CLIQ ou techniquement équivalent)
* Cadenas de grade 3,4,5,6-séries :PLLW330/340/350/362**,** ABLOY PROTECT² CLIQ ou techniquement équivalent,
* Serrure pour casier connecté, filaire ou radio fréquence ;
* Bouton poussoir sans contact ;
* Alimentation type AES;
* Kits d’adaptation pour béquille antipanique de marque habituellement utilisée comme ECO, BKS, DORMA, ISEO, CISA, ANTIPANIC, TESA,…

Ces produits pourront être commandés dans le cadre du marché, par application de la remise sur les achats hors bordereau (cf. Article 2 du CCAP).

Aucune commande ne peut être effectuée sans une validation expresse du devis par le pouvoir adjudicateur.

## Prestations d’intégration du système de contrôle d’accès

### Paramétrages et intégrations des solutions « logiciels/applicatifs »

le titulaire du présent marché devra intégrer dans son offre les prestations détaillées ci-dessous et devra les détailler dans son BPU :

* Fourniture et présentation des méthodologies des déploiements des applicatifs/logiciels avec planifications à valider par le CHUT par site et pour l’ensemble des sites du CHUT, permettant la mise en œuvre des solutions « logiciels » du nouveau système de contrôle d’accès sur les différents sites du CHUT.
* Les études nécessaires permettant les déploiements et les mises en œuvre des solutions « logiciels » du nouveau système de contrôle d’accès sur les différents sites du CHUT.
* Les participations aux réunions suivant les spécifications de la DSN (voir chapitre :5 du présent programme), permettant les déploiements et les mises en œuvre des solutions « logiciels » du nouveau système de contrôle d’accès sur les différents sites du CHUT.
* La fourniture et la mise en place des applicatifs/logiciels (Gestion, supervision technique, logiciel de chiffrement et enrôlement des badges, logiciel des serrures et cylindres électroniques, logiciel des cylindres et serrures des clés mécatroniques, logiciel de lecteur de plaque d’immatriculation), au niveau du serveur virtuel cloisonné et redondé pour couvrir l’ensemble des sites du CHU de Toulouse
* La fourniture et mise en place des applicatifs/logiciels de gestion de contrôle d’accès de type client léger par site et par poste pour l’ensemble des sites du CHU de Toulouse
* La fourniture et mise en place des applicatifs/logiciels de supervision technique par poste utilisateur et par site pour les gestionnaires des droits d’accès
* La fourniture et mise en place des applicatifs/logiciels de supervision par poste utilisateur pour les opérateurs techniques pour l’ensemble des sites du CHU de Toulouse
* Les fournitures les mises en place des extensions des logiciels et applicatifs selon les demandes du maître d’ouvrage
* Les échanges et préparations nécessaires permettant ces déploiements avec les différents services du CHU de Toulouse, pour validation (services techniques, services informatiques, gestionnaires des droits d’accès, la maîtrise d’œuvre et le maître d’ouvrage)
* les réunions en présentiel sur les différents sites du CHUT, nécessaires permettant de présenter la méthodologie, la planification envisagées pour validation par le CHUT
* les réunions en présentiel sur les différents sites du CHUT nécessaires permettant de réaliser ces présentations de déploiements des applicatifs
* la réalisation des études nécessaires lui permettant de réaliser ces prestations avec les validations nécessaires avec la maîtrise d’œuvre et le maître d’ouvrage et l’ensemble des services du CHUT concernés par les travaux avant toute intervention
* les paramétrages et les programmations nécessaires des différents applicatifs permettant les déploiements de la nouvelle solution de contrôle d’accès, en présentiel sur les différents sites du CHUT
* interfaces du logiciel de supervision de contrôle d’accès avec le logiciel de supervision de la GTC « PC Vue » existant sur les différents sites du CHUT, permettant le renvoi de la synthèse/défaut des équipements de contrôle d’accès depuis le logiciel de supervision de contrôle d’accès vers le logiciel de supervision GTC PCVue existant sur les différents sites du CHUT
* Les interfaces du logiciel de supervision de contrôle d’accès avec les bases de données du CHUT des différents logiciels (AGIRH, annuaire centralisé…) permettant d’automatiser l’attribution des droits d’accès depuis le logiciel de gestion des droits de la nouvelle solution de contrôle d’accès.
* les essais et les mises en service nécessaires après les déploiements des applicatifs ou les extensions des applicatifs
* les mises à disposition de la documentation technique et les manuels d’utilisation nécessaires.

Le titulaire du présent lot devra présenter une méthodologie et une planification détaillées à valider avec la maîtrise d’œuvre, le maître d’ouvrage et l’ensemble des services du CHU de Toulouse concernés par ces travaux pour validation avant toute intervention.

### Prestations de préparations, études et de migrations

#### Migrations entre les anciennes et la nouvelle solution de contrôle d’accès

le titulaire du présent marché devra intégrer dans son offre les prestations détaillées ci-dessous et devra les détailler dans son BPU, permettant la migration entre les anciennes solutions de contrôle d’accès existantes sur les différents sites du CHUT et la nouvelle solution de contrôle d’accès à déployer dans le présent marché, avec notamment :

* Fourniture et présentation des méthodologies de migration détaillées avec planifications à valider par le CHUT par site et pour l’ensemble des sites du CHUT, permettant la migration entre anciennes solutions de contrôle d’accès existantes sur les sites du CHUT et la nouvelle solution à mettre en place
* Audits des installations et équipements existants lui permettant de réaliser la migration entre anciennes solutions de contrôle d’accès existantes sur les sites du CHUT et la nouvelle solution à mettre en place
* Les extractions des bases de données existantes au sein des différentes solutions de contrôle d’accès existantes au sein des différents sites du CHUT de Toulouse. (Toutes les bases de données existantes sur toutes les solutions et installations de contrôle d’accès existantes sur tous les sites du CHU de Toulouse)
* Analyses et préparations des bases de données existantes (y compris nettoyages de toutes les bases de données existantes), adaptions et mises à jour de ces bases de données pour réutilisation au sein de la nouvelle solution de contrôle d’accès et pour l’ensemble des sites du CHUT
* Intégrations des bases de données existantes à mettre à jour au sein de la nouvelle solution de contrôle d’accès
* Les réalisations des études techniques et des relevés sur les sites du CHUT autant de fois que nécessaire en fonction de ces travaux de migration pour l’ensemble des sites du CHUT.
* Les réalisations des échanges et réunions nécessaires avec les services du CHUT, permettant la validation de la méthodologie de migration et la mise en place de cette migration
* Assurer une continuité de services des installations de contrôle d’accès durant toute la phase de migration (entre anciennes solutions de contrôle d’accès et la nouvelle solution)
* les paramétrages et les programmations nécessaires des différents applicatifs permettant les déploiements de la nouvelle solution de contrôle d’accès
* les essais et les mises en service nécessaires en fonction de ces travaux
* les mises à disposition de la documentation technique et les manuels d’utilisation nécessaires.

Le titulaire du présent marché assistera et conseillera le maître d’ouvrage tout le long de la procédure de migration ; ce dernier proposera différentes solutions avec des planifications détaillées adaptées à l’activité, à l’usage et au fonctionnement du CHUT, pour validation.

#### Migrations entre les anciennes et les nouvelles cartes de professionnels de santé (badges)

le titulaire du présent marché devra intégrer dans son offre les prestations détaillées ci-dessous et devra les détailler dans son BPU, permettant la migration entre anciennes cartes de professionnels de santé et badges existants sur les différents sites du CHUT et les nouvelles cartes de professionnels de santé CPSx (CPS 3/ 4)/CPE à déployer dans le futur, avec notamment:

* **La définition et l’élaboration de la charte de chiffrement, d’encodage et d’enrôlement des badges avec les services concernés du CHU de Toulouse (la DSN, le service de sécurité, les gestionnaires et administrateurs des différents sites…) et suivant les recommandations et les exigences ANSSI en vigueur**
* Fourniture et présentation des méthodologies de migration détaillées avec planifications à valider par le CHUT par site et pour l’ensemble des sites du CHUT, permettant la migration entre anciennes cartes de professionnels de santé (badges) existantes sur les sites du CHUT et la nouvelle carte de professionnels de santé (CPS 3 /4 et CSPx)/CPE
* Audits des installations et des équipements existants lui permettant de réaliser la migration entre anciennes entre les anciennes cartes de professionnels de santé (badges) existantes sur les sites du CHUT et les nouvelles cartes de professionnels de santé (CPS 3 /4 et CSPx)/CPE
* Extractions des bases de données existantes au sein des différentes solutions de contrôle d’accès existantes au sein des différents sites du CHUT de Toulouse. (Toutes les bases de données existantes sur toutes les solutions et installations de contrôle d’accès existantes sur tous les sites du CHU de Toulouse)
* Analyses et préparations des bases de toutes les données existantes, adaptions et mises à jour de ces bases de données pour réutilisation au sein de la nouvelle solution de contrôle d’accès et pour l’ensemble des sites du CHUT
* Intégrations des bases de données existantes à mettre à jour au sein de la nouvelle solution de contrôle d’accès, y compris les paramétrages et les programmations nécessaires des différents applicatifs de contrôle de contrôle d’accès
* Réalisations des études techniques et relevés à réaliser sur les sites du CHUT autant de fois que nécessaires en fonction de ces travaux, sur l’ensemble des sites du CHT.
* Les réalisations des échanges et réunions nécessaires avec les services du CHUT, permettant la validation de la méthodologie de migration et la mise en place de cette migration
* Assurer une continuité de services des installations de contrôle d’accès durant toute la phase de migration (entre les anciennes générations de badges et cartes professionnels de santé du CHU de Toulouse « CHUT » et les nouvelles cartes professionnels de santé CPS 3 / 4 et CPSx )/CPE
* les essais et les mises en service nécessaires en fonction de ces travaux
* les mises à disposition de la documentation technique et les manuels d’utilisation nécessaires.

Le titulaire du présent marché assistera et conseillera le maître d’ouvrage tout le long de la procédure de migration ; ce dernier proposera différentes solutions avec des planifications détaillées adaptées à l’activité, à l’usage et au fonctionnement du CHUT, pour validation.

### Prestations d’interfaçage automatique avec la base de données AGIRH

Le titulaire du présent marché devra prévoir également toutes les prestations nécessaires à l’interfaçage automatique de la base de données du logiciel RH du CHU de Toulouse « AGIRH », avec les logiciels et les applicatifs de la nouvelle solution de contrôle d’accès de marque Synchronic ou techniquement équivalent.

Les droits d’accès seront attribués automatiquement ou manuellement aux choix du M.O à partir de cette base de données via les unités fonctionnelles/administratives (UF ou UA) définis dans la base de données AGIRH.

Le présent lot intégrera dans son BPU les échanges nécessaires avec les gestionnaires des droits d’accès des différents sites du CHU de Toulouse lui permettant : de créer, d’établir, de modifier ou de supprimer ou de mettre à jour les différentes UF/UA et les droits d’accès à attribuer en fonction des différents sites du CHUT.

Les droits d’accès seront mis à jour automatiquement au sein des applicatifs de la nouvelle solution de contrôle d’accès en fonction de la mise à jour de la base de données AGIRH (personnels entrants et sortants, droit à créer ou à supprimer).

La fréquence de mise à jour de cette base de données sera définie en phase de déploiement et intégration des applicatifs de la nouvelle solution de contrôle d’accès.

### Paramétrages et intégrations des équipements de contrôle d’accès

Le titulaire du présent marché devra prévoir dans son offre et détailler dans le BPU (par tranche de nombre d’équipement), les prestations suivantes :

* les paramétrages, les programmations nécessaires des équipements de contrôle d’accès et notamment, en fonction de chaque projet (prestations à réaliser sur site) :
  + Coffret UTL/UTP,
  + UTL,
  + UTP,
  + Autres cartes d’interfaçages,
  + Têtes de lecteurs (tout type) :
    - Lecteurs de badges RFID (tout type)
    - Lecteurs de badges UHF longue portée
    - Serrures et cylindres électroniques
    - Serrures et cylindres mécatroniques
    - Lecteurs de plaques d’immatriculation
    - …..
  + Différents accessoires :
    - Hubs et antennes des serrures et cylindres électroniques
    - Boitiers de programmations et transmissions des serrures , cylindres des clés mécatroniques
  + BP/BG
  + ….
* Les intégrations, les créations et les mises à jour des logiciels de gestion des droits d’accès et de supervision technique des équipements de contrôle d’accès (UTL/UTP/LB/têtes de lectures :LB RFID et LB UHF, serrures et cylindres électroniques et mécatroniques, lecteurs de plaques d’immatriculation, hub et antennes des serrures électroniques/boitiers de transmissions et de programmations des clés mécatroniques/BP/BG) en fonction de chaque projet (prestation à réaliser sur site)
* Les échanges nécessaires avec les différents services techniques du CHU de Toulouse (DSN/contrôle d’accès/gestionnaires des sites/services techniques…) permettant les paramétrages, les programmations et intégrations des équipements de contrôle d’accès en fonction de chaque projet spécifique.
* Les échanges nécessaires avec les différents intervenants (maîtrise d’ouvrage, maîtrises d’œuvres, les entreprises qui installeraient les équipements de contrôle d’accès) en fonction de chaque projet spécifique permettant les paramétrages, les programmations et intégrations des équipements de contrôle d’accès
* Les participations aux réunions en présentiel avec l’ensemble des intervenants permettant les paramétrages, les programmations et intégrations des équipements de contrôle d’accès en fonction de chaque projet spécifique
* interfaces du logiciel de supervision de contrôle d’accès « Horizon Vision » ou équivalent avec le logiciel de supervision de la GTC « PC Vue » existant sur les différents sites du CHUT, permettant le renvoi de la synthèse/défaut des équipements de contrôle d’accès depuis le logiciel de supervision de contrôle d’accès vers le logiciel de supervision GTC « PCVue » existant sur les différents sites du CHUT, compris les paramétrages, programmations et intégrations des équipements de contrôle d’accès permettant de réaliser cette fonction.
* Les fournitures des tableaux détaillant les informations nécessaires de chaque UTL à la DSN :
  + Le site
  + Le bâtiment
  + Le niveau du bâtiment
  + Le numéro de la pièce/ou du local
  + le numéro de prise RJ45
  + le numéro de l’UTL
  + le type d’équipement
  + l’adresse MAC de l’UTL
* Ces éléments permettront à la DSN de fournir les éléments listés ci-dessous au fabricant titulaire du présent lot, pour que ce dernier puisse réaliser les paramétrages, les programmations et intégrations des équipements de contrôle d’accès :
  + L’adresse IP fixe
  + Le masque
  + La passerelle réseau
  + Le DSN1
  + Le DSN2

* Les fournitures des documentations techniques des équipements, schémas de câblages des équipements de contrôle d’accès
* Les participations en présentiel aux essais et aux mises en service des installations de contrôle d’accès en fonction de chaque projet de contrôle d’accès.

### Prestations de paramétrages et programmations des badges UHF

Le titulaire du présent marché devra prévoir dans son offre et détailler dans le BPU (par tranche de nombre de badges), les prestations suivantes :

* les paramétrages, les programmations nécessaires des badges UHF (tout type)
* Les intégrations, les créations et les mises à jour des logiciels de gestion des droits d’accès tenant compte des badges à créer ou à modifier
* les participations aux réunions nécessaires avec les différents intervenants (maîtrise d’ouvrage, maîtrises d’œuvres, entreprises intégratrices, les services techniques du CHUT : contrôle d’accès, sécurité, gestionnaires de sites…), permettant les paramétrages des badges UHF et leurs intégrations au sein des logiciels et applicatifs de gestion de la nouvelle solution de contrôle d’accès
* les participations aux essais et à la mise en service des badges UHF
* …..

### Prestations de chiffrement d’encodage et d’enrôlement des badges

Le titulaire du présent marché devra prévoir dans son offre et détailler dans le BPU (par tranche de nombre de badges), les prestations concernant les chiffrements, les encodages et les enrôlements des badges conformément aux exigences ANSSI en vigueur. Le présent lot devra notamment les prestations listées ci-dessous :

* les chiffrements, les encodages et les enrôlements des badges conformément aux exigences ANSSI en vigueur et à la charte de chiffrement à définir avec le CHUT
* Les intégrations, les créations et les mises à jour des logiciels de gestion des droits d’accès tenant compte des badges à encoder et à enrôler
* Les participations aux réunions nécessaires avec les différents intervenants (maîtrise d’ouvrage, maîtrises d’œuvres, entreprises intégratrices, les services techniques du CHUT : contrôle d’accès, sécurité, gestionnaires de sites…), permettant les paramétrages des badges à enrôler et à encoder et leurs intégrations au sein des logiciels et applicatifs de gestion de la nouvelle solution de contrôle d’accès
* les participations aux essais et à la mise en service des badges à chiffrer, à encoder et à enrôler
* ….

### Prestations de paramétrages et programmations des clés mécatroniques

Le titulaire du présent marché devra prévoir dans son offre et détailler dans le BPU (par tranche de nombre de badges), les prestations suivantes :

* les paramétrages, les programmations nécessaires des clés mécatroniques (tout type)
* Les intégrations, les créations et les mises à jour des logiciels de gestion des droits d’accès tenant compte des badges à créer ou à modifier
* les participations aux réunions nécessaires avec les différents intervenants (maîtrise d’ouvrage, maîtrises d’œuvres, entreprises intégratrices, les services techniques du CHUT : contrôle d’accès, sécurité, gestionnaires de sites…), permettant les paramétrages des clés mécatroniques et leurs intégrations au sein des logiciels et applicatifs de gestion de la nouvelle solution de contrôle d’accès
* les participations aux essais et à la mise en service des clés mécatroniques
* …..

### Prestations de paramétrages et programmations badges dématérialisés sur smartphones (contrôle d’accès par smartphone)

Le titulaire du présent marché devra prévoir dans son offre et détailler dans le BPU (par tranche de nombre de badges), les prestations suivantes :

* les paramétrages, les programmations nécessaires des badges dématérialisés sur smartphones
* Les intégrations, les créations et les mises à jour des logiciels de gestion des droits d’accès tenant compte des badges à créer ou à modifier
* les participations aux réunions nécessaires avec les différents intervenants (maîtrise d’ouvrage, maîtrises d’œuvres, entreprises intégratrices, les services techniques du CHUT : contrôle d’accès, sécurité, gestionnaires de sites…), permettant les paramétrages des clés mécatroniques et leurs intégrations au sein des logiciels et applicatifs de gestion de la nouvelle solution de contrôle d’accès
* les participations aux essais et à la mise en service des clés mécatroniques
* …..

## Prestations de formation du personnel

Le titulaire du présent marché devra assurer la formation du personnel chargé de la surveillance de l'établissement et de la gestion des droits d’accès à l'utilisation de l'ensemble des matériels et le logiciel de gestion et d’exploitation du système de contrôle d’accès. Il devra à minima prévoir les formations suivantes :

* Formations des gestionnaires/administrateurs des sites (soit 5 personnes par site): à
  + L’utilisation et l’exploitation des logiciels de gestion de droits d’accès (avec l’ensemble des modules et des fonctionnalités de la solution globale logicielle de contrôle d’accès),
  + L’utilisation et l’exploitation du logiciel de supervision technique des équipements de contrôle d’accès,
  + L’utilisation et l’exploitation des logiciels des serrures, cylindres électroniques et clés mécatroniques,
  + L’utilisation et l’exploitation du logiciel de gestion des clés de chiffrement,
  + Les programmations, les paramétrages, les encodages, les chiffrements et les enrôlements des :
    - Badges, (actuelles cartes et badges utilisés sur les différents sites du VHT ainsi que les futures cartes et badges CPSx V4)/CPE,
    - Des badges et étiquettes UHF (futures et actuelles à réutiliser avec la nouvelle solution de contrôle d’accès),
    - Des clés mécatroniques (tout type),
    - Contrôle d’accès biométrique par empreinte,
    - Contrôle d’accès par QR Code,
    - Contrôle d’accès par smartphone : Badges numériques dématérialisés sur smartphones
    - Contrôle d’accès des plaques d’immatriculation
    - …..
* Formations du personnel du service technique et d’exploitation du CHUT **(niveau 1)** à :
  + l’utilisation et l’exploitation du logiciel de supervision technique,
  + ainsi qu’à l’utilisation, l’exploitation des équipements de contrôle d’accès
  + formation aux fonctionnements des installations de contrôle d’accès de la nouvelle solution de contrôle d’accès à déployer dans le cadre du présent projet, y compris aux équipements et aux logiciels des serrures, cylindres électroniques et clés mécatroniques et câblages et aux raccordements de l’ensemble des équipements de contrôle d’accès de cette nouvelle solution (UTL, LB, serrures, cylindres électroniques et mécatroniques, lecteurs de plaques d’immatriculation, bornes UHF…) .

La formation intégrera également la partie : les mises en œuvre, les installations, et les paramétrages des cartes des lecteurs de badges, les diagnostics des cartes et des lecteurs de badges, les remplacements des cartes et des lecteurs de badges. Il sera prévu :

* + 1 formation pour le personnel technique de Purpan, soit 12 personnes,
  + 1 formation pour le personnel technique de Rangueil, soit 8 personnes,
  + 1 formation pour l’équipe exploitation, soit 2 personnes,
  + 1 formation par site (pour les autres sites) pour le personnel technique, soit 2 personnes,
  + 1 formation annuelle pour le maintien des acquis pour 6 personnes, pour le personnel technique
* Formations du personnel du service technique et d’exploitation du CHUT **(niveau 2)** :
  + Formations aux paramétrages, aux programmations et à l’intégration des équipements de contrôle d’accès (UTL,UTP, LB, toutes les têtes de lecteurs prévues dans le cadre du présent marché) sur les différents logiciels de la nouvelle solution de contrôle d’accès, y compris l’utilisation et l’exploitation des logiciels embarqués et des logiciels permettant de paramétrer et programmer les différents équipements de contrôle d’accès, (tous les équipements de contrôle d’accès prévus dans le cadre du présent marché). Il sera prévu :
  + 1 formation pour le personnel technique pour 6 personnes
  + 1 formation annuelle pour le maintien des acquis pour 6 personnes
* Formations du personnel de la DSN quant au fonctionnement des équipements et des installations de contrôle d’accès (et notamment pour le volet informatique), y compris les formations à l’ensemble des logiciels (applicatifs) de la nouvelle solution de contrôle d’accès à déployer dans le cadre du présent projet. (Soit 5 personnes par site)
* Formation du personnel concernant la personnalisation des badges et l’utilisation du logiciel de personnalisation **XT Print** ou équivalent ainsi que les outils d’impression des badges

Les sites seront organisés et cloisonnés sur un seul serveur virtuel, comme détaillé ci-dessous :

* Site :Purpan-Garonne
* Site :Rangueil-Larrey
* Site : Chapitre
* Site : Logipharma
* Sites :Hôtel-Dieu-La Grave
* Site :Salies du salat
* Site :IUCT Oncopole

Chaque formation devra être réalisée au sein des locaux spécifiques du CHU de Toulouse, le fabricant fournira les outils, les applicatifs nécessaires permettant le bon déroulement de la formation du personnel du CHUT.

Le titulaire du présent marché fournira en fin de formation, les supports de formation nécessaires, ainsi qu’un mémoire et un manuel d’utilisation pour chaque personne de chaque groupe de formation (en fonction du type et niveau de formation) leur permettant une utilisation et une prise en main aisée de la nouvelle solution de contrôle d’accès (partie : logiciels et partie : matériels)

## Prestations de Maintenance et prestations diverses

Le titulaire du présent marché proposera un contrat de maintenance de type « service complet » sur toute la durée du présent marché, intégrant à minima les prestations détaillées ci-dessous :

* Une assistance téléphonique, hotline (client et partenaire) **disponible du lundi au vendredi de 8h00 à 18h00, avec prise en charge immédiate.** (**Pas de coupure entre 12h et 14h**. Pas de limitation de temps). Cette prise en charge par l’assistance technique du fabricant titulaire du présent marché permettra :
  + Au personnel d’exploitation et de maintenance du CHU de Toulouse : d’analyser, de diagnostiquer les équipements qui dysfonctionneraient (avec l’assistance technique du fabricant titulaire du présent marché), afin d’apporter une solution pérenne au dysfonctionnement matériel des installations de contrôle d’accès.
  + De répondre aux différents besoins et aux demandes du personnel d’exploitation et de maintenance du CHU de Toulouse, suivant les différents dysfonctionnements des équipements et des installations de contrôle d’accès qui peuvent apparaître sur les différents sites du CHUT de Toulouse, afin d’accompagner ces derniers, pour apporter une solution pérenne à ces dysfonctionnements.
  + Au personnel d’exploitation et de maintenance du CHU de Toulouse de réaliser les opérations de maintenance sur le terrain de l’ensemble des équipements et des installations de contrôle d’accès (avec l’assistance technique du fabricant titulaire du présent marché).
  + Autres demandes du personnel d’exploitation et de maintenance du CHU de Toulouse suivant les différents besoins et les différents dysfonctionnements des équipements et des installations de contrôle d’accès qui peuvent apparaître sur les différents sites du CHUT de Toulouse.
  + …..
* Téléassistance, passage par un bastion pour les logiciels dits « client lourd » installés sur le serveur suivant les spécifications de DSN du CHUT, par session Teams pour les logiciels dits clients légers à installer sur les PC)
* Mise en place du processus de reprise, dépannage et réparation du matériel défectueux, y compris les déplacements nécessaires sur les sites du CHUT, les frais de transports, d’expéditions et de réexpéditions des équipements à la charge du fabricant titulaire du présent marché suivant les préconisations détaillées dans le chapitre 3.3.2 du présent programme.
* Prise en charge de l’intégration des données en masse via fichiers d’import, notamment en début de marché
* Assister le CHUT dans l'utilisation dudit logiciel et dans l’analyse des éventuels dysfonctionnements constatés,
* Assister le CHUT pour remettre dans de bonnes conditions d'exploitation les logiciels et les fichiers à la suite d'un accident causé par un mauvais fonctionnement du logiciel,
* Assister le CHUT pour les mises à jour et les nettoyages de toutes bases de données des solutions de contrôle d’accès existantes ainsi que la future solution de contrôle d’accès à déployer dans le cadre du présent marché.
* Informer le CHUT de toutes évolutions apportées au logiciel maintenu et à lui remettre toute documentation à ce sujet,
* Mettre à disposition du CHU de Toulouse et faire bénéficier d'une équipe de techniciens opérationnels, maîtrisant le logiciel et le matériel de contrôle d’accès.
* Corriger toute erreur ou anomalie de fonctionnement qui constituerait un bug **(applicatif, y compris logiciels embarqués dans les équipements de contrôle d’accès et notamment l’UTL)**. Délais de correction en fonction de l’importance du problème et du degré de criticité, avec notamment :

|  |  |  |
| --- | --- | --- |
| **PRIORITE** | **NOM** | **DEFINITION** |
| P1 | Critique | Interruption complète d'un service, d'un système, du réseau, d'une application ou d'un élément de configuration identifié comme critique. |
| P2 | Important | Un événement qui provoque la perte minime d'un service. Une solution permanente ou de contournement est disponible pour restaurer la fonctionnalité du service. |
| P3 | Modéré | Un événement constituant un dérangement pour l'utilisateur, pour lequel il existe une alternative ou une réparation possible mais qui n'empêche en rien l'utilisateur de travailler. |
| P4 | Basse | Un dysfonctionnement ou une anomalie mineur(e) relevé(e) par un utilisateur, sans que cela n’ait le moindre impact sur son travail. |

|  |  |  |
| --- | --- | --- |
| **Type incident** | **GTI** | **GTR** |
| 1 - critique | 1h. | 8h |
| 2 - important | 2h | 32h |
| 3 - modéré | 2j | 10 j |
| 4 - bas | 10j | Prochaine version.  Délais de résolution à préciser dans les 30 jours maximum suivant la création du ticket |

* Les exigences minimales de prise en compte globale et traitement des incidents ainsi que les pénalités associées sont détaillées dans le CCAP. **(Voir l’annexe détaillant la liste des types d’incident (1-critique, 2-important, 3-modéré,  4-bas) pour la partie : logiciels/applicatifs de la solution de contrôle d’accès jointe au présent programme)**

|  |  |  |
| --- | --- | --- |
| **Type incident** | **Exigence minimale de prise en compte globale** | **Exigence minimale de niveau de résolution** |
| 1 - critique | **98%** en moins de 2h | **98%** en moins de 16 heures |
| 2 - important | **80%** en moins de 8h | **80%** en moins de 4j |
| 3 - modéré | **70%** en moins de 10j | **70%** en moins de 30j |
| 4 - bas | **50%** | Sans objet |

* Mises à jour régulières des logiciels à réaliser sur les sites du CHUT, par le fabricant de la solution globale de contrôle d’accès (pour l’ensemble des têtes de lecteurs). **Le coût de la mise en œuvre est supporté par le fabricant, incluant l’installation des mises à jour sur tous les équipements concernés.** Le service maintenance du CHUT , le service DSN, les administrateurs seront prévenus 15 jours avant l’intervention du fabricant pour les mises à jour des applicatifs (logiciels) de la nouvelle solution de contrôle d’accès.
  + Pour cette prestation de mise à jour des applicatifs, le fabricant s’assurera avant toute intervention de l’état de bon fonctionnement des équipements (UTL,LB) et signalera tout dysfonctionnement aux services de maintenance CHUT et à la DSN, avant tout déploiement des mises à jour des logiciels
  + Après validation du service de maintenance du CHUT, de la DSN et des administrateurs des droits, le fabricant pourra déployer les mises à jour des logiciels.
  + **En cas de création de bugs/dysfonctionnements des équipements de contrôle d’accès (UTL/LB...) liés à ces mises à jour, le fabricant devra et à sa charge unique avec sa propre équipe de techniciens (et sans solliciter le personnel du CHUT) débugger et remettre en état de bon fonctionnement l’ensemble des équipements de contrôle d’accès (UTL/LB), suivant l’état de fonctionnement des équipements de contrôle d’accès avant son intervention. (En aucune façon, les mises à jour ne devront venir dégager l’état de bon fonctionnement des équipements de contrôle d’accès)**
* L'intégration des nouvelles fonctionnalités et technologies, à réaliser sur les sites du CHUT par le fabricant
* Assurer la compatibilité avec les nouveaux systèmes d'exploitation et services packs.
* Maintenir en bon état de fonctionnement des logiciels concernés par ce contrat, de la solution globale de contrôle d’accès (pour l’ensemble des têtes de lecteurs)
* Bénéficier dans le cadre du contrat de maintenance et sans surcoût financier complémentaire, des nouvelles versions logicielles dès leur publication et ce durant toute la durée du présent marché et pour l’ensemble des logiciels et matériel constituant la solution de contrôle d’accès :
  + PC PASS Evolution/XT manager/Horizon vision/Secur’Evolution/XT Print/XT visiteur ou techniquement équivalent
  + Logiciel Web manager CLIQ/logiciels des serrures électroniques APERIO ou techniquement équivalent
  + Logiciel des lecteurs de plaques d’immatriculation…
  + Autres logiciels des fabricants des badges dématérialisés, bornes UHF et autres solutions de contrôle d’accès détaillées dans le présent programme.
  + ….
* La maintenance évolutive de la solution de contrôle d’accès (tous les logiciels/applicatifs de la nouvelle solution de contrôle d’accès, y compris les logiciels des autres fabricants qui fonctionneraient en fond de tâche interfacé avec le logiciel natif de la nouvelle solution de contrôle d’accès)
* **Le contrat de maintenance de type « Service Complet » devra inclure la fourniture, la main d’œuvre et le déplacement sur les sites du CHU de Toulouse. En pratique, si le logiciel dysfonctionne, le fabricant se déplace et répare sans aucun frais pour le CHUT.**
* Garantir un prix préférentiel de prestations en cas d’intervention sur site hors contrat de maintenance

Le titulaire du présent marché transmettra un plan de maintenance et une planification détaillée précisant toutes les prestations et tâches de maintenance à prévoir annuellement au niveau des applicatifs et du matériel de contrôle d’accès dans le cadre du présent marché.

## Continuité de service et retrocompatibilité

Durée d’approvisionnement : le titulaire 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 mémoire technique.

Le titulaire s’engage à fournir l’ensemble des équipements déployés, ou techniquement équivalent, pendant une durée de 15 ans minimum.

**Il devra assurer une compatibilité ascendante et une rétrocompatibilité (applicatifs/logiciels et équipements) entre ancienne et nouvelle génération de technologie de solution de contrôle d’accès (applicatifs/logiciels et équipements) sur une durée de 15 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.

## Obligation de conseil

Le titulaire du présent marché mettra à disposition de l’établissement (CHUT) un chef de projet, un référent dédié au présent marché ayant les compétences et le degré de responsabilité nécessaires pour valider les choix envisagés.

Il mettra également à disposition et dans le cadre du présent marché une équipe technique de techniciens opérationnels maîtrisant le logiciel et le matériel de contrôle d’accès de la solution proposée dans le cadre du présent marché, afin d’assurer les différentes missions spécifiées dans le cadre du présent programme et notamment dans les chapitres ci-dessus (4.4, 4.5 et 4.6).

# PRESCRIPTIONS spécifiques informatiques/DSN

## Description du fonctionnement futur envisagé

### Contexte

Le CHU de Toulouse souhaite acquérir une solution applicative de gestion des contrôles d’accès qui s’intègre au système d’information interne. Ce dernier doit parfaitement couvrir l’ensemble des besoins des sites en termes de sécurité, accréditation des droits d’accès aux agents et s’intégrer dans le SI de façon transverse sans changement du mode de fonctionnement actuel.

**L’ensemble des prestations de la DSN détaillées dans le présent CCTP devront être intégrées, au bordereau des Prix Unitaires (BPU).**

### Les enjeux du Système d’Information Hospitalier

Le système d’information hospitalier couvre l’ensemble des informations utilisées dans un établissement de santé et vise à améliorer la qualité des soins, mais aussi à optimiser les coûts (réduction des tâches administratives, réduction de la durée des séjours, diminution des frais de personnel). Concrètement, le SIH permet de faciliter l’intégration en temps réel des informations entre l’opérationnel et le décisionnel

### Enjeux liés à la sécurité des systèmes d’information

L’organisation de la sécurité de l’information en place au Centre Hospitalier Universitaire de Toulouse doit assurer une évolution optimale de la maturité de l’établissement. L’approche mise en œuvre s’inscrit dans une démarche d’amélioration continue qui a pour objectif la mise en œuvre d’un système de management de la sécurité du système d’information intégré aux systèmes de management existants.

L’objectif est notamment de permettre au Centre Hospitalier Universitaire de Toulouse de se mettre en conformité avec les cadres législatifs et règlementaires en s’appuyant sur les référentiels nationaux tels que ceux de l’agence du Numérique en Santé (ANS), du ministère de la santé, le référentiel général de sécurité et les bonnes pratiques du domaine de la sécurité de l’information.

La mise en place de chantiers métier majeurs (dossier patient informatisé, gestion électronique de document, ouverture vers l’extérieur…) nécessitent la prise en compte des problématiques de sécurité de l’information sur l’ensemble de son cycle de vie justifiant une certification ISO 27001.

A ce jour, l’institution du CHU de Toulouse est certifiée ISO 27001 sur un périmètre précis. Celui-ci évolue à chaque instant. A terme, tous les sous-ensembles, systèmes d’information dont le DPI fait partie devront satisfaire à ces exigences.

## Besoins fonctionnels détaillés

### Paramétrage

#### Structure de l'établissement

Le système doit permettre de paramétrer les éléments suivants :

* Une ou plusieurs entités juridiques
* Les établissements
* Les unités fonctionnelles

Le système doit pouvoir aussi gérer des niveaux hiérarchiques ainsi que des dates d’effets afin de pouvoir au mieux planifier les ouvertures et fermetures de droits d’accès.

#### Habilitations au logiciel

Le système doit être connecté à l’AD ou Entra ID pour permettre de donner les droits d’accès au logiciel. La solution est en capacité de se connecter en SSO et via du provisionning de compte IAM.

La solution doit permettre le MFA.

Pour chaque utilisateur est associé un profil métier et une affectation à une unité fonctionnelle.

A chaque profil métier est associé un plan d'habilitation (zone d’accès restreint ou non).

Les accès à l’application doivent être tracé. Ces traces doivent être exploitables par un administrateur nommé qui garantira le bon fonctionnement du système.

#### Gestion des habilitations

Le système doit permettre de gérer les différents droits d‘accès :

* Gestion par profil métier
* Rattachement de l’agent à une ou des UFs, conformité RGPD

|  |  |  |
| --- | --- | --- |
| Rôles | Besoin | Valeur métier |
| Administrateur fonctionnel | Gérer les utilisateurs de l’application | Associer un utilisateur à un rôle utilisateur afin qu’ils puissent accéder à un ensemble de fonctionnalités de la solution. |
| Administrateur fonctionnel | Gérer les rôles utilisateur | Créer et paramétrer chaque rôle utilisateur afin de définir les accès aux différentes fonctionnalités de la solution :   * Accès aux différents modules de la solution * Visualisation des différentes vues * Génération et visualisation de requêtes et statistiques * Paramétrage de la solution |
| Administrateur technique | Gérer la maintenance et les évolutions des systèmes installés | * Créer et paramétrer chaque équipement du système, maintenir (Préventif et Curatif) tous les équipements. * Superviser à distance tous les équipements * Gérer les autorisations des profils techniques |
| Gestionnaire de site | Programmer des droits d’accès  Créer et Programmer des plages horaires  Programmer des UA et code métier  Créer et programmer des groupes d’accès  Visualiser l’état des contrôleurs  Editer des rapports-historiques  Créer, Programmer des zones de lieu | * Attribuer des droits d’accès à plusieurs niveaux (UA, métier) et à plusieurs profils de personne (professionnels CHU, prestataires, tiers, …) * Evaluation des dysfonctionnements des cartes d’accès |
| Sécurité | Pouvoir faire un audit des traces | Génération et visualisation de requêtes et statistiques :   * La liste des accès en dehors des plages horaires normales de travail et en dehors des jours ouvrés durant la semaine écoulée (pour les services avec paramétrage sur plage horaire) ; * La liste des accès refusés de la semaine, afin de détecter des tentatives d’accès frauduleuses répétées ; * Accès refusé à une zone sensible (à déterminer si possibilité de faire fonctionner des requêtes types sur un ensemble de LB et/ou UTL) ; * La liste des accès forcés (sera-t-on capable avec l’outil de produire ce type de liste ? Quel critère technique pour le CA déterminant l’accès dit « forcé ») ; * Un rapport listant les badges qui n’ont pas été utilisés lors des X derniers mois (fréquence à déterminer), permettant de s’assurer que les badges sont bien tous actifs, et d’identifier des badges qui au[1]raient dû être désactivés mais qui ne le sont pas ; * Tentatives d’accès refusées et répétées (2 fois sur une même tête de lecture et sur une période donnée, ou 2 fois par le même badge par exemple) ; * La liste complète des badges tagués visiteurs et/ou prestataires sur une période donnée ; * L’extraction de la journalisation d’usage d’un badge spécifique sur une période donnée ; * L’extraction de la journalisation d’un LB et/ou d’une UTL sur une période donnée.   La possibilité de planifier ou créer de nouvelles requêtes avec envoie automatique à une liste de destinataires selon le besoin |
| Technicien proximité (électricien) | Pouvoir superviser et maintenir le système en mobilité | * Se connecter aux équipements en local pour établir un diagnostic et, le cas échéant, réaliser les opérations de maintenance * Réaliser un pré-diagnostic à distance |

#### Gestion des droits d’accès au site

En fonction de l’UF de rattachement du profil donner accès à un UTL/un bâtiment. Pour le cas des syndicats par exemple, donner la possibilité d’avoir des droits multisites.

#### Planification des droits d’accès

Le logiciel doit permettre de planifier des droits d’accès dans le cadre de déménagement.

En effet, ce dernier doit pouvoir planifier des droits aux agents lors de recrutement, stage et autres.

Également, le logiciel doit pouvoir mettre des dates d’effet sur des personnels et sur des UFs

#### Reporting

Le logiciel doit permettre d’effectuer des reportings d’accès : volume, profil…

#### Historique

Le logiciel doit permettre d’accéder à l’historique des passages à un UTL ou d’un badge.

### Procédures critiques : modes dégradés, plan de continuité de l’activité et plan de reprise de l’activité

Le titulaire détaille comment sa solution permet :

* D’assurer la continuité du service. Le titulaire détaille dans son mémoire technique les conséquences organisationnelles pour la gestion des accès
* D’éviter la perte de données, en définissant les modes opératoires ainsi que la reprise des données après rétablissement des services, dans le cas de dysfonctionnements suivants :
  + Arrêt du serveur,
  + Indisponibilité du réseau,
  + Coupure des interfaces (détail des procédures dégradées par interface),
  + Panne informatique autre

Afin d'éviter la perte de données de l'application et l’indisponibilité de sa solution, le titulaire, en concertation avec le CHU, prévoira le temps nécessaire à l’élaboration des procédures détaillées, des modes dégradés ainsi que les plans de continuité et de reprise d’activité de sa solution.

Les UTLs devront pouvoir fonctionner en autonomie en cas de panne et devront pouvoir échanger l’historique et les paramétrages avec le serveur dès le rétablissement.

Les UTLs doivent pouvoir être administrables par les protocoles :

* SSH
* HTTPS
* TelNet

### Reprise des données

Le titulaire détaille comment sa solution permet :

* La reprise des données existantes
* Le plan de migration prévu (si la migration est par lot ou en masse) avec une estimation de la charge afin de minimiser l’indisponibilité du service.
* La vérification des données

## Interfaces

### Flux structure

Le logiciel de gestion des accès doit reposer sur les référentiels des établissements constitués :

* Des structures et nomenclatures de l’Établissement, géographiques, de coût, de responsabilité médicale
* De l’ensemble des annuaires et référentiels

Le soumissionnaire décrira comment il envisage la communication avec les référentiels de structure et quelles en sont les limitations.

Au CHU de Toulouse,

* Le logiciel de gestion des structures est GDR Structures.
* L’export de la structure et des référentiels est fait de manière automatique quotidiennement
* Les données sont alors envoyées aux applications cibles, selon leurs capacités à réceptionner les informations aux formats suivants :
  + HL7 MFN (soit MLLP, soit dépôt de fichier) lorsque la donnée se prête à un tel format
  + XML en dépôt de fichier
* Les échanges se font via l’EAI (Cloverleaf) ou via une plateforme FHIR

### Flux avec le système gestion administrative RH

Le logiciel de gestion des accès doit reposer sur le référentiel RH mis en place actuellement. Une interface quotidienne est mise en place pour récupérer les informations administratives RH.

Au CHU de Toulouse,

* Le flux RH provient de l’application AGIRH édité par le MIPIH
* L’EAI produira deux types de fichiers : Un fichier comportant les données et un autre du même nom mais avec extension « . ok ».
* Les échanges se font via l’EAI (Cloverleaf) ou via une plateforme FHIR

## Description du contexte technique

### Attentes et contraintes techniques

#### Hébergement

L’application sera installée sur l’infrastructure du CHU. Le titulaire devra décrire l’architecture préconisée. L’annexe infrastructure détaille les standards infrastructure du CHU. Les serveurs doivent correspondent à la norme ISO 27001 dans une bulle dédiée.

#### Accessibilité

L’application doit être accessible par des utilisateurs répartis sur des pôles et lieux distants, idéalement via un client léger. Ce client doit pouvoir être déployer par notre outil de gestion des applications poste de travail SCCM et idéalement via du packaging.

#### Ergonomie

Il convient que l’outil offre une interface ergonomique et intuitive.

La solution doit fonctionner sur tout type d’écran et conforme au standard.

#### Disponibilité

L’application doit être disponible 24h/24h., 7j/7, et dans le respect des GTI /GTR définies ci-dessous.

L’application doit être disponible avec un taux minimum de 95 % d’utilisation sur une plage de 24h. Le prestataire précise les conditions concernant les opérations de maintenance du service.

Le taux de disponibilité est mesuré sur une période « glissante » d’une (1) année et par rapport à la somme de toutes les durées d’interruption constatée dans la période de mesure.

#### Sécurité des données

L’annexe SSI (clausier SSI) permettra au titulaire de détailler sa politique de sécurité des systèmes d’information.

L’ensemble des transactions entre les différents systèmes doit être sécurisées. Le titulaire doit fournir ses préconisations et s’assurer qu’aucunes données ne peut être déchiffrées en dehors des applications du système. Il devra préciser les protocoles utilisés et vérifier au cadre réglementaire (ANSSI,RGPD,etc.…)

#### Cloisonnement des données

Le prestataire doit assurer le cloisonnement des données entre ses différents clients utilisant le même système. Il doit décrire la façon dont ce cloisonnement est réalisé et détailler la politique de sécurité des données dans son système.

Le CHU demande la mise en place à minima de deux bases pour deux environnements différents :

* Production,
* Test

#### Bases de données

L'utilisation d'une base de données non propriétaire de l’éditeur est préférable.

Au CHU de Toulouse, les SGBD utilisés sont :

* SQL Server
* MariaDB
* PostgreSQL
* MySQL

Le titulaire devra détailler l’architecture de la base de données afin de permettre à l’équipe de l’exploitation le maintien en condition opérationnel.

La base de données doit permettre aux équipes de pouvoir intervenir sans blocage de la part de l’éditeur. Le prestataire fournira une documentation détaillée sur les différents aspects mis en place.

La base de données doit pouvoir être auditable dans le cadre des audits internes.

#### Performances

L’application doit fonctionner, avec des temps de réponse inférieurs à 2 secondes en moyenne.

Le prestataire indique les moyens mis en place et les garanties qu’il donne en matière de performance pour faire face à une volumétrie importante. Il doit pouvoir garantir des performances toujours constantes dans le choix de son infrastructure.

Le niveau de performance de la solution doit être mesuré et doit être communiqué trimestriellement dans un rapport sur les résultats obtenus.

#### Supervision

L’application doit pouvoir remonter des alertes sur des comportements anormaux (négligences humaines, accès interdit).

### Attentes applicatives

L’architecture applicative doit être évolutive et respecter les standards du marché. Elle doit être compatible avec les principaux systèmes de gestion de base de données relationnelle (SGBD) du marché et s’appuyer sur les nouvelles technologies et les principaux standards d’interopérabilités (HTTP, XML, etc.…).

La solution doit également rester compatible avec les évolutions régulières des composants d’infrastructure technique (patch, service pack, version...) et également les futures montées de versions ne doivent pas compromettre les fonctionnalités déjà existantes.

## Organisation du pilotage INFORMATIQUE

### Les acteurs du pilotage

#### Equipe du titulaire

Le titulaire doit désigner un directeur de projet ou un chef de projet comme étant l’interlocuteur unique pour le CHU de Toulouse. Il doit proposer une équipe adaptée au contexte et aux structures mises en place par le CHU de Toulouse et décrites ci-après et doit mettre en œuvre l’organisation et les moyens nécessaires pour mener à bien le projet.

La mission du directeur de projet ou chef de projet du titulaire est :

* D’assurer l’interface entre ses équipes et les représentants de la maitrise d’ouvrage, lors des comités de pilotage, des réunions d’avancement, des vérifications, ainsi qu’à l’occasion de toutes les réunions ponctuelles pour lesquelles le CHU de Toulouse jugerait sa présence nécessaire
* De veiller au bon déroulement du projet et à la bonne exécution des travaux

Le titulaire assure un accompagnement sur toute la période de mise en œuvre, avec déploiement dans un premier temps sur un site pilote servant de plateforme test, ajustement, puis déploiement sur les autres sites.

#### D.S.N. (Direction des Services Numériques)

La Direction des Services Numériques du CHU de Toulouse s’appuie sur une organisation ITIL.

La stratégie du Système d’Information est en étroite collaboration avec le centre d’expertise et de compétences médico soignant pour le numérique de la DSN et les directions fonctionnelles et de pôle du CHU.

La gestion des données du SI et l’alimentation du Big Data sont pilotés par le service Données de la DSN.

Les études et la mise en œuvre des nouvelles solutions sont pilotées par le Centre de Solution et expertise.

Les architectes applicatifs sont en charge du pilotage du contrat, aux côtés du responsable contractuel de la Direction des Achats.

Le suivi de la production est piloté par le Centre des Opérations. Des administrateurs applicatifs mettent en œuvre ce pilotage pour le domaine Dossier Patient Informatisé.

Le responsable MOE désigné au sein de la DSN estl’architecte du domaine.

#### Direction des achats

La direction des achats porte l’élaboration du contrat en cohérence avec les exigences techniques et fonctionnelles.

**L’acheteur** est le référent contractuel de la maitrise d’œuvre et de la maîtrise d’ouvrage et assure le suivi commercial du projet.

#### La maîtrise d’ouvrage

La maîtrise d’ouvrage représente le métier utilisateur de la solution applicative. Il participe au pilotage du contrat.

A ce titre, elle spécifie les exigences fonctionnelles à tous les stades du projet depuis l’élaboration du cahier des charges jusqu’à la recette fonctionnelle. Elle prend en compte les exigences d’utilisation opérationnelles des sites.

### Le pilotage du contrat

Tous les comités sont organisés dans les locaux du CHU ou en visioconférence.

La date de chaque comité est établie en concertation entre le titulaire et le CHU au moins un mois à l’avance. L’ordre du jour est fixé par le CHU (hors comité opérationnel hebdomadaire).

Le titulaire fournit aux participants un document de préparation au comité par courriel au moins 7 jours ouvrés avant la réunion (hors comité opérationnel hebdomadaire).

Un projet de compte-rendu du comité de pilotage, rédigé par le titulaire, est adressé aux participants dans les cinq jours consécutifs au comité par courriel. Le CHU doit retourner le document validé dans un délai de 15 jours. À défaut de réponse, le compte-rendu est réputé approuvé par le CHU.

#### Le comité de pilotage

Le comité de pilotage, pilote l’exécution du contrat établi entre le titulaire et le pouvoir adjudicateur au sens métier (MOA)

Il effectue de manière trimestrielle le bilan de la période écoulée et valide les engagements pour la période à venir pour :

* La mise en œuvre des projets : Il suit et vérifie la mise en œuvre des phases de déploiement. Il arbitre les décisions nécessaires au déroulé des projets. Il valide les étapes contractuelles des projets.
* L’exécution du support : suivi des indicateurs de qualité et de respect des objectifs.

Il est composé de :

* De la Direction Patrimoine et Constructions
* De la Direction des Achats représentée par l’acheteur
* De la Direction des Systèmes Numériques
* Des différentes directions parties prenantes au projet
* Du chef de projet du titulaire

#### Le comité de suivi SI (mensuel)

Le Comité de suivi SI, l’exécution du contrat établi entre le titulaire et le pouvoir adjudicateur au sens maîtrise d’œuvre. Il se réunit 1 fois par mois.

Il assure plus particulièrement le pilotage et le suivi détaillé de l’activité sous la forme d’une revue des projets, du support et des performances, et le pilotage financier du contrat.

Le Titulaire effectue un bilan du mois écoulé sur la mise en œuvre de l’ensemble des projets et chantiers du domaine : plan de charges, planning des différents chantiers, gestion des risques.

Le Titulaire présente un état des réceptions validées depuis le précédent Comité et une projection des vérifications à réaliser dans la période à venir.

Le titulaire communiquera lors de ce Comité toute mise à jour de l’organigramme fonctionnel associé à l’exécution des prestations et permettant l’identification de l’ensemble des contacts, ceux désignés au titre du processus d’escalade compris.

Le Comité de suivi SI est composé de :

* De la Direction des Systèmes Numériques représentée le chef de projet SI et différents représentants de la DSN en fonction des besoins
* Du chef de projet du titulaire
* D’un représentant de la maitrise d’ouvrage

### Méthodologie projet

Chaque acquisition et mise en œuvre de nouveau module, solution ou interface sera réalisée dans le respect du processus projet CHU et fera l’objet d’un bon de commande établi sur un devis, ou d’un marché subséquent.

Les validations du lancement des différentes étapes seront formalisées dans le cadre des comités de pilotages.

L’opportunité du projet est évaluée par simple qualification ou lors d’une phase de pré-étude.

La particularité du CHU de Toulouse est la répartition des pôles d’activité en Multi site tel que décrit dans le cahier des charges (partie 2.1)

Ceci entraine des pratiques et des spécificités très diverses au sein des pôles et des sites en termes d’activité programmée et non programmée.

Nous souhaitons être accompagné de manière identique pour chaque phase déclinée dans la partie 2.1.

Chaque projet est décomposé en plusieurs phases :

* Phase d’étude/cadrage
* Phase de réalisation/conception
* Phase de déploiement.

Les décisions de mise en œuvre des phases successives d’un projet sont établies par le Bureau d’Instruction des Projets du CHU de Toulouse.

Le suivi détaillé de l’avancement au cours de chaque phase sera réalisé lors des comités opérationnels hebdomadaires.

Dans ce cadre, il est demandé au titulaire de détailler sa méthodologie projet et de décrire l’accompagnement proposé au cours des différentes phases de projet.

A minima les étapes suivantes doivent être positionnées dans le calendrier de démarrage produit par le prestataire :

* Audit préalable
* Installation
* Paramétrage
* Mise en place des interfaces
* Formation des différents utilisateurs
* Accompagnement au déploiement

#### Phase Etude d’opportunité

Chaque acquisition de module ou de fonctionnalité régie par licence sera évaluée par une phase d’étude d’opportunité ayant pour objectif une décision d’opportunité, formalisant le GO de lancement de la phase d’étude de mise en œuvre.

Le module ou la fonctionnalité sera mis à disposition sur un environnement « de bac à sable » fourni par le CHU de Toulouse. La licence sera fournie à titre gracieux et ne pourra excéder une durée convenue préalablement entre les parties. Les prestations nécessaires à la mise en œuvre feront l’objet d’un devis et l’objet d’une commande.

Cette phase a pour objectif l’évaluation d’opportunité d’un projet. Elle prend fin avec la décision prise par le Bureau d’Instruction des Projets (BIP Etude).

#### Phases d’étude.

Cette phase démarre suite à une validation d’opportunité en Bureau d’Instruction des Projets (BIP d’Etude), elle permet le lancement de la phase d’’étude, avant la réalisation d’un projet.

Cette phase a pour objectif la constitution du dossier d’étude technique et fonctionnel, l’étude de sécurité, d’urbanisation et des modalités de mise en œuvre.

Sont également formalisés dans le dossier d’étude :

* Le planning du projet et sa gouvernance,
* L’évaluation des ressources humaines et financières nécessaires à la réalisation, le déploiement,
* L’impact sur le maintien en condition opérationnelle de la solution.

Dans le cadre de l’étude, le Titulaire devra fournir l’ensemble des éléments techniques, fonctionnels, sécurité, juridiques et financiers nécessaires à la constitution du dossier d’étude.

La contractualisation d’une étude sera réalisée par bon de commande.

La phase d’étude s’achève suite à un avis favorable du Bureau d’Instruction des Projets (BIP de réalisation), formalisant la validation du lancement de la phase de réalisation du projet.

Le Bureau d’Instruction des Projets peut demander une étude complémentaire, nécessitant des éléments complémentaires du Titulaire, s’il juge le dossier d’étude incomplet. L’étude complémentaire pourra faire l’objet d’une commande, en accord entre les Parties.

Les prestations nécessaires à l’étude font l’objet d’une commande.

#### Phase de réalisation.

La phase de réalisation comprend la contractualisation, le lancement et la mise en œuvre du projet.

La contractualisation du projet sera réalisée par bon de commande.

Le lancement est officialisé par une réunion de lancement. Le pilotage du projet est réalisé par un chef de projet ou un architecte.

La mise en œuvre de la solution applicative est réalisée sur les différents environnements. Elle comprend l’installation, le paramétrage, les tests, la préparation de la mise en production et les formations.

La décision technique de passage en production est instruite par le Comité de Release Management. **Le Comité de Release Management** sera programmé à minima 6 semaines avant le démarrage en production.

Le titulaire devra fournir l’ensemble des éléments nécessaires à la constitution des livrables attendus par le Comité de Release Management : le dossier d’architecture, le dossier sécurité, la documentation d’administration et d’exploitation de la solution.

L’ensemble des dossiers devront être finalisés et validés lors du Comité de Release Management pour un démarrage en production.

#### Phase de déploiement.

Le déploiement démarre à la date de mise en production sous condition d’avis favorable du Comité de Release Management et du Comité de pilotage du projet

La phase de déploiement se termine par la réunion de clôture du projet.

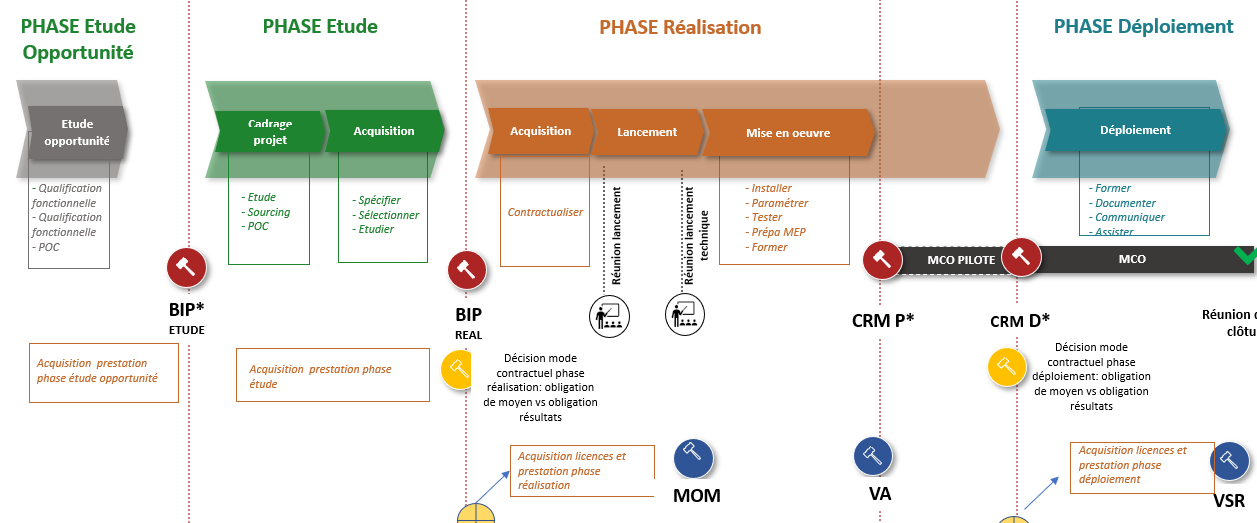
### Vérifications

Les vérifications sont effectuées aux étapes suivantes :

* ***MOM (Mise en ordre de Marche)***

Les vérifications suivantes sont effectuées :

* La réunion de lancement du projet a été effectuée
* La solution est livrée sur un environnement de tests et est opérationnelle pour effectuer les tâches de réalisation
* La documentation nécessaire à la phase de réalisation est livrée
* La réunion de lancement technique, initialisant la mise en œuvre de la solution est réalisée



* ***VA Vérification d’Aptitude***

Les vérifications suivantes sont effectuées :

* Le Comité de Release Management a émis un avis favorable pour le passage en production de la solution
* La documentation nécessaire au passage en production a été livrée
* Le démarrage en production est effectif.
* ***VSR (Vérification Service Régulier)***

Les vérifications sont effectuées en amont de la réunion de clôture du projet. La décision de VSR est formalisée dans la réunion de clôture du projet.

Les vérifications seront effectuées au plus tard 2 mois après la VA. Les résultats sont formalisés. En cas de réserve bloquante ou majeur, la signature de la VSR est ajournée. Le titulaire présentera un plan d’actions avec échéances de résolution. De nouvelles vérifications seront effectuées après livraison des corrections. La VSR sera signée lorsque l’intégralité des réserves seront levées.

## Organisation du support et attentes

### Plan d’assurance qualité

Un projet de plan d’assurance qualité est fourni à l’appui de l’offre technique du titulaire. Ce plan précise les buts et engagements du titulaire en termes de finalité et d'objectifs, assortis d'indicateurs. Il présente comment la prestation proposée s'inscrit dans la démarche qualité de la direction des services numériques du CHU. Ensuite, le PAQ proposé par le Titulaire sera discuté lors du 1er comité de suivi et réactualisé à la date anniversaire du début de marché. Ce PAQ présente les instances de contrôle mises en place, l'organisation déployée pour le suivi du projet, les processus, procédures et modes opératoires pour la réalisation des prestations ainsi que le mode de gestion documentaire et de modification du PAQ. Il expose tous les moyens matériels, humains et méthodologiques mis en œuvre par le titulaire pour répondre aux attentes du pouvoir adjudicateur quant à la qualité des prestations.

### Maintenance et services d’assistance

Dans le cadre de la maintenance, le titulaire assure pendant la durée du marché :

* La maintenance préventive (Services Managés):

Il s’agit des actions de maintenance visant à éviter un dysfonctionnement dans la solution logicielle.

Le Titulaire s’engage à répondre aux demandes de validation spécifiques des mises à jour OS, Systèmes du CHU requise supportant la solution délivrée sur l’ensemble des environnements, dans un souci de sécurité et robustesse du SIH

* La maintenance corrective :

Il s’agit des actions de maintenance visant à résoudre un dysfonctionnement apparu dans la solution logicielle.

* La maintenance adaptative :

Il s’agit d’une action de maintenance due à la nécessité de s’adapter à une évolution externe à la solution logicielle elle-même, comme une modification de la version d’un Système d’Exploitation ou un changement de Système d’exploitation, en garantissant le besoin métier en termes de performance/sécurité et périmètre fonctionnel.

Le Titulaire informe le Bénéficiaire des prérequis techniques, notamment la compatibilité entre les versions applicatives et versions des Systèmes d’exploitation, la portabilité vers de nouvelles technologies six (6) mois avant le lancement d’une version.

* La maintenance réglementaire

La Maintenance Réglementaire porte sur la fourniture de Versions et de Correctifs du Progiciel portant sur des dispositions législatives et réglementaires :

i) Présentant un caractère impératif

ii) Lorsque les modalités d’application sont totalement et précisément définies et applicables à l’ensemble des Clients relevant de la même activité

* La maintenance évolutive :

Au titre de la maintenance évolutive, le Titulaire s’engage à informer le bénéficiaire, six (6) mois avant le lancement d’une nouvelle version fonctionnelle. L'information est communiquée par voie électronique.

Le titulaire s’engage à fournir 3 mois avant le lancement :

* Les notes de mise à jour de l'application qui sont disponibles sur le site web du Titulaire.
* La documentation administrateur et la documentation utilisateur qui sont disponibles sur le site web du Titulaire.
* Toute information disponible propre à évaluer l’impact de la nouvelle version.
* Les préconisations au sujet des **prérequis** (matériels, logiciels et infrastructure) nécessaires à l’installation des nouvelles versions.

Le Titulaire informe le Bénéficiaire des prévisions de disponibilité de toutes les nouvelles versions des logiciels dès leurs incorporations dans son Plan Produit désignant une représentation graphique séquencée dans le temps permettant de communiquer aux Bénéficiaire l'intention stratégique du Titulaire sur sa gamme de produits et les fonctionnalités additionnelles des Logiciels.

Les demandes d’évolution seront réalisées et suivies suivant les modalités décrites dans l’offre du titulaire.

Le Pouvoir Adjudicateur participera au club utilisateur, lorsqu’il existe, pour porter ses demandes d’évolutions et participer aux arbitrages de priorisations des demandes avec les autres sites utilisateurs selon les modalités décrites dans l’offre du titulaire

#### Exercice du support

Le Titulaire s'engage à assurer, tant que l’établissement n'a pas notifié sa décision de résiliation, un service de support.

Les modalités techniques du support sont décrites dans l’annexe 9 – Modalités d’accès au support.

Toute modification des modalités d’accès au support devra être communiquée par le titulaire à minima 1 mois avant sa mise en application.

Cette prestation est concrétisée par la mise à disposition de l’établissement d’un service de support destiné à lui fournir les solutions ou corrections relatives à un éventuel dysfonctionnement de la solution.

L’établissement après avoir informé le Titulaire de l’existence d’une anomalie de fonctionnement, lui fournira tous les éléments en sa possession de nature à décrire le problème constaté.

Le Titulaire pourra demander à l’établissement d’effectuer des opérations permettant de compléter la description de l’incident.

Toutefois, en cas de dysfonctionnement bloquant, quand un problème n'est pas identifié ou qu'il reste non résolu après que l’établissement a exécuté les actions décrites dans la documentation fournie par le Titulaire et celles prescrites par le centre de support du Titulaire, le Titulaire se réserve la possibilité de classer l’établissement en tant que « site prioritaire » et d’affecter à ce titre un dispositif dédié à la résolution du dysfonctionnement ou le reclassement de ce dysfonctionnement à un niveau inférieur.

Dans cette hypothèse, le Titulaire fournira à l’établissement, une correction temporaire à ce problème ou une suggestion pour le contourner et/ou une correction définitive ou une prévision concernant la disponibilité de cette correction.

Le Titulaire pourra aussi proposer à l’établissement l’installation d’un état technique comportant la solution au dysfonctionnement rencontré.

Cette correction ou cet état technique sera ensuite inclus dans une mise à niveau du progiciel qui sera fournie à l’établissement dans le cadre du suivi.

Dans le cadre du support matériel et logiciel, le titulaire met à disposition à l’établissement gratuitement la documentation nécessaire.

Afin de diminuer les actions de maintenance corrective des matériels et du progiciel le titulaire effectue au titre de la prestation forfaitaire de suivi support une maintenance préventive des installations de l’établissement.

* ***Modalités de Support***

Les prestations de support ont pour but de maintenir de façon constante le logiciel objet du marché au niveau des performances dans les propositions et notices publiées de l’éditeur. Le Titulaire s'engage à assurer un service de maintenance dont les modalités sont décrites dans son offre.

Dans l’hypothèse où le pouvoir adjudicateur a retenu l’offre de base (acquisition du logiciel et hébergement dans l’établissement), la maintenance prend effet à l’issue de la garantie d’un an. La garantie s’applique à partir de la date d’effet de la décision de réception relative à toute acquisition relevant du présent marché.

Le titulaire décrit dans le mémoire technique les modalités de contact ainsi que les plages horaires et journalières ouvrées. Il précise selon quelles modalités un établissement peut accéder au suivi de ses tickets ainsi que ceux des autres établissements.

D’éventuelles modifications de celui-ci peuvent être demandées au Titulaire en accord avec les exigences définies au Titulaire.

#### Définitions des différents niveaux de dysfonctionnement

Un incident est qualifié en prenant en compte les éléments suivants :

Incident Critique : Interruption complète d'un service, d'un système, du réseau, d'une application ou d'un élément de configuration identifié comme critique.

Incident Elevé : S'applique lorsque le service, le système, le réseau, l'application ou l'élément de configuration peut procéder mais dont la performance est considérablement réduite et/ou les fonctionnalités sont très limitées.

Incident Important : Un événement qui provoque la perte minime d'un service. Une solution permanente ou de contournement est disponible pour restaurer la fonctionnalité du service.

Incident Modéré : Un événement constituant un dérangement pour l'utilisateur, pour lequel il existe une alternative ou une réparation possible mais qui n'empêche en rien l'utilisateur de travailler.

Incident Bas : Un dysfonctionnement ou une anomalie mineure(e) relevé(e) par un utilisateur, sans que cela n’ait le moindre impact sur son travail.

La qualification de l’Incident est effectuée en premier lieu par le Bénéficiaire. Le Titulaire dispose d’un droit de contestation dans la qualification d’un Incident.

Au cours de cet échange, le Bénéficiaire et le Titulaire s’efforcent de trouver une qualification commune.

La contestation de la qualification est motivée et documentée par le Titulaire dans son Outil de gestion d’Incidents.

Le Titulaire dispose d’un délai d’un (1) mois pour contester à compter de la création du ticket. La contestation fait l’objet d’une discussion dans le cadre du Comité de pilotage à venir.

En cas de contestation, le Titulaire reste tenu d’appliquer les délais de résolution tels que définis par la qualification du Bénéficiaire.

Par garantie du temps d’intervention, il est entendu le délai durant lequel le Titulaire, alerté par le Bénéficiaire, prend connaissance de l’incident et entame des mesures de diagnostic. Ce délai prend effet :

* Si l’incident est signalé pendant les horaires du contrat souscrit, le délai prend effet à la date et heure de création du ticket dans l’Outil de gestion des Incidents ou du mail de déclaration d’incident
* Si l’incident est signalé en dehors des horaires du contrat souscrit, le délai prend effet dès le début de la plage de support souscrit. Le Titulaire devra permettre au Bénéficiaire d’ouvrir un incident sur le portail dédié en indiquant l’impact dans les champs adéquats, ce qui permettra le calcul de la priorité de celui-ci avec les engagements de service requis (cf. table ci-dessous).

|  |  |  |
| --- | --- | --- |
| **Type incident** | **GTI** | **GTR** |
| 1 - critique | 1h. | 8h |
| 2 - important | 2h | 32h |
| 3 - modéré | 2j | 10 j |
| 4 - bas | 10j | Prochaine version.  Délais de résolution à préciser dans les 30 jours maximum suivant la création du ticket |

|  |  |  |
| --- | --- | --- |
| PRIORITE | NOM | DEFINITION |
| P1 | Critique | Interruption complète d'un service, d'un système, du réseau, d'une application ou d'un élément de configuration identifié comme critique. |
| P2 | Important | Un événement qui provoque la perte minime d'un service. Une solution permanente ou de contournement est disponible pour restaurer la fonctionnalité du service. |
| P3 | Modéré | Un événement constituant un dérangement pour l'utilisateur, pour lequel il existe une alternative ou une réparation possible mais qui n'empêche en rien l'utilisateur de travailler. |
| P4 | Basse | Un dysfonctionnement ou une anomalie mineure relevé(e) par un utilisateur, sans que cela n’ait le moindre impact sur son travail. |

Les exigences minimales de prise en compte globale et traitement des incidents ainsi que les pénalités associées sont détaillées dans le CCAP.

|  |  |  |
| --- | --- | --- |
| **Type incident** | **Exigence minimale de prise en compte globale** | **Exigence minimale de niveau de résolution** |
| 1 - critique | **98%** en moins de 2h | **98%** en moins de 16 heures |
| 2 - important | **80%** en moins de 8h | **80%** en moins de 4j |
| 3 - modéré | **70%** en moins de 10j | **70%** en moins de 30j |
| 4 - bas | **50%** | Sans objet |

* ***Problèmes et gestion de crise***

Le Titulaire doit décrire dans son mémoire technique, les modalités de gestion des problèmes, le processus d’escalade des incidents et de gestion de crise.

#### Evolution du système de la solution logicielle



##### Etats techniques

Le Titulaire se réserve la possibilité de créer des états techniques intermédiaires entre deux mises à niveaux du logiciel, états comportant la correction de bogues ou d’anomalies de fonctionnement, et de fournir dans le cadre de la maintenance, la mise à disposition de ces états techniques à l’établissement qui rencontrerait ces bogues ou ces anomalies lors de l’utilisation du logiciel.

Les évolutions introduites avec ces états techniques sont ensuite inclues dans la prochaine mise à niveau du progiciel.

##### Mise à niveau

Le Titulaire mettra à la disposition à l’établissement des mises à niveau de la solution comportant notamment les corrections d’erreurs ou bogues observées sur le niveau précédent de la solution et ayant été éventuellement inclues dans des états techniques intermédiaires.

La fourniture de ces mises à niveau fait partie intégrante du service de maintenance. Le Titulaire informera au plus tôt l’établissement de la disponibilité prochaine d’une mise à niveau.

Le Titulaire assure au titre de la maintenance l’adaptation de la solution aux nouvelles versions éventuelles du logiciel d’exploitation des PC, serveurs, PDA et du Système de gestion de base de données aussi longtemps que cette adaptation est techniquement réalisable et que la compatibilité ascendante des versions successives du logiciel d’exploitation et du SGBD est assurée par le constructeur du matériel utilisé par le Pouvoir Adjudicateur.

##### Nouvelles versions

L'enrichissement de la solution du Titulaire par l'édition de nouvelles versions dites majeures, rentre dans le cadre du suivi de la solution. Le Titulaire se réserve le droit de commercialiser séparément certains ajouts fonctionnels à la solution, soit sous forme de module additionnel, soit sous forme de produit séparé. Les fonctionnalités déjà incluses dans le périmètre de la solution acquise ne pourront être objets d’une commercialisation additionnelle, liée à leur évolution.

L’établissement aura la possibilité de différer ou refuser la mise en œuvre de cette nouvelle version, afin de prendre toutes dispositions en vue de régler la question d’une éventuelle incompatibilité avec d’autres applications.

Lors de versions majeures, le CHU pourra demander la présence physique sur site d’un support à la mise en place de version afin d’améliorer la réponse aux éventuels problèmes générés, dont les frais résultants de cette intervention seront à la charge du CHU.

Le Titulaire s’engage à assurer le suivi de la version N de la solution commercialisée.

Le Titulaire s’engage à assurer le suivi de la version N-1 de la solution commercialisée pendant au moins 12 mois à compter de la commercialisation d’une nouvelle version. La montée en version pourra être refusée par l’établissement en cas de régression ou d’évolution contradictoire avec l’organisation en place. Si une régression est constatée en version supérieure, le titulaire s’engage à maintenir la version utilisée par l’établissement dans l’attente de la correction des régressions constatées.

Le Titulaire s’engage à informer l’établissement du cycle de vie des versions du logiciel.

La correction des dysfonctionnements est assurée sur le dernier service pack de la dernière version commercialisée. Cependant, le Titulaire s’engage à fournir les correctifs des incidents bloquants et majeurs sur la version commercialisée N-1 pendant les 12 mois à compter de la commercialisation de la dernière version commercialisée.

#### Exclusion de la maintenance

Le service ne comprend pas les prestations suivantes qui pourront faire l'objet d'une facturation :

* Intervention à la suite d’une utilisation de la solution s’appuyant sur des systèmes progiciels sous-jacents qui ne seraient plus maintenus par leur fournisseur. Cette réserve s’applique en particulier au système d’exploitation du matériel d’utilisation et aux modules progiciels qui lui sont associés,
* La Maintenance ne comprend pas la remise en état du Logiciel et/ou logiciel Tiers vétuste. La vétusté logicielle s’étend à tout Logiciel ne faisant plus l’objet de mise à jour évolutive et/ou de mise à jour corrective de la part de son éditeur. La non-conformité ou l’état du Système Opératoire peuvent engendrer un mauvais fonctionnement de la configuration et/ou du Logiciel et/ou Logiciel Tiers et de fait, rendant sa maintenance impossible.

Si le Bénéficiaire décide de ne pas faire procéder à ses frais à la remise en état proposée par le Titulaire, le Logiciel concerné sera soustrait du Contrat et ce, sans préavis.

* Correction de problèmes causés par une utilisation inadaptée du système ou par négligence,
* Régénération de la solution consécutive à des erreurs non imputables au Titulaire,
* Adaptation de la solution fournie par d'autres fournisseurs que le Titulaire,
* Développement de modifications à la demande de l’établissement susceptibles d'altérer les fonctions de la solution,
* Intervention sur un progiciel modifié à l'initiative de l’établissement, et sans l'accord du Titulaire,
* Intervention à la suite d’une perturbation imputable à une autre application de l’établissement,
* Intervention à la suite d’un mauvais fonctionnement de l’environnement d’utilisation,
* La fourniture ou l'échange d'accessoires, fournitures ou consommables tels que définis par le Constructeur,
* La mise en place, le contrôle et le maintien de l'environnement physique de l'installation,
* Les opérations d’installation des Versions mineures et majeures, des Service Update et des Hotfixes,
* L’assistance sur les Systèmes opératoires ne figurant pas dans le BP,
* La mise en œuvre de procédures régulières prévues, comme par exemple la mise en œuvre de requêtes, mises à jour des outils d’habilitation, etc.
* Le paramétrage RIS dans le cadre de changement (CCAM ou autre paramètre indépendant de Titulaire).

De même la responsabilité du Titulaire ne pourra être recherchée dans les cas suivants :

* Si le mauvais fonctionnement de la solution résulte du matériel ou de l'utilisation de données, de progiciels non fournis par le Titulaire ou de l'application ou de la mise en œuvre de procédures erronées par le personnel de l’établissement ou par toute personne agissant pour son compte,
* À la suite d'une intervention non autorisée par le Titulaire et effectuée par l’établissement et/ou par un tiers,
* À la suite d'une erreur de manipulation ou d'une utilisation non conforme à la documentation ou non conforme aux instructions communiquées par le Titulaire,
* En cas d'erreur générée par un autre progiciel non fourni par le Titulaire,
* Cyberattaque du système d’information du Client impactant l’écosystème supportant la solution de Titulaire (infection virale, ransomware, intrusion logique externe, etc.),
* Accidents, incendies, dégâts des eaux, orages, émeutes, action des pouvoirs publics ou militaires,
* Dommages causés directement ou indirectement ou par suite d’une catastrophe nucléaire,
* Dispositifs non couverts par le présent Marché et raccordés au Logiciel, Logiciel Tiers et/ou Matériel (les lignes de transmission des réseaux, les ordinateurs et autres produits associés),
* Les travaux de connexion électrique ou au réseau téléphonique,
* Le déménagement ou le déplacement du Logiciel, Logiciel Tiers et/ou Matériel ainsi que sa remise en ordre de marche ou son contrôle,
* Les opérations de sauvegarde du Logiciel, Logiciel Tiers et autres données ou informations, y compris celles générées par le logiciel.

#### Suivi pour évolution du système d'exploitation

Le suivi s'entend par la mise à niveau technique de la solution concédée par le Titulaire suite aux évolutions des systèmes d'exploitation si le constructeur assure la compatibilité ascendante.

#### Collaboration/ obligations des parties

Si au cours de la prestation de maintenance une difficulté apparaissait, l’obligation de collaboration des parties les engage à alerter l’autre partie dans les meilleurs délais et à se concerter pour mettre en place une solution adaptée.

D’un commun accord les parties conviennent que le titulaire est soumis à une obligation de moyens dans l’exécution de ses prestations, sauf en ce qui concerne l’engagement du respect des délais d’intervention en cas d’indisponibilité du progiciel qui relèvent d’une obligation de résultat.

**Registre des incidents :** L’établissement assurera la tenue d’un registre des incidents.

Il sera fourni par le Titulaire (livrable), un rapport d’activité semestriel afin de suivre les interventions de tous types et quels que soient les prescripteurs.

### Documentation

La documentation de la solution logicielle, en langue française, doit comporter :

* 1 volet « administration » : Exploitation
* 1 volet « fonctionnel »
* 1 volet « technique » : Installation/équipements-matériels

### Formation

Le titulaire prend en charge la formation des administrateurs et le cas échéant de services pilotes.

Pour chaque formation dispensée par le titulaire, il est indiqué à minima :

* Le public concerné et le nombre de personnes admises par session de formation,
* La durée,
* Le programme.

L’établissement prend en charge l’organisation des séances de formation dans ses locaux (réservation des locaux, informations des utilisateurs) ainsi que l’inscription des stagiaires aux séances de formation et la convocation des stagiaires.

Le titulaire fournit un support de formation à l’établissement qui a le droit d’effectuer des reproductions à l’attention de stagiaires qu’il forme lui-même.

Les séances de formation sont prévues pour un maximum de *10 personnes*.

En vue du déploiement de la solution, le besoin de formation concerne :

* *Formation administrateurs techniques : 5 personnes,*
* *Formation administrateurs fonctionnels : 5 personnes,*
* *Formation utilisateurs du service pilote, le cas échéant : 20 personnes.*

Livrables attendus :

* Support de formation administrateur et utilisateur de base,
* Feuilles de présence,
* Enquêtes de satisfaction.

**Les frais de déplacement et d’hébergement font partie intégrante du coût de la prestation de formation.**

## Conditions de droit d’usage du logiciel

### Plateforme de test

Dans le cadre de validation de modules additionnels ou de nouvelles versions, le logiciel ainsi que l’ensemble des modules et interfaces maintenus sera installé par le Titulaire sur une plate-forme fournie par le Pouvoir Adjudicateur.

Cette plate-forme présentera les caractéristiques minimales permettant une utilisation :

* De l’ensemble des modules maintenus,
* De l’ensemble des interfaces maintenues,
* Par 10% maximum des utilisateurs de la plate-forme de production.

La maintenance du logiciel présent sur cette plate-forme ainsi que les mises à jour du logiciel vis-à-vis de la plateforme de production sont à la charge du Titulaire.

### Evolution des équipements

Le Pouvoir Adjudicateur se réserve la faculté de changer l'équipement (ordinateur ou système général d'exploitation) sur lequel le logiciel opère. Si la version en cours s’avère incompatible avec ce changement, le titulaire s’engage à fournir une nouvelle version compatible, dont les frais et prestations afférents seront facturés en sus après acceptation d’une proposition commerciale du titulaire par le CHU

Si le Titulaire ne dispose pas d'une version appropriée au nouvel équipement, il s'engage à négocier avec le Pouvoir Adjudicateur les conditions de développement d'une telle version dont les frais et les prestations afférents seront facturés en sus après acceptation d’une proposition commerciale du titulaire par le CHU

Dans le cas où le Pouvoir Adjudicateur transférerait son matériel dans un autre site, le Titulaire s'engage à continuer la maintenance de la solution sur le nouveau site, aux conditions du présent marché moyennant un préavis de 30 jours.

### Utilisation des produits du titulaire sur des centres provisoires

En cas de panne du matériel, le Pouvoir Adjudicateur peut utiliser le logiciel du Titulaire sur un centre de secours. Il devra pour cela en avertir le Titulaire.

Il devra cependant prendre toutes les dispositions nécessaires pour que le logiciel ne soit pas utilisé sur ce centre par des tiers, et qu'il n'y ait pas de transmission volontaire ou involontaire de logiciels.

Le Titulaire s'engage à "déverrouiller" le logiciel existant ou à mettre en place une version provisoire sur le site de remplacement (les frais résultants de ces modifications étant à la charge du Pouvoir Adjudicateur).

## ANNEXES AU CCTP

* + ANNEXE 1 – CHARTE D’UTILISATION DU SYSTEME D’INFORMATION
  + ANNEXE 2 – SECURITE DES SYSTEMES D’INFORMATION
  + ANNEXE 3 – INFRASTRUCTURE
  + ANNEXE 4 – INTEGRATION EAI
  + ANNEXE 5 – POSTE DE TRAVAIL
  + ANNEXE 6 – RESEAU
  + ANNEXE 7 – REVUE DU SUPPORT