



CAHIER DES CLAUSES TECHNIQUES PARTICULIERES **(CCTP)**

**Accord-cadre de techniques de l'information et de la communication
N° 2025.03**

**Fourniture, mise en œuvre et maintenance
d'équipements d'automatisation RFID
pour la BU SHS de l'Université de Lille**

Sommaire

1. Présentation générale	5
2. Éléments spécifiques au projet et besoins quantitatifs	8
2.1. Contexte technique	8
2.1.1. Technologie RFID utilisée	8
2.1.2. Cartes de lecteur	8
2.2. Interface avec les systèmes tiers	9
2.3. Circulation des documents	9
2.4. Équipements à fournir	9
2.4.1. Volumétrie	9
2.4.2. Points spécifiques concernant les équipements	10
2.5. Calendrier prévisionnel de déploiement de l'automatisation	13
3. Besoins techniques et fonctionnels généraux	14
3.1. Normes, standards, réglementations techniques et sanitaires	14
3.1.1. Technologie, normes et standards RFID	14
3.1.2. Compatibilité avec l'environnement technique de l'Université	14
3.1.3. Conformité avec les réglementations techniques et sanitaires en vigueur	14
3.2. Interfaces et logiciels fournis avec les équipements d'automatisation	15
3.2.1. Interface avec les systèmes tiers	15
3.2.2. Sécurité	15
3.2.3. Compatibilité avec l'infrastructure informatique et réseau de l'Université	16
3.2.4. Postes professionnels de l'Université	16
3.2.5. Postes et boîtiers informatiques fournis par le titulaire	17
3.2.6. Logiciels hébergés sur une plate-forme extérieure appartenant au titulaire	18
3.3. Exploitation par l'Université	19
4. Protection des données à caractère personnel	20
4.1. Présentation générale	20
4.2. Qualification de la responsabilité des parties	20
4.3. Description du traitement de données à caractère personnel	20
4.4. Obligations du titulaire	21
4.4.1. Échanges de données avec des systèmes tiers	21
4.4.2. Autorisation de désignation d'un autre prestataire	21
4.4.3. Droit d'information des personnes concernées	22
4.4.4. Exercice des droits des personnes	22
4.4.5. Notification des violations de données à caractère personnel	22
4.4.6. Aide du titulaire dans le cadre du respect par l'Université de ses obligations	23
4.4.7. Mesures de sécurité des données à caractère personnel	23
4.4.8. Sort des données	23
4.4.9. Délégué à la protection des données	23
4.4.10. Registre des catégories d'activités de traitement	23
4.4.11. Documentation	24
4.5. Obligations de l'Université	24
4.6. Prestations de services attendues de la part du titulaire	24
4.6.1. Prestations de services attendues pour la mise en œuvre	24
4.6.2. Prestations de services attendues pour la garantie et la maintenance	24

5. Besoins techniques et fonctionnels concernant les équipements d'automatisation	25
5.1. Platines RFID	25
5.1.1. Description matérielle	25
5.1.2. Modalités d'implantation dans le mobilier – Ergonomie	25
5.1.3. Logiciels - Lien avec le SIGB	25
5.1.3.1. Logiciel d'encodage	25
5.1.3.2. Logiciel pour l'utilisation courante des platines	26
5.2. Portique antivol	27
5.2.1. Portique antivol fixé au sol	27
5.2.2. Box éventuellement associée au portique antivol	28
5.2.3. Logiciel de gestion centralisée	28
5.3. Compteurs de passage avec caméra	28
5.4. Automates de prêt-retour libre-service	29
5.4.1. Fonctionnalités attendues	29
5.4.2. Caractéristiques physiques et modèles	31
5.4.3. Accessibilité	31
5.4.4. Intégration bâtiment et mobilier	32
5.4.5. Logiciel de gestion centralisée	32
5.5. Système de retour	32
5.5.1. Boîte de retour SIP2	33
5.5.2. Robot de tri	34
5.5.3. Autres équipements	35
5.5.4. Intégration bâtiment	35
5.5.5. Logiciel de gestion centralisée	36
5.5.6. Chiffage dans le BPU	36
5.6. Terminaux RFID mobiles	36
5.6.1. Inventaires, recherches, modification des données	36
5.6.2. Prêts et retours	37
5.6.3. Caractéristiques générales	37
5.7. Remarque générale concernant l'alimentation PoE des matériels d'automatisation	37
6. Prestations de services attendues pour la mise en œuvre	38
6.1. Prestations de conduite de projet - Calendrier	38
6.1.1. Calendrier prévisionnel des prestations	38
6.1.2. Conduite de projet et équipe proposée	38
6.2. Prestations concernant l'équipement des collections	39
6.3. Prestations de conseil pour l'implantation des équipements d'automatisation dans la BU SHS restructurée et l'aménagement des espaces	39
6.4. Prestations de spécifications de la configuration et du paramétrage des équipements d'automatisation	40
6.5. Prestations d'installation des matériels, de déploiement des logiciels et de réalisation des paramétrages	41
6.6. Prestations liées à la protection des données personnelles	42
6.7. Prestations de formation	42
6.7.1. Modalités de formation	42
6.7.2. Liste des formations attendues	42
6.7.2.1. Présentation de la solution du titulaire	42
6.7.2.2. Formation à l'équipement des documents avec des étiquettes RFID	43
6.7.2.3. Formation à l'utilisation des platines (prêt-retour), du portique antivol, des compteurs de passage et des automates	43

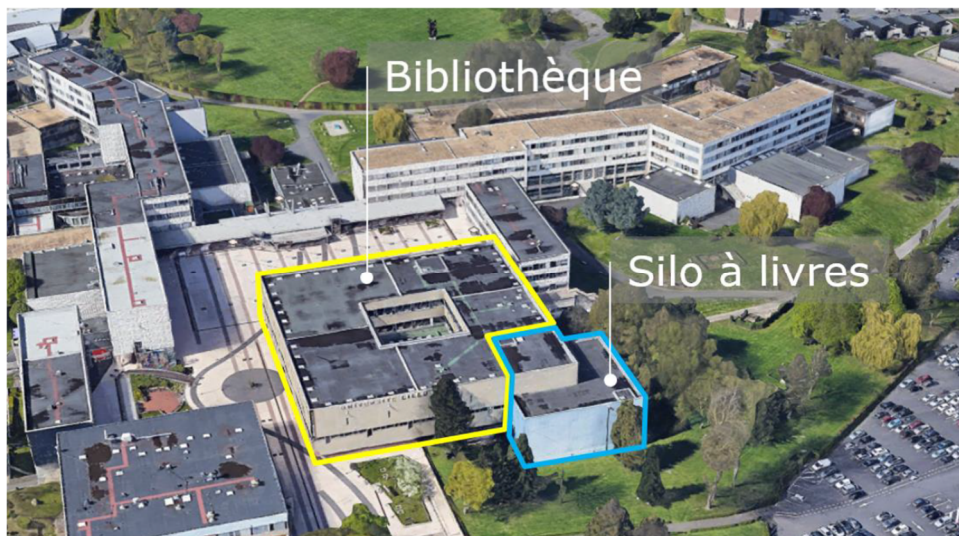
6.7.2.4.	Formation à l'administration et à l'exploitation techniques et fonctionnelles des platines, du portique antivol, des compteurs de passage, des automates	43
6.7.2.5.	Formation à l'utilisation du système de retour	44
6.7.2.6.	Formation à l'administration et à l'exploitation techniques et fonctionnelles du système de retour	44
6.7.2.7.	Formation à l'utilisation et à l'administration technique et fonctionnelle des terminaux RFID mobiles	44
6.7.3.	Déroulement des formations - Supports	45
6.8.	Fourniture de la documentation.....	45
6.9.	Assistance au démarrage	45
6.10.	Vérification des prestations	45
7.	Prestations de services attendues pour la garantie et la maintenance ...	46
7.1.	Présentation générale.....	46
7.2.	Besoins concernant la garantie et la maintenance.....	46
7.2.1.	Objet de la garantie et de la maintenance	46
7.2.2.	Accès au service de garantie et de maintenance par l'Université	47
7.2.3.	Accès au système par le titulaire.....	47
7.2.4.	Traitement préventif	48
7.2.5.	Traitement correctif.....	48
7.2.6.	Pièces détachées et livraisons	49
7.2.7.	Traitement évolutif et adaptatif	50
7.2.8.	Prestations liées à la protection des données personnelles.....	51

1. Présentation générale

La bibliothèque universitaire des Sciences Humaines et Sociales du Campus Pont de Bois fait partie du réseau des 4 BU/Learning center de l'Université de Lille qui, outre la BU SHS, comprend :

- Un learning center innovation : Lilliad
- Une BU Santé
- Une BU Droit-Gestion.

La BU SHS est implantée sur le Campus Pont de Bois à Villeneuve-d'Ascq.



Elle possède un fonds de 800 000 documents, dont l'essentiel (640 000 documents) est conservé en magasin (silo). Ses collections intègrent un riche fonds patrimonial (21 000 documents).

L'université de Lille a lancé un projet de restructuration complet du bâtiment qui est en cours de réalisation. La BU a transféré ses activités dans un bâtiment provisoire également situé sur le Campus Pont de Bois. Celui-ci n'héberge qu'une petite partie des collections, la majeure partie ayant été transférée dans des magasins de conservation à Laon.



La BU avant le début du projet de restructuration



Le projet de restructuration de la BU – Image Carta - Reichen et Robert Associés

Le projet de restructuration implique :

- La réhabilitation de l'ensemble bâtiminaire (environ 16 400 m² de surface de plancher)
- Le désamiantage
- La mise aux normes énergétique
- La mise aux normes pour l'accessibilité et la conservation des ouvrages
- La création d'espaces de travail confortables, modulables, modernes et connectés
- La création d'un tiers lieu avec notamment un espace cafétéria.

Le processus choisi pour la réalisation de l'opération est un marché global de performance au sens de l'article L.2171-3 du Code de la commande publique. Le groupement, dont le mandataire est la société Rabot Dutilleul associée à l'agence d'architecture Carta - Reichen et Robert Associés, a été retenu en juin 2023. L'ouverture de la BU restructurée est prévue pour la rentrée de septembre 2026.

La BU restructurée s'articulera sur 4 niveaux :

- Rez-de-jardin : espace de détente à destination des étudiants appelé « quartier libre » et bureaux de l'Atelier de Numérisation et de Reproduction des Thèses (ANRT)
- Rez-de-forum : espaces d'accueil, de rencontres, d'événements, d'expositions, de restauration et de travail collaboratif
- R+1 : espaces de consultation, salles de travail en groupe et pôle recherche (réservé aux doctorants et postdoctorants de l'Université ainsi qu'aux chercheurs en résidence)
- R+2 : espaces de consultation, salles de travail en groupe et bureaux du personnel.

Avant sa fermeture pour rénovation, la BU SHS, comme les autres BU/Learning center de l'Université, était équipée d'une solution d'automatisation RFID. Dans le cadre du 1^{er} équipement du bâtiment restructuré, la BU souhaite se doter de nouveaux équipements RFID. C'est l'objet du présent accord-cadre. Seules des platines existantes seront conservées.

Les équipements nouvellement acquis devront être compatibles avec les étiquettes actuellement apposées sur les documents et avec le matériel déjà en possession de l'Université. Les étiquettes et équipements existants fonctionnent en technologie HF (équipements fournis par la société Bibliotheca).

L'accord-cadre comprend :

- La fourniture des équipements suivants :
 - Platines
 - Portique antivol fixé au sol
 - Compteurs de passage avec caméra
 - Automates de prêt-retour libre-service

- Système de retour comprenant 1 boîte intérieure et un robot de tri à 7 bacs
 - Terminaux RFID mobiles (qui seront principalement utilisés pour les inventaires)
- La réalisation des prestations de service associées :
 - Conduite de projet
 - Conseil pour l'implantation des équipements d'automatisation et l'aménagement des espaces
 - Spécifications de la configuration et du paramétrage des équipements et logiciels d'automatisation
 - Installation des équipements dans la BU restructurée, déploiement des logiciels et réalisation des paramétrages
 - Formation du personnel
 - Assistance au démarrage et à la vérification des prestations
 - Garantie (1 an) et maintenance.

2. Éléments spécifiques au projet et besoins quantitatifs

2.1. Contexte technique

2.1.1. Technologie RFID utilisée

La technologie RFID utilisée par l'Université est la suivante :

- Les puces et antennes RFID fonctionnent à la fréquence de 13,56 MHz (HF).
- Les étiquettes RFID sont conformes à la norme ISO 18000-3.
- Les données sont encodées selon la recommandation IDRABIB version 2008.
- L'information antivol est gérée de deux manières :
 - Champ AFI (Application Family identifier)
 - Bit de sécurité EAS.

Le règlement de la consultation du présent accord-cadre prévoit la fourniture d'exemples d'étiquettes encodées (AFI et EAS) aux candidats afin qu'ils puissent valider le bon fonctionnement de leur solution avec ces étiquettes.

Les équipements existants ont été fournis par la société Bibliotheca

2.1.2. Cartes de lecteur

Deux types de cartes de lecteur sont utilisés par la BU :

- Des cartes multiservices pour les étudiants et le personnel
- Des cartes dotées uniquement d'un code à barres, notamment pour les lecteurs extérieurs.

Caractéristiques des cartes multiservices (Cartes MultiServices ou CMS)

Les caractéristiques des cartes CMS sont les suivantes :

- Fournisseur Monecarte
- Technologie MIFARE DESFire EV1
- Les accès bâtiment utilisent le numéro de série (CSN) de la carte.
- La BU utilise un autre numéro stocké dans la carte : le numéro lecteur
 - Type : AES
 - AID : F586E0
 - Id fichier : 0
 - Numéro de clé : 3
 - Type : Standard
 - Com : Chiffrée
 - Type de donnée : entier
 - Donnée : UID position 1
 - Longueur : 4
 - Clé de lecture : transmise sur demande

Fonctionnement attendu

- Automates :
 - Les automates devront être équipés par le titulaire de lecteurs de cartes compatibles avec les cartes CMS :
 - Le numéro lecteur devra obligatoirement être utilisé (et non le CSN de la carte).
 - Pour information, la BU utilise actuellement les lecteurs de cartes OMNIKEY CardMan 5x21, Identive CLOUD 4700F et ELATEC TWN4, mais les candidats peuvent proposer un autre modèle de lecteur dès lors qu'il est compatible avec les cartes CMS.
 - Le règlement de la consultation du présent accord-cadre prévoit la fourniture d'un exemple de carte CMS aux candidats afin qu'ils puissent valider le bon fonctionnement de leurs équipements avec ces cartes.
 - Les automates devront également permettre l'utilisation des cartes code à barres (Interleaved 2 of 5).

- Système de retour :
 - Aucune identification des usagers n'est nécessaire. Le système sera uniquement utilisé pour le retour.
- Terminaux RFID Mobiles utilisés pour des opérations de prêt-retour :
 - Principalement utilisés pour les opérations d'inventaire ;
 - Les opérations de prêt-retour devront être possibles ainsi que l'utilisation des cartes code à barres ;
 - La possibilité d'utiliser une carte CMS sera appréciée.

2.2. **Interface avec les systèmes tiers**

SIGB

Les nouveaux équipements RFID devront s'interfacer avec le système de gestion de bibliothèque Alma de la société Ex Libris (Clarivate) qui est utilisé par l'Université :

- Alma est hébergé par Ex Libris (Clarivate).
- Les équipements RFID réalisant des opérations de prêt-retour dialoguent avec Alma en utilisant le protocole SIP2. Les échanges empruntent un tunnel VPN afin d'être chiffrés. Ce tunnel est géré par le bureau informatique documentaire de la DGDNum de l'Université (Direction Générale Déléguée au Numérique).

Affluences

- La BU SHS est abonnée à la solution Affluences. Celle-ci devra pouvoir accéder en temps réel (décalage de moins de 15 minutes) aux informations de comptage provenant du système mis en place par le titulaire. Des postes sont prévus dans le BPU pour la réalisation du paramétrage nécessaire.

2.3. **Circulation des documents**

Les documents circulent entre les différentes BU/Learning center de l'Université de Lille. Les équipements RFID auront donc à gérer des documents provenant de plusieurs établissements.

2.4. **Équipements à fournir**

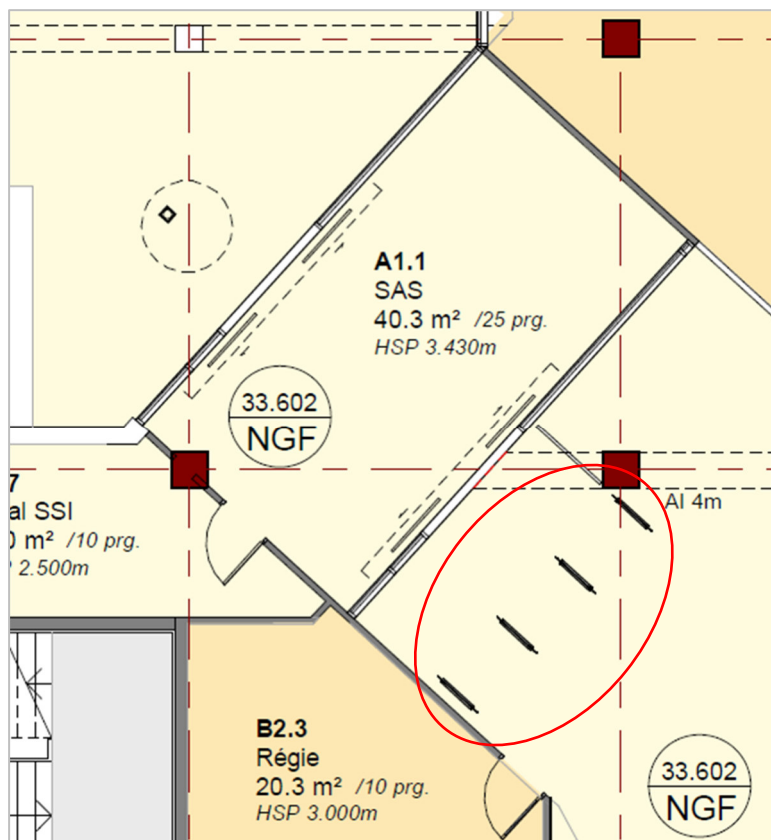
2.4.1. **Volumétrie**

Matériel	Quantité
Platines	7
Portique antivol 3 unités de passage	1
Compteur(s) de passage à caméra	Pour 1 issue
Automates de prêt-retour libre-service sur pied	2
Automates de prêt-retour libre-service à poser (éventuellement, automate à intégrer)	2
Système de retour : 1 boîte intérieure et 1 robot de tri à 7 bacs	1
Terminaux RFID mobiles (qui seront principalement utilisés pour les inventaires)	2

2.4.2. Points spécifiques concernant les équipements

Portique antivol et compteur(s) de passage à caméra

Le portique et le(s) compteur(s) de passage équiperont l'entrée principale de la BU restructurée au rez-de-forum :



Le portique devra comporter 4 panneaux délimitant 3 unités de passage d'environ 1,40 m de large (le BPU demande cependant le chifrage d'une gamme complète avec des portiques allant de 1 à 5 unités de passage).

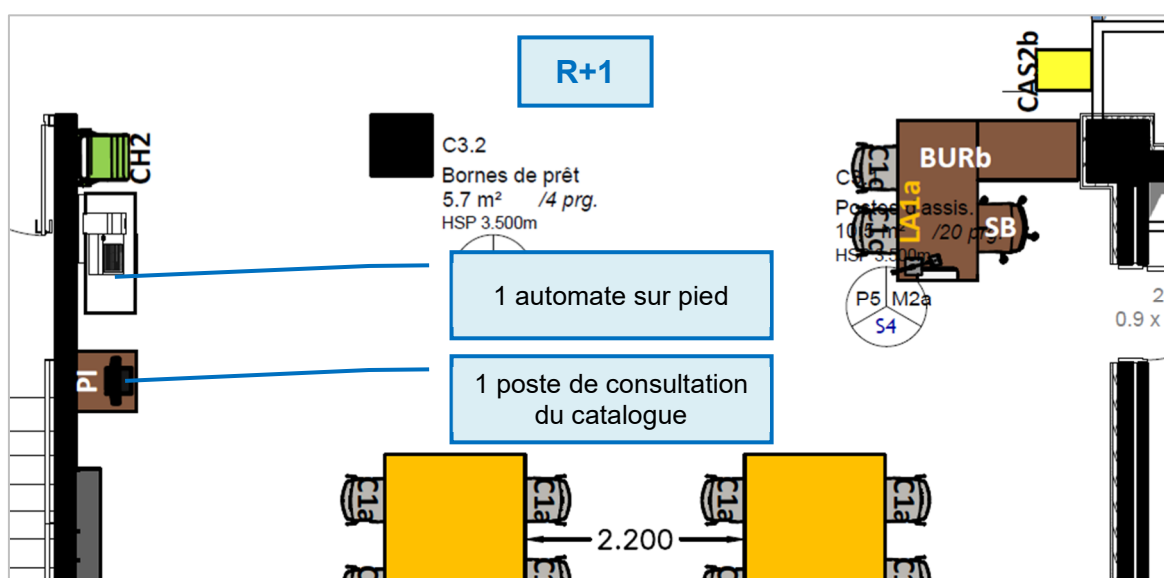
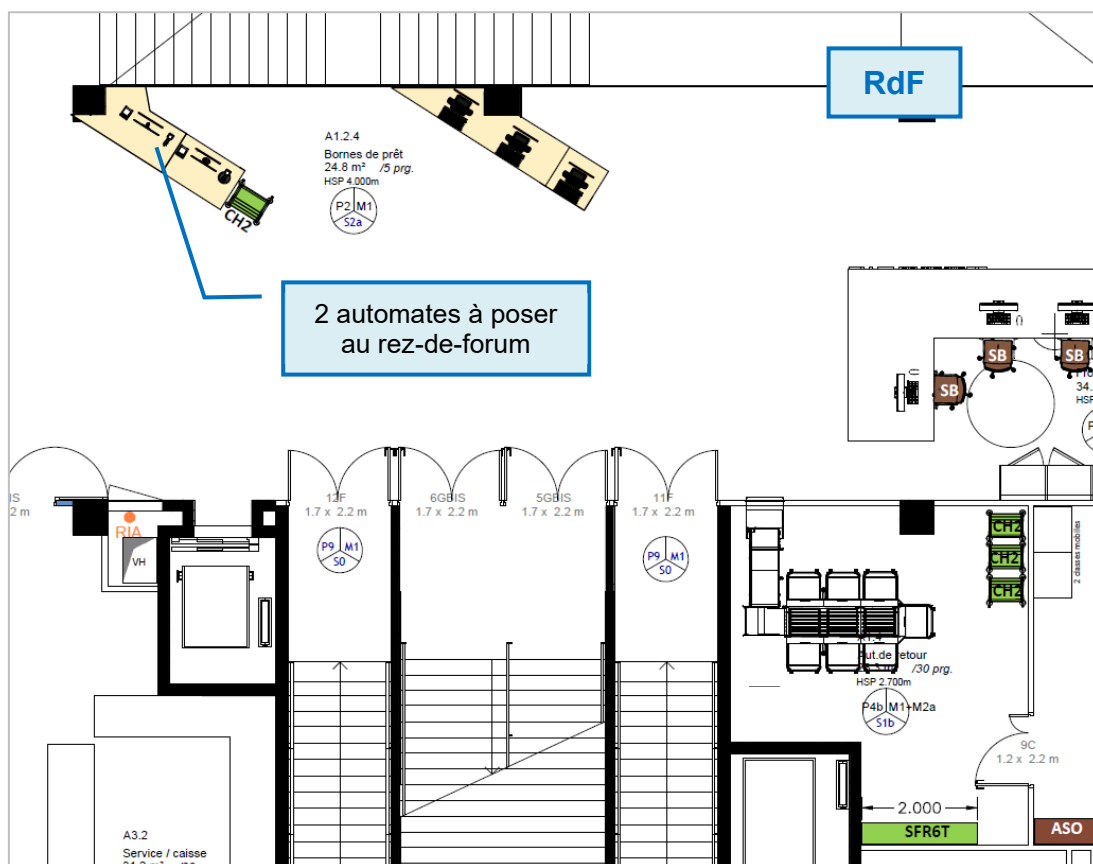
Le nombre de compteurs de passage (1 ou 2) dépendra de la largeur couverte par un seul compteur. La distance entre les panneaux d'extrémité du portique sur le plan est d'environ 3x1,4 m, soit 4,20 m.

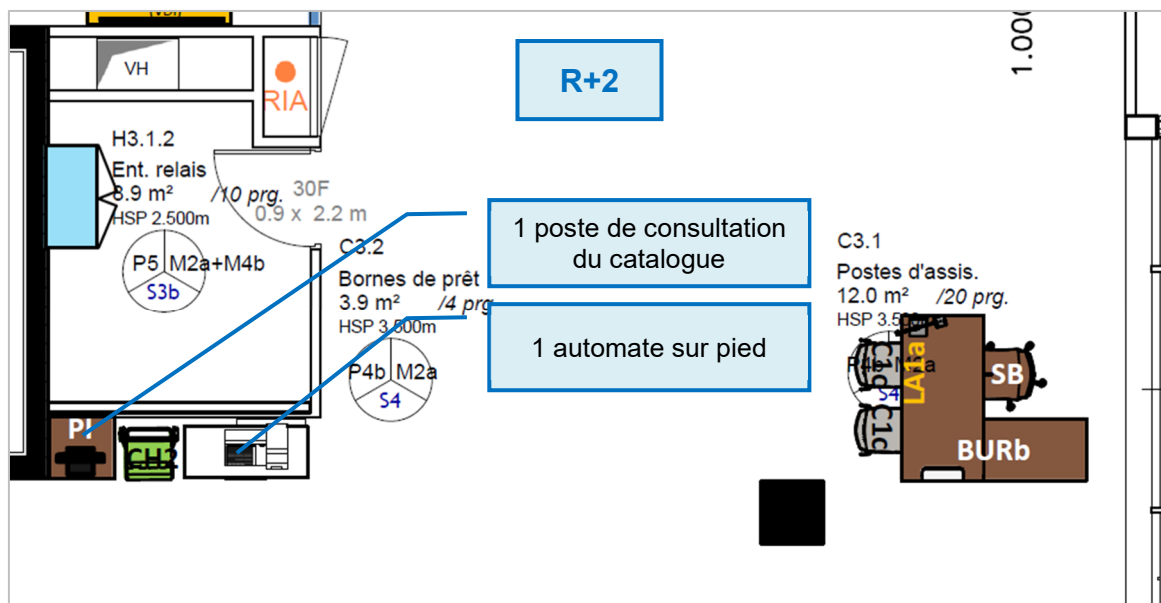
Automates

Deux types d'automates sont prévus :

- 2 automates sur pied (bornes) :
 - Le BPU permet de chiifrer différents modèles, dont un modèle réglable en hauteur par les usagers.
 - L'un des automates sera installé au R+1 et l'autre au R+2.
- 2 automates à intégrer ou à poser sur du mobilier :
 - Ces automates seront associés à du mobilier réalisé sur mesure.
 - Les automates à intégrer posent le problème d'installation d'une unité centrale et de la platine sous le plateau du meuble.
 - Pour éviter ces difficultés, des automates à poser ont la préférence de la BU. Le BPU permet le chifrage de deux modèles présentant des encombrements différents, un modèle peu volumineux ayant la préférence de l'Université.
 - Le BPU demande également le chifrage d'un modèle à intégrer comportant obligatoirement un PC tout-en-un pour éviter d'avoir à masquer une unité centrale indépendante de l'écran.
 - Les 2 automates seront installés au rez-de-forum, à proximité du système de retour.

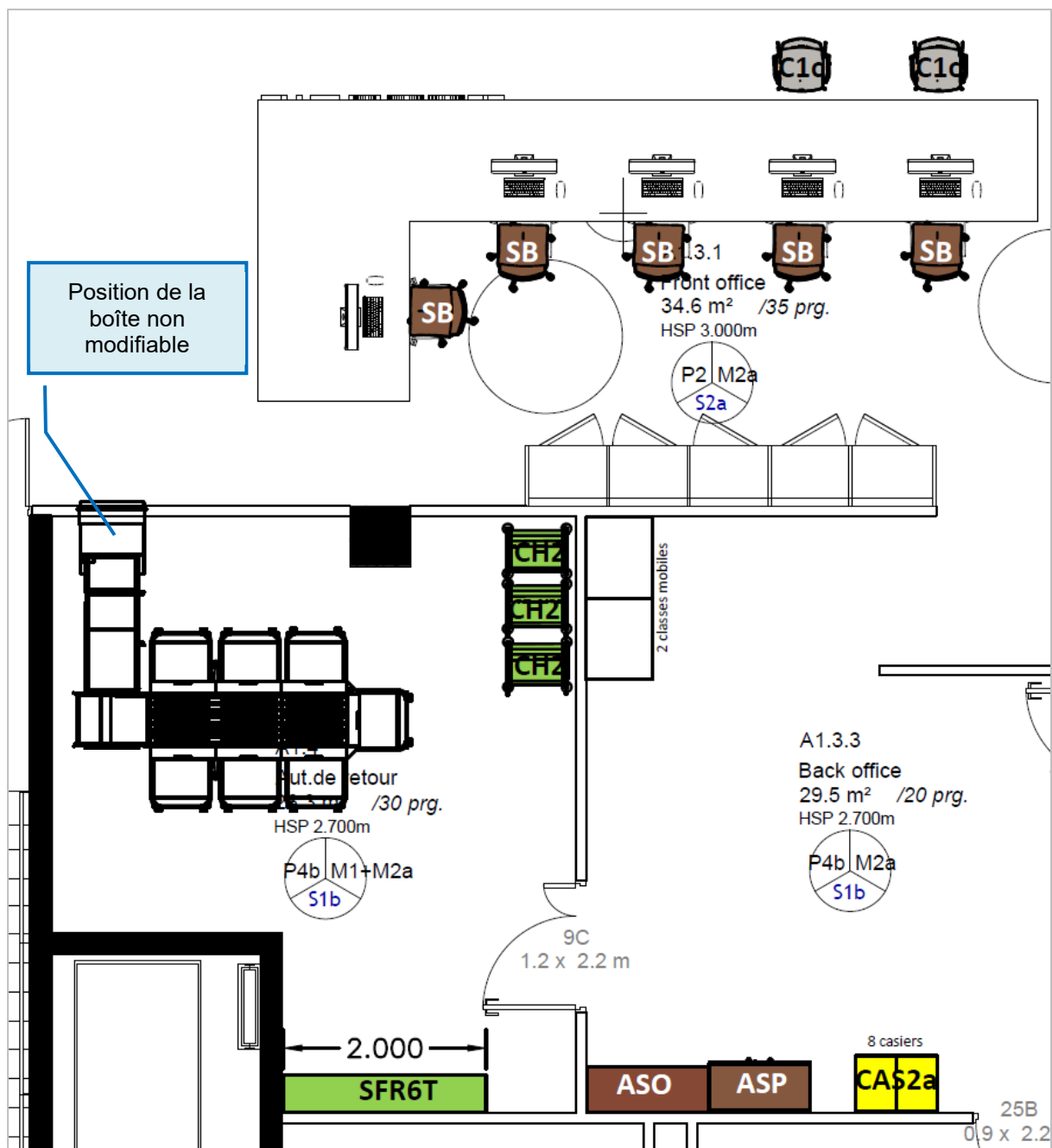
- En fonctionnement normal, les automates permettront uniquement le prêt. En cas de panne du système de retour, les 2 automates du rez-de-forum seront configurés pour assurer également les retours ; un chariot sera mis en place pour recueillir les documents retournés.
- Position des automates sur les plans :





Système de retour

- Le système de retour sera installé dans une salle dédiée (référence « A1.4 Aut. de retour » sur le plan)
- Le système de retour comportera :
 - 1 boîte de retour intérieure
 - 1 robot de tri à 7 bacs
 - 2 bacs supplémentaires pour remplacement immédiat d'un bac plein par un bac vide.
- L'implantation montrée ci-dessous n'est qu'un exemple. Les candidats sont libres de proposer l'implantation qui leur semble optimale. Il y a cependant une seule exception : **la position de la boîte de retour ne peut pas être modifiée en raison de présence de la banque d'information.**
- Les éléments en vert correspondent à des mobiliers. Les éléments « CH2 » sont des chariots mobiles dont la position peut être adaptée.



Plan DWG du rez-de-forum

Le plan DWG du rez-de-forum où seront installés le portique antivol et système de retour est annexé au présent CCTP.

2.5. Calendrier prévisionnel de déploiement de l'automatisation

L'installation des équipements RFID est prévue au 1^{er} trimestre 2026, la BU restructurée ouvrant ses portes à la rentrée de septembre 2026. Ce calendrier est susceptible d'évoluer.

3. Besoins techniques et fonctionnels généraux

3.1. Normes, standards, réglementations techniques et sanitaires

Le système d'automatisation RFID devra permettre :

- l'identification des documents
- et la protection antivol des documents.

3.1.1. Technologie, normes et standards RFID

Les équipements et logiciels RFID devront respecter les normes et standards suivants :

- Fréquence de fonctionnement : 13,56 MHz (HF)
- Communication entre les puces et les matériels : normes ISO 18000-3 et ISO 15693
- Modèle de données :
 - Recommandation IDRABIB version 2008
 - Même si ce n'est pas le modèle de données actuellement utilisé par l'Université de Lille, le support du modèle ISO 28560-2 est également obligatoire. Il devra pouvoir être utilisé simultanément avec le modèle IDRABIB (reconnaissance automatique du modèle).
 - Dans tous les cas, seront présents dans la puce, au minimum :
 - Identifiant du document
 - Code RCR de la bibliothèque
 - Pour les documents comportant plusieurs étiquettes : rang de la puce et nombre total de puces équipant le document.
- Gestion de l'information antivol :
 - L'antivol devra être stocké dans la puce et devra pouvoir être géré selon deux modes actifs simultanément :
 - Utilisation du champ AFI (Application Family Identifier ISO 15961 ; valeur hexa C2 pour un document non protégé et valeur hexa 07 pour un document protégé)
 - Bit de sécurité EAS pour les puces compatibles.
- Protocole pour le dialogue entre le SIGB Alma et les équipements RFID gérant des transactions de prêt-retour :
 - SIP2
 - Les échanges avec Alma empruntent un tunnel VPN afin d'être chiffrés.

3.1.2. Compatibilité avec l'environnement technique de l'Université

Les équipements et logiciels fournis par le titulaire devront fonctionner dans le contexte technique décrit paragraphe « 2.1 - Contexte technique » et être compatibles avec les étiquettes et les équipements déjà en place dans les BU/Learning center de l'Université.

3.1.3. Conformité avec les réglementations techniques et sanitaires en vigueur

Les équipements proposés devront être conformes aux réglementations techniques et sanitaires en vigueur, notamment en ce qui concerne l'exposition des personnes à des rayonnements électromagnétiques. Ces rayonnements devront être limités au maximum afin de ne pas exposer inutilement le personnel et le public.

3.2. Interfaces et logiciels fournis avec les équipements d'automatisation

3.2.1. Interface avec les systèmes tiers

SIGB

Les équipements RFID devront s'interfacer avec le SIGB Alma utilisé par l'Université :

- Alma est hébergé par Ex Libris (Clarivate).
- Le protocole SIP2 sera obligatoirement utilisé pour tous les échanges entre le SIGB et les équipements RFID réalisant des transactions de prêt-retour (automates, système de retour) :
 - Les échanges empruntent un tunnel VPN afin d'être chiffrés. Ce tunnel est géré par le bureau informatique documentaire de la DGDNum de l'Université (Direction Générale Déléguée au Numérique).
 - Les licences SIP2 nécessaires pour les équipements d'automatisation sont incluses dans l'abonnement Alma. Elles ne sont donc pas à fournir dans le présent accord-cadre.
- Logiciel pour l'utilisation courante des platines installé sur les postes professionnels :
 - Le logiciel devra autoriser l'activation-désactivation automatique de la puce RFID d'un document en fonction de la transaction (retour ou prêt) réalisée dans le SIGB sur un poste professionnel (dans la limite des capacités fonctionnelles d'Alma). Cela évitera la gestion manuelle de la position antivol de la platine (activation ou désactivation) par le personnel.
 - Le logiciel devra permettre le fonctionnement de la platine avec le module « prêt secouru » du SIGB en cas de problème réseau ou d'indisponibilité du serveur SIGB, dans la mesure où ce module « prêt secouru » le permet.

Affluences

La BU SHS est abonnée à la solution Affluences. Celle-ci devra pouvoir accéder en temps réel (décalage de moins de 15 minutes) aux informations de comptage provenant du système mis en place par le titulaire. Des postes sont prévus dans le BPU pour la réalisation du paramétrage nécessaire.

3.2.2. Sécurité

RGI, RGS et CCSC

Le système proposé devra être conforme d'un point de vue technique avec les normes et bonnes pratiques du Référentiel Général d'Interopérabilité (RGI) et du Référentiel Général de Sécurité (RGS) qui sont applicables aux administrations publiques.

La conformité avec le RGS est très importante dans le cadre de la protection des données à caractère personnel.

Le titulaire devra fournir un dossier montrant la conformité du système installé au RGS version 2.0 pour les éléments relevant de sa responsabilité (donc hors éléments strictement dépendants de l'infrastructure informatique et réseau de l'Université).

Le titulaire devra fournir les identifiants et mots de passe des comptes administrateur/root des postes, et boîtiers fournis par ses soins et installés dans l'infrastructure de l'Université.

Le cahier des clauses simplifiées de cybersécurité (CCSC) est applicable.

Chiffrement des communications

Tous les échanges réseau liés au système d'automatisation devront être chiffrés, notamment les échanges faisant intervenir une plate-forme extérieure appartenant au titulaire. Le titulaire devra fournir tous les certificats requis.

Pour le transfert de fichiers entre serveurs, le protocole HTTPS sera privilégié ; les protocoles SFTP et FTPS sont à éviter.

Document à fournir dans l'offre (voir également « 4 - Protection des données à caractère personnel »)

- Le plan d'assurance sécurité (PAS) du titulaire
- La politique de sécurité du système d'information (PSSI) du titulaire

- La politique de sécurité des données à caractère personnel du titulaire (complément éventuel au PAS et au PSSI si ces documents ne traitent pas du sujet)
- Le plan de continuité d'activité (PCA) du titulaire.

3.2.3. Compatibilité avec l'infrastructure informatique et réseau de l'Université

VLAN et DMZ

Dans l'infrastructure informatique et réseau de l'Université, la sécurisation des flux est assurée :

- Par des VLAN internes avec un contrôle strict des communications inter-VLAN
- Par des équipements de type pare-feux, proxies et reverse proxies pour le filtrage des accès depuis et vers Internet.

L'Université a décidé de créer un VLAN spécifique pour connecter les équipements RFID (portique antivol, compteurs de passage avec caméra, automates de prêt-retour, système de retour).

Le système d'automatisation fourni par le titulaire devra être compatible avec cette architecture.

Aucun flux lié aux équipements d'automatisation ne devra être « entrant » vis-à-vis du réseau local (pas de flux UDP entrant, flux TCP entrant uniquement à la suite d'une connexion initiale TCP sortante).

Paramétrage IP

Le paramétrage réseau des équipements d'automatisation devra respecter les règles générales de configuration des équipements dans les réseaux informatiques de l'Université (adressage IP, masque, routage, etc.).

Les matériels et logiciels fournis dans le cadre du présent accord-cadre devront être compatibles avec une infrastructure réseau IPv4 ou IPv6.

Accès extranet pour la télémaintenance

Les accès depuis Internet pour la télémaintenance des matériels et des logiciels installés dans les locaux de l'Université sont décrits dans le chapitre « 7 - Prestations de services attendues pour la garantie et la maintenance ».

Émission de mails

Les logiciels fournis par le titulaire et installés dans l'infrastructure informatique et réseau de l'Université pourront utiliser un serveur SMTP déjà en place dans l'infrastructure pour l'émission des mails. Ces émissions devront être ponctuelles (par exemple, mail envoyé à la suite d'une transaction de prêt-retour sur un automate) ; aucun mailing de masse ne sera autorisé.

Les logiciels hébergés sur une plate-forme extérieure appartenant au titulaire devront intégrer une solution d'envoi de mails propre ; l'utilisation d'un serveur SMTP de l'Université par ces logiciels ne sera pas possible.

3.2.4. Postes professionnels de l'Université

Postes professionnels

Les postes professionnels à partir desquels les équipements d'automatisation seront utilisés, fonctionnent sous Windows 10 ou 11 Professionnel.

Installation de composants sur les postes professionnels

Le titulaire devra fournir les packages permettant le déploiement silencieux des logiciels d'automatisation sur les postes professionnels.

Cette installation privilégiera un dossier applicatif à l'exclusion des dossiers système par défaut comme le répertoire Windows. Les répertoires système ne peuvent pas être accessibles en écriture ou en modification.

Les utilisateurs disposent de droits restreints. En aucun cas, des droits d'administration ne devront être requis pour faire fonctionner les logiciels sur les postes clients.

IHM Web

Les applications accessibles en mode Web devront fonctionner a minima à partir des navigateurs les plus couramment utilisés :

- Chrome, Edge, Firefox, Firefox ESR, Opera, Safari...
- sur PC (Windows ou Linux), Mac (Mac OS) et tablettes (Android, iOS, Windows)
- dans une version datant de moins de deux ans ou à défaut dans leur dernière version publiée et intégrant dans tous les cas toutes les mises à jour de sécurité publiées.

Compatibilité avec la solution antivirus utilisée par l'Université sur les postes professionnels

Les candidats préciseront les paramétrages spécifiques ou les problèmes d'incompatibilité de leur solution avec les logiciels antivirus courants du marché. Les paramétrages spécifiques ne devront pas remettre en cause la politique de sécurité mise en place par l'Université.

À ce jour, l'Université utilise la solution antivirus WithSecure.

3.2.5. Postes et boîtiers informatiques fournis par le titulaire

Les postes et boîtiers informatiques fournis par le titulaire, notamment les postes des automates et du système de retour ainsi que la box éventuellement requise pour le portique antivol, devront respecter les règles d'intégration décrites ci-dessous.

Sauvegardes

Les postes et boîtiers fournis par le titulaire ne feront l'objet d'aucune sauvegarde de la part de l'Université.

Aucune base de données (ou informations nécessaires pour les statistiques) ne devra être stockée sur ces postes.

La réinstallation d'un poste ou d'un boîtier (après changement matériel éventuel) sera totalement à la charge du titulaire dans le cadre de la garantie et de la maintenance ; cela inclut la fourniture de l'ensemble des logiciels et données nécessaires à cette réinstallation.

Protection antivirale

Une protection antivirale fournie par le titulaire devra être installée sur les postes et boîtiers du titulaire.

L'Université pourra également décider d'installer sa propre solution antivirus. Le titulaire devra fournir l'assistance nécessaire à l'Université.

Les candidats préciseront les paramétrages spécifiques ou les problèmes d'incompatibilité de leur solution avec les logiciels antivirus courants du marché. Les paramétrages spécifiques ne devront pas remettre en cause la politique de sécurité mise en place par l'Université.

Mises à jour

Le titulaire gérera les mises à jour logicielles des postes et boîtiers qu'il aura fournis, système d'exploitation inclus. Pour plus de détails, cf. « 7 - Prestations de services attendues pour la garantie et la maintenance ».

L'Université pourra également décider de gérer l'installation régulière des patches de sécurité. Si elle fournit l'antivirus, elle gérera également à la mise à jour de l'antivirus.

Agent SNMP

Un agent SNMP pourra être installé par l'Université sur les postes et boîtiers fournis par le titulaire. Celui-ci devra fournir l'assistance nécessaire à l'Université.

3.2.6. Logiciels hébergés sur une plate-forme extérieure appartenant au titulaire

Si la solution du titulaire fait intervenir des logiciels hébergés sur une plate-forme extérieure lui appartenant ou louée par lui, les demandes suivantes devront être respectées, dans le cadre des prix portés au BPU :

- Mise à disposition des serveurs physiques et virtuels nécessaires au fonctionnement du système RFID
- Sécurité physique des serveurs :
 - Accès sécurisé aux salles serveur
 - Système anti-incendie
 - Alimentation secourue.
- Sécurité côté hébergement :
 - Sécurité réseau :
 - Sites d'hébergement possédant une infrastructure réseau ad hoc intégrant notamment des équipements permettant de prévenir les attaques informatiques (firewalls, reverse proxies, etc.)
 - Protection antivirale des serveurs.
 - Installation des mises à jour de sécurité des systèmes d'exploitation, SGBD et autres outils largement répandus dès leur disponibilité.
 - Sécurité des données :
 - Stockage des données de préférence en France, sinon au sein de l'Union européenne, sans possibilité de communication légale à des pays hors Union européenne
 - Mise en œuvre de tous les moyens nécessaires pour interdire la communication à des personnes non autorisées
 - Traçabilité des actions effectuées par le personnel du titulaire ou ses sous-traitants
 - Sauvegarde des serveurs par le titulaire :
 - La sauvegarde devra être réalisée sur des supports physiques indépendants des serveurs (pas de connexion au même réseau).
 - Le stockage des sauvegardes devra s'effectuer sur un site de sauvegarde géographiquement distinct du site de production hébergeant les serveurs faisant fonctionner le système RFID (distance supérieure à 1 km).
 - En cas de restauration, la perte de données tolérée correspondra au maximum aux données produites durant les dernières 24 heures.
 - La rétention des sauvegardes devra respecter les règles suivantes :
 - Sauvegardes de moins de 24 heures : au moins une sauvegarde disponible
 - Sauvegardes de plus de 24 heures et jusqu'à 3 mois au moins : une sauvegarde disponible par semaine
 - Outre les données, les sauvegardes devront comporter les machines virtuelles elles-mêmes afin d'autoriser une restauration rapide des serveurs en cas de perte de tout ou partie du site de production.
 - Les sauvegardes devront être chiffrées.
 - Les licences des logiciels de sauvegarde nécessaires ainsi que les supports physiques sont à la charge du titulaire.
 - Le titulaire devra obligatoirement fournir à l'Université :
 - Le plan d'assurance sécurité (PAS) de l'hébergement
 - La politique de sécurité du système d'information (PSSI) de l'hébergement :
 - La mise en œuvre de la norme ISO 27001 sera fortement appréciée
- Fourniture de l'accès à Internet côté hébergement :
 - Le coût de location de l'accès à Internet côté hébergement devra être inclus dans le cadre de la garantie et dans les coûts de maintenance ; aucun coût additionnel ne devra être à la charge de l'Université.
 - Le débit de l'accès à Internet côté hébergement devra être suffisant pour respecter les demandes de performances exprimées dans ce CCTP. La durée pour l'affichage complet d'une page Web provenant d'un site fonctionnant sur la plate-forme extérieure appartenant au titulaire devra être inférieure à 1,5 seconde (avec une liaison Internet, côté terminal de test, dotée d'une bande passante disponible d'au moins 20 Mbit/s).

- Prise en charge de tous les outils nécessaires pour l'émission de mails vers les usagers (passerelle mail, etc.) sans utilisation des passerelles et serveurs mail de l'Université
- Sécurité réseau côté Université :
 - Les règles de sécurité exigées par l'Université s'appliqueront à la plate-forme extérieure du titulaire. Cela concerne notamment la compatibilité avec le RGS et la sécurisation des échanges réseau (cf. « 3.2.2- Sécurité »).
 - Les flux de données entrants et sortants pourront être analysés par les firewalls, proxies et reverse proxies de l'Université ; ils ne devront pas compromettre la sécurité de l'infrastructure réseau et informatique de l'Université. En particulier, aucun flux ne devra être « entrant » vis-à-vis du réseau local (pas de flux UDP entrant, flux TCP entrant uniquement à la suite d'une connexion initiale TCP sortante).
- Si possible, disponibilité de serveurs sur le site de sauvegarde :
 - Ces serveurs devront permettre un redémarrage très rapide de la plate-forme en cas de perte des serveurs du site de production et, cela, sans que le titulaire ait à négocier la location de nouveaux serveurs.
 - Dans tous les cas, le titulaire devra obligatoirement fournir à l'Université le plan de reprise d'activité (PRA) appliqué en cas de perte du site de production.
- Conditions de disponibilité :
 - Elles devront permettre de respecter les délais de corrections des anomalies demandés dans le présent CCTP dans le cadre de la maintenance.
 - L'indisponibilité totale ou partielle de la plate-forme extérieure sera traitée comme une anomalie dans le cadre de la maintenance ; le non-respect des délais de correction entraînera l'application des pénalités prévues au CCAP.
- Protection des données à caractère personnel :
 - Les conditions d'hébergement de la plate-forme devront permettre de respecter les obligations légales et réglementaires liées à la protection des données à caractère personnel, concernant notamment la sécurité et les lieux de stockage des données (cf. « 4 - Protection des données à caractère personnel »).

3.3. Exploitation par l'Université

Le titulaire devra fournir la liste des éléments pertinents à superviser afin de prévenir d'éventuels dysfonctionnements ou de faciliter le diagnostic en cas de problème.

La charge d'exploitation devra être la plus faible possible.

Comme déjà dit plus haut, l'Université pourra décider d'installer un agent SNMP sur les postes et boîtiers fournis par le titulaire.

4. Protection des données à caractère personnel

4.1. Présentation générale

Le titulaire et l'Université sont tenus au respect des règles relatives à la protection des données à caractère personnel auxquelles ils ont accès pour les besoins de l'exécution du présent accord-cadre. Ces règles sont issues du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ci-après désigné « le règlement européen sur la protection des données », et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

4.2. Qualification de la responsabilité des parties

Au sens de la réglementation, l'Université est qualifiée de « responsable de traitement » en ce qu'elle détermine les finalités et les moyens de traitement des données à caractère personnel. Le titulaire est qualifié, pour sa part, de « sous-traitant de données à caractère personnel » en ce qu'il traite des données à caractère personnel pour le compte du responsable de traitement.

4.3. Description du traitement de données à caractère personnel

Le sous-traitant est autorisé à effectuer pour le compte de l'Université les traitements de données à caractère personnel décrits ci-après :

- L'objet du traitement est strictement limité à la fourniture des prestations objet du présent CCTP et aux opérations suivantes :
 - Collecte de données
 - Enregistrement de données
 - Organisation de données
 - Structuration de données
 - Conservation de données
 - Consultation de données
 - Utilisation de données
 - Effacement de données
 - Destruction de données
- Les finalités du traitement sont :
 - Réalisation des prêts, retours et prolongations de documents en libre-service par les usagers de la BU, consultation par les usagers de la BU de leur dossier d'abonné.
- Les catégories de données à caractère personnel traitées sont :
 - Données courantes :
 - Informations du dossier de lecteur du SIGB Alma : nom, prénom, adresse, téléphone, adresse mail, prêts et retours réalisés...
 - Données sensibles ou à caractère hautement personnel :
 - Aucune
- Les catégories de personnes concernées sont :
 - Lecteurs Alma majeurs et mineurs utilisant les équipements RFID de la BU.
- Pour l'exécution du présent contrat, l'Université met à la disposition du sous-traitant les informations nécessaires pour la réalisation des opérations de traitement :
 - Accès aux données « abonnés » du SIGB Alma par l'intermédiaire du protocole SIP2 exposé par le SIGB.
- Supports de traitement des données :
 - Automates, système de retour et terminaux portables RFID, logiciels installés sur des postes professionnels ou des serveurs de l'Université :
 - Localisation : BU et, éventuellement, infrastructure informatique de l'Université (pour les logiciels hors matériels RFID)
 - Éventuelle plate-forme extérieure du titulaire :
 - Localisation : de préférence en France et obligatoirement dans l'Union européenne

- Autres équipements informatiques appartenant au titulaire ou loués par lui :
 - Traitement possible uniquement pour la correction de dysfonctionnements.
 - Localisation : de préférence en France et obligatoirement dans l'Union européenne.
- Durée de l'autorisation du traitement :
 - Durée du présent accord-cadre.
 - À l'issue de l'accord-cadre, le sous-traitant devra détruire toutes les données à caractère personnel hébergées sur des équipements informatiques lui appartenant ou loués par lui et devra justifier par écrit de leur destruction.
- Durée de conservation des données à caractère personnel :
 - Automates, système de retour et terminaux portables RFID, logiciels installés sur des postes professionnels ou des serveurs de l'Université :
 - 4 mois au maximum (application de la norme simplifiée n° 9 de la CNIL, même si cette norme n'est plus officiellement en vigueur)
 - Éventuelle plate-forme extérieure du titulaire :
 - Une journée au maximum.
 - Autres équipements informatiques appartenant au titulaire ou loués par lui :
 - 4 mois au maximum (application de la norme simplifiée n° 9 de la CNIL, même si cette norme n'est plus officiellement en vigueur).

4.4. Obligations du titulaire

Le titulaire s'engage à :

- Traiter les données uniquement pour les seules finalités du traitement objet de la sous-traitance.
- Traiter les données conformément aux instructions de l'Université. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des États membres relative à la protection des données, il en informe immédiatement le responsable de traitement.
- En outre, si le titulaire est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, il doit informer l'Université avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.
- Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité, reçoivent la formation nécessaire en matière de protection des données à caractère personnel.
- Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

4.4.1. Échanges de données avec des systèmes tiers

Les échanges de données avec des systèmes tiers avec lesquels l'Université n'a pas établi de contrat devront obligatoirement faire l'objet d'une convention préalable entre l'Université et le titulaire.

4.4.2. Autorisation de désignation d'un autre prestataire

Le titulaire peut faire appel à un autre prestataire, désigné « le sous-traitant ultérieur », pour mener des activités de traitement spécifiques dans le respect des règles suivantes :

- a) Le sous-traitant n'est pas autorisé à sous-traiter à un sous-traitant ultérieur les opérations de traitement qu'il effectue pour le compte du responsable du traitement en vertu des présentes clauses sans l'autorisation écrite spécifique préalable du responsable du traitement.
- b) Au cours de l'exécution du présent accord-cadre, le sous-traitant soumet la demande d'autorisation spécifique de recourir à un nouveau sous-traitant ultérieur au moins 30 jours avant le recrutement de celui-ci, ainsi que les informations nécessaires pour permettre au responsable du traitement de prendre une décision au sujet de l'autorisation visée ci-dessus (a).
- c) La liste des sous-traitants ultérieurs effectuant une ou plusieurs opérations de traitement visées à l'article 4.3 ci-dessus est communiquée au responsable de traitement par le sous-traitant avant la conclusion de l'accord-cadre et à toute mise à jour de celle-ci.

- d) Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679.
- e) À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.
- f) Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.
- g) Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel.

4.4.3. Droit d'information des personnes concernées

Il appartient à l'Université de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

4.4.4. Exercice des droits des personnes

Le titulaire aide l'Université à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement.

Lorsque les personnes concernées exercent auprès du titulaire des demandes d'exercice de leurs droits, le titulaire doit adresser ces demandes dès réception par courrier électronique adressé à l'Université, dans un délai maximum de 8 jours ouvrés.

4.4.5. Notification des violations de données à caractère personnel

Le titulaire notifie à l'Université toute violation de données à caractère personnel dans un délai maximum de **48 heures ouvrées limité à 72 heures calendaires**, après en avoir pris connaissance, par courrier électronique, puis par téléphone et, enfin, par lettre recommandée avec accusé de réception.

Cette notification est accompagnée de toute documentation utile afin de permettre à l'Université, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

La notification contient au moins :

- La description de la nature de la violation de données à caractère personnel (catégories et nombre approximatif de personnes concernées par la violation et d'enregistrements de données)
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact
- La description des conséquences probables de la violation de données à caractère personnel
- La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord de l'Université, le titulaire communique, au nom et pour le compte l'Université, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les mêmes éléments que la notification ci-dessus.

Le sous-traitant n'est pas autorisé à notifier à l'autorité de contrôle compétente, au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel.

4.4.6. Aide du titulaire dans le cadre du respect par l'Université de ses obligations

Le titulaire aide l'Université pour la réalisation d'analyses d'impact relative à la protection des données ainsi que pour la réalisation de la consultation préalable de l'autorité de contrôle.

4.4.7. Mesures de sécurité des données à caractère personnel

Le titulaire s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles adaptées au risque, afin de respecter son obligation légale de sécurité dans son traitement de données à caractère personnel.

Le titulaire s'engage à remettre au responsable de traitement s'il en fait la demande, les documentations qu'il détient et met à jour, sur les mesures de sécurité technique et organisationnelle qu'il déploie pour assurer la sécurité des données personnelles.

4.4.8. Sort des données

Au terme de l'accord-cadre, le titulaire s'engage à envoyer toutes les données à caractère personnel au responsable de traitement. L'envoi devra s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du titulaire. Le titulaire devra justifier par écrit de la destruction.

4.4.9. Délégué à la protection des données

Le titulaire communique à l'Université le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément au règlement européen sur la protection des données. À défaut d'avoir désigné un délégué à la protection des données, il communique l'identité et les coordonnées de toute autre personne habilitée à traiter des questions relatives à la collecte et au traitement de données à caractère personnel.

4.4.10. Registre des catégories d'activités de traitement

Le titulaire déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'Université comprenant :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels autres prestataires et, le cas échéant, du délégué à la protection des données
- Les catégories de traitements effectués pour le compte de l'Université
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées le cas échéant
- Une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - La pseudonymisation et le chiffrement des données à caractère personnel
 - Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement
 - Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique
 - Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

4.4.11. Documentation

Le titulaire met à la disposition de l'Université, la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par l'Université ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

4.5. Obligations de l'Université

L'Université s'engage à :

- Documenter par écrit toute instruction concernant le traitement des données par le titulaire
- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du titulaire
- Superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire.

4.6. Prestations de services attendues de la part du titulaire

4.6.1. Prestations de services attendues pour la mise en œuvre

Les prestations de mise en œuvre chiffrées par les candidats dans le BPU doivent inclure :

- l'assistance que le titulaire devra apporter à l'Université pour l'intégration du système d'automatisation dans l'ensemble des dispositions mises en place par l'Université pour la protection des données personnelles
- et la fourniture de toutes les documentations requises.

Cette assistance portera notamment sur la cartographie et la liste des traitements liés au système d'automatisation que le titulaire devra tenir par écrit pour le compte de l'Université (registre des traitements).

Si des dispositions liées à la protection des données ne sont pas prévues au départ ou jugées insuffisantes par l'Université, le titulaire devra les adapter. Cela pourra notamment concerner :

- Les processus de purge automatique qui devront nécessairement être mis en place
- La minimisation des données à caractère personnel collectées dans le cadre des traitements mis en œuvre
- La gestion par les usagers de leurs données personnelles
- La gestion du consentement des usagers.

4.6.2. Prestations de services attendues pour la garantie et la maintenance

La garantie et la maintenance devront inclure obligatoirement et sans surcoût par rapport aux prix portés au BPU, toutes les prestations nécessaires au respect des obligations légales liées à la protection des données personnelles. À ce titre, le titulaire devra, notamment (liste non exhaustive) :

- Informer l'Université de toute modification apportée à un traitement et, cela, préalablement à la mise en place des modifications ; cela inclut la modification des pays où les données personnelles sont susceptibles d'être hébergées
- Informer l'Université de tout changement dans l'organisation ou le service délivré par son propre personnel ou ses sous-traitants lorsqu'ils impactent le traitement des données personnelles et, cela, préalablement à la mise en place des modifications
- Notifier l'Université de toute perte, divulgation ou vol de données sensibles, de toute suspicion ou découverte de faille ou incident de sécurité dans les plus brefs délais
- Informer l'Université de toute plainte ou demande d'exercice des droits, émise par une personne concernée par un traitement, sans répondre à la plainte ou demande sauf autorisation contraire et instructions précises données par l'Université
- Coopérer avec les autorités de protection des données, notamment en cas de contrôle ou de demande d'information qui lui serait adressée directement ou par l'intermédiaire de l'Université
- Prendre en compte toute évolution de la réglementation en vigueur sur les données personnelles
- Mettre à jour le registre des catégories d'activités de traitement dès qu'un traitement est modifié et, cela, quelle que soit la cause de cette modification.

5. Besoins techniques et fonctionnels concernant les équipements d'automatisation

5.1. Platines RFID

5.1.1. Description matérielle

- Les platines RFID fournies par le titulaire devront permettre l'écriture et la lecture de données dans les puces RFID.
- Il devra être possible de lire simultanément le contenu de plusieurs puces RFID :
 - Documents multiéléments
 - Documents en pile.
- Le temps de réponse pour la lecture ou l'écriture d'informations sera inférieur à 1 seconde. Si possible, la platine devra émettre un signal sonore et, de préférence, lumineux indiquant que le traitement est effectué ; le signal sonore devra pouvoir être désactivé.
- Les platines RFID seront installées sur les banques d'accueil et de prêt-retour des espaces publics et dans les bureaux du personnel. Elles seront simplement posées sur les banques et les bureaux.
- Les platines devront posséder une connexion informatique de type USB et devront être alimentées par cette connexion USB.
- Pour les postes utilisant les platines pour des opérations de lecture seulement, il sera apprécié que les platines soient automatiquement reconnues comme périphériques HID (« clavier ») sans nécessité d'installer un logiciel spécifique.
- Par l'intermédiaire d'un dispositif de « blindage », le rayonnement électromagnétique des platines devra être circonscrit à la face supérieure et donc très faible latéralement et sur la face inférieure.
- Le BPU permet de chiffrer deux modèles :
 - Un modèle peu encombrant (surface réduite) pour un usage standard
 - Un modèle pour le traitement de gros volumes permettant une lecture plus efficace de documents en pile.

5.1.2. Modalités d'implantation dans le mobilier – Ergonomie

Les modalités d'implantation des platines devront permettre de proposer des conditions de travail et d'utilisation ergonomiques pour le personnel, notamment en banque de prêt-retour.

Les platines devront avoir une sensibilité raisonnable au métal pouvant être présent dans les mobiliers.

5.1.3. Logiciels - Lien avec le SIGB

Le titulaire devra fournir les composants logiciels permettant l'utilisation des platines notamment en lien avec le SIGB Alma.

5.1.3.1. Logiciel d'encodage

Le titulaire devra fournir le logiciel permettant l'encodage des puces apposées sur les documents.

Le fonctionnement devra être possible depuis un PC professionnel de l'Université relié à une platine fournie par le titulaire, sans connexion réseau ou liaison avec le SIGB.

Le logiciel devra permettre :

- L'encodage
 - Des collections existantes en utilisant le code à barres déjà présent sur les documents y compris pour les documents multiéléments.

- Des nouveaux documents non équipés de code à barres avec une étiquette RFID ne comportant pas de code à barres pré-imprimé
 - L'écriture et la lecture pour vérification
 - Du numéro d'exemplaire SIGB
 - Du numéro RCR de la bibliothèque
 - De la protection antivol (activée ou bien désactivée) :
 - Le logiciel devra permettre de choisir la valeur antivol encodée par défaut dans la puce (antivol activé ou désactivé).
 - Le réencodage d'une étiquette déjà encodée (par exemple, si le code à barres est changé).
- Le logiciel sera insensible à la position de verrouillage majuscule/minuscule du clavier.

Le logiciel prendra également en compte les documents multiéléments dotés de plusieurs puces mais d'un unique numéro d'exemplaire SIGB :

- Encodage dans chaque puce du rang de la puce et du nombre total de puces.
- Cela devra permettre de vérifier la présence de tous les éléments équipés d'une puce via une simple lecture sur une platine RFID.

5.1.3.2. Logiciel pour l'utilisation courante des platines

Ce logiciel sera installé sur les postes professionnels. Les fonctions suivantes devront être disponibles :

- Sans lien avec le SIGB, ni connexion réseau :
 - Lecture, écriture et modification des données d'identification dans les étiquettes équipant les documents (identifiant du document et code RCR de la bibliothèque)
 - Lecture, écriture et modification de l'information antivol
 - Vérification de la complétude d'un document multiélément avec indication précise des éléments manquants ou étrangers.
- En lien avec le SIGB :
 - Le logiciel devra autoriser la lecture des identifiants des documents par le SIGB (par le module de recherche bibliographique, par exemple) pour assurer toutes les opérations du SIGB nécessitant une identification des exemplaires.
 - Le logiciel devra permettre l'activation-désactivation automatique de la puce RFID d'un document en fonction de la transaction (retour ou prêt) réalisée dans le SIGB sur un poste professionnel (dans la limite des capacités fonctionnelles d'Alma). Cela évitera la gestion manuelle de la position antivol de la platine (activation ou désactivation) par le personnel.
 - Le logiciel devra autoriser le fonctionnement de la platine avec le module « prêt secours » du SIGB en cas de problème réseau ou d'indisponibilité du serveur SIGB, dans la mesure où ce module « prêt secours » le permet.
- Possibilité de « mise en veille » du logiciel et de la platine pour empêcher la lecture aléatoire lors d'autres opérations effectuées par les agents sur les postes professionnels, pour limiter les rayonnements électromagnétiques et pour réaliser des économies d'énergie :
 - La mise en veille devra être réalisable manuellement et, si possible, automatiquement après une durée d'inactivité paramétrable.
- Temps de lecture/écriture maximum incluant les délais liés à la platine et au logiciel fourni par le titulaire, mais hors délais liés au SIGB : 0,25 seconde.
- Insensibilité à la position de verrouillage majuscule/minuscule et à l'activation/désactivation du pavé numérique du clavier

Certains postes professionnels pourront être équipés à la fois d'un lecteur de codes à barres et d'une platine RFID. Sur ces postes, les logiciels associés à la platine ne devront pas perturber le fonctionnement des lecteurs de codes à barres, y compris si ces lecteurs simulent une saisie clavier. Aucune manipulation pour basculer du mode « platine RFID » au mode « lecteur de codes à barres » ne devra être nécessaire.

Dans la mesure du possible, la configuration du logiciel sera centralisée et téléchargée automatiquement sur chaque PC professionnel.

Logiciel pour le tri rapide de documents

Dans la mesure du possible, la BU souhaite disposer d'un logiciel adapté au tri rapide de documents disposés en pile sur une platine. Ce logiciel devra autoriser la récupération de tous les identifiants des documents disposés sur la platine sans manipulation unitaire des documents par les bibliothécaires.

En lien avec le SIGB et dans la limite des opérations autorisées par le protocole SIP2 (ou Web Service), le logiciel fourni par le titulaire devra permettre :

- Pour chaque document présent dans la pile, l'affichage du titre, de l'auteur, de l'identifiant, de la cote, du statut (disponible, prêté, réservé, perdu...), du statut antivol, de la complétude, de la bibliothèque et de la localisation d'appartenance, avec possibilité de tri et filtrage sur ces éléments.
- Des opérations de retour par lot.

La liste devra se mettre à jour en temps réel si des documents sont ajoutés ou retirés de la pile.

Ce logiciel devra pouvoir fonctionner sans avoir besoin de l'identification d'un abonné (un logiciel de type « automate » ne convient donc pas).

Ce logiciel devra être installable sur les postes professionnels ou bien, préférentiellement, sera de type Web.

5.2. Portique antivol

5.2.1. Portique antivol fixé au sol

- L'issue principale de la BU restructurée devra être équipée d'un portique antivol fixé au sol (voir le paragraphe « 2.4.2 - Points spécifiques concernant les équipements »).
- Ce portique devra émettre une alarme sonore accompagnée d'une alarme visuelle lorsqu'un document équipé d'une étiquette RFID avec antivol activé sera placé entre les panneaux du portique.
- L'alarme devra être déclenchée alors que l'utilisateur porteur du document se trouve entre les panneaux ou ne s'est pas éloigné vers la sortie de plus de 50 cm.
- Le volume de l'alarme sonore devra être réglable.
- Le portique devra prendre en compte correctement les documents multimédias, dont certains peuvent être métallisés, ainsi que les documents multiéléments qui impliquent la lecture simultanée de plusieurs étiquettes RFID très proches les unes des autres et souvent superposées.
- L'alarme devra ne pas s'activer pour une étiquette dont le code RCR ne fait pas partie d'une liste de codes soumis à alarme (liste modifiable par l'Université ; la liste devra permettre de gérer le cas « code RCR absent de la puce »).
- Le portique devra être visuellement discret et s'harmoniser avec les choix d'aménagement de la BU.
- Il devra être conforme aux contraintes d'un établissement recevant du public :
 - Angles et arêtes arrondis pour éviter tout risque de blessure
 - Fixation au sol solide et bonne résistance aux chocs
 - Passage possible des voitures d'enfants et des fauteuils roulants.
- Le portique devra être relié au réseau informatique pour la remontée des données statistiques, les opérations de télémaintenance et l'affichage des titres des documents ayant déclenché une alarme.
- Le portique proposé devra supporter un espacement entre les panneaux pouvant aller jusqu'à 160 cm.
- Afin de limiter les rayonnements électromagnétiques et de réaliser des économies d'énergie, le portique devra se mettre en veille automatiquement (durée paramétrable) après le passage du dernier usager et se réactiver automatiquement à l'approche d'utilisateurs.

- Le portique devra être facilement intégrable dans le bâtiment :
 - Absence ou bien encombrement le plus faible possible d'un éventuel boîtier contrôleur associé au portique et non intégré dans les panneaux
 - Sensibilité raisonnable du portique vis-à-vis du métal présent dans les structures du bâtiment et notamment les huisseries
 - Distances minimales à respecter entre les différents équipements suffisamment faibles pour avoir peu d'effet sur les choix d'aménagement
 - Facilité et simplicité du raccordement courant fort/courant faible.
 - Respect du règlement de sécurité contre l'incendie relatif aux établissements recevant du public.
- Le BPU demande le chiffrage de différents portiques (de 1 à 5 unités de passage) avec fourniture ou pas d'un passe-câble métallique à installer sur le sol :
 - Le passe-câble sera mis en place si aucun fourreau dans le sol n'est disponible.
 - Le passe-câble devra être très résistant et présenter des pentes très faibles afin de ne pas être un obstacle sur lequel les usagers pourraient trébucher ou qui pourrait gêner le passage d'un fauteuil roulant.

5.2.2. **Box éventuellement associée au portique antivol**

Si la solution retenue requiert un boîtier informatique (« box ») pour le fonctionnement du portique, ce boîtier devra être le moins encombrant et le plus silencieux possible.

5.2.3. **Logiciel de gestion centralisée**

- Un logiciel devra permettre d'accéder de manière centralisée et à distance au portique antivol :
 - Configuration du portique
 - Informations :
 - État de fonctionnement du portique
 - Nombre d'alarmes déclenchées
 - Liste des documents ayant provoqué une alarme sur le portique :
 - Cette fonctionnalité devra être aisément accessible pour la vérification des documents d'un usager venant de déclencher une alarme ; un « push » automatique de cette information vers des postes professionnels associés au portique sera apprécié.
- Les informations seront disponibles pour une période paramétrable. Elles seront affichées sous forme de tableaux et de graphiques.
- Ces données seront exportables au format Excel, Word ou PDF.
- Les interfaces du logiciel de gestion centralisée seront de type Web et toutes disponibles en français.
 - L'accès sera nominatif. Des droits d'accès devront être gérés afin de pouvoir limiter les actions possibles pour l'utilisateur (par exemple, pas de changement de configuration autorisé).

5.3. **Compteurs de passage avec caméra**

Pour compter les passages au niveau de l'entrée principale de la BU restructurée, l'Université souhaite l'installation de compteurs de passage avec caméra fixés au plafond (voir le paragraphe « 2.4.2 - Points spécifiques concernant les équipements »).

Ces compteurs seront les plus discrets possible. Ils devront distinguer les entrées d'une part, et les sorties d'autre part, et couvrir une largeur de passage d'au moins 2 mètres.

Les compteurs devront être connectés au réseau et alimentés par son intermédiaire (PoE).

Afin que les compteurs ne puissent pas être assimilés à de la vidéoprotection, aucun flux vidéo ne devra pouvoir être extrait de ces équipements. Les seules informations générées par les compteurs devront être des informations de comptage totalement anonymes.

Les compteurs seront utilisés pour vérifier que la jauge maximale du bâtiment n'est pas dépassée. Ils devront être donc fiables, avec un faible taux d'erreurs de comptage. Si plusieurs compteurs sont installés, les informations de comptage devront être cumulées, sans double comptage.

Une page Web affichant le nombre de personnes présentes dans la BU devra être obligatoirement disponible. Cette page inclura un mécanisme permettant le rafraîchissement des données avec un décalage maximum de 30 secondes par rapport à la réalité. Il devra être également possible de paramétrer une fonction d'alarme permettant de déclencher l'envoi automatique d'une notification par mail en cas de dépassement de la jauge fixée par l'utilisateur.

Un logiciel de gestion centralisée devra permettre d'accéder aux informations de tous les compteurs de passage. Ce sera, si possible, le même logiciel que pour le portique antivol. Il devra permettre d'obtenir le nombre d'entrées, le nombre de sorties, le nombre de personnes présentes dans la BU par tranche de dates et tranche horaire (statistiques) et également « en temps réel » (décalage de moins de 15 minutes).

L'accès sera nominatif. Des droits d'accès devront être gérés afin de pouvoir limiter les actions possibles pour l'utilisateur (par exemple, pas de changement de configuration autorisé).

Affluences

La BU SHS est abonnée à la solution Affluences. Celle-ci devra pouvoir accéder en temps réel (décalage de moins de 15 minutes) aux informations de comptage provenant du système mis en place par le titulaire. Des postes sont prévus dans le BPU pour la réalisation du paramétrage nécessaire.

5.4. Automates de prêt-retour libre-service

5.4.1. Fonctionnalités attendues

- Les automates acquis par l'intermédiaire du présent accord-cadre devront autoriser les usagers à réaliser de manière autonome les opérations de prêt, de prolongation de prêt et de retour pour tous les types de documents proposés par les BU/Learning center de l'Université et équipés d'étiquettes RFID (imprimés, périodiques, CD, DVD et plus généralement documents multimédias et multiéléments).
- Les automates devront être facilement configurables par le personnel pour assurer
 - seulement les opérations de prêt et de prolongation de prêt
 - seulement les opérations de retour
 - à la fois le prêt et le retour.
- Un automate devra être désactivable ; son écran présentera alors un message d'indisponibilité.
- Les automates devront pouvoir être mis sous/hors tension automatiquement selon un calendrier paramétrable.
- Les automates dialogueront avec le SIGB Alma en utilisant le protocole SIP2. Toute fonctionnalité définie par ce protocole et supportée par Alma devra pouvoir être mise en œuvre.
- Les automates devront identifier les usagers selon les modalités suivantes :
 - Identification avec une carte CMS :
 - Les automates et le système de retour devront pouvoir identifier un usager en lisant le contenu de sa carte multiservice (carte CMS) par l'intermédiaire d'un lecteur de cartes ad hoc installé sur l'équipement et fourni par le titulaire. L'équipement devra obligatoirement utiliser le numéro lecteur stocké dans la carte pour identifier l'usager et non le CSN de la carte (voir « 2.1 - Contexte technique »).
 - Le règlement de la consultation du présent accord-cadre prévoit la fourniture d'un exemple de carte CMS aux candidats afin qu'ils puissent valider le bon fonctionnement de leurs équipements avec ces cartes.
 - Pour information, la BU utilise actuellement les lecteurs de cartes OMNIKEY CardMan 5x21, Identive CLOUD 4700F et ELATEC TWN4, mais les candidats peuvent proposer un autre modèle de lecteur dès lors qu'il est compatible avec les cartes CMS.
 - Identification avec une carte uniquement dotée d'un code à barres de type Interleaved 2 of 5 (lecteurs extérieurs).

- La fonction d'identification par saisie manuelle du numéro lecteur devra pouvoir être désactivée si elle est disponible, la BU ne souhaitant pas sa mise en œuvre.
- Un message très visible devra inviter l'utilisateur à se déconnecter en fin d'opération.
- Une déconnexion automatique devra être réalisée par l'automate après une durée d'inactivité paramétrable.
- Les automates devront offrir les fonctionnalités suivantes pour les transactions de prêt-retour :
 - Les transactions de retour devront être réalisables sans identification de l'utilisateur (comportement paramétrable).
 - Les automates devront identifier les documents à partir de leur étiquette RFID.
 - Ils devront activer / désactiver la protection antivol RFID des documents une fois la transaction validée par le SIGB.
 - Ils devront interdire une transaction :
 - Sur refus du SIGB (dossier de l'inscrit en litige, quotas de prêt dépassés, expiration de l'abonnement, document non empruntable, document réservé, document ne pouvant faire l'objet d'un prêt et/ou retour par l'intermédiaire d'un automate...)
 - Si le code RCR présent dans la ou les étiquettes ne fait pas partie d'une liste de codes autorisés (liste modifiable par l'Université ; la liste devra permettre de gérer le cas « code RCR absent de la puce »)
 - En raison d'une anomalie détectée par l'automate au niveau d'un document multiélément (élément manquant ou étranger).
 - Ils devront afficher des messages précis et clairs à l'utilisateur (messages paramétrables par l'Université) ainsi que tous les messages transmis par le SIGB (raison du refus d'une transaction, message précisant un éventuel lieu de dépôt particulier pour le document retourné, etc.).
- Les automates autoriseront également les usagers à consulter leur compte d'inscrit SIGB :
 - Dans la limite des informations transmises par le SIGB, seront affichés :
 - Les prêts en cours avec indication des retards
 - Les réservations et mises de côté en cours avec indication des documents disponibles
 - Les amendes dues et les dates de suspension associées
 - Les messages à destination de l'utilisateur.
 - Les usagers devront pouvoir procéder à la prolongation d'un ou plusieurs prêts sans que la présence des documents ne soit requise.
- Les automates devront pouvoir délivrer un reçu aux usagers (identification de l'utilisateur, liste des documents rendus ou empruntés, date limite de prêt...). Le reçu devra être paramétrable par l'Université. Les usagers devront pouvoir choisir :
 - De ne recevoir aucun reçu
 - De le recevoir par mail à l'adresse présente dans leur compte SIGB
 - De le charger sur leur smartphone par l'intermédiaire d'un QR code affiché sur l'écran de l'automate
 - D'imprimer le reçu sur l'imprimante à ticket qui équipera obligatoirement chaque automate.
- Dans toutes les opérations décrites ci-dessus, le temps de traitement par les automates des informations transmises par le SIGB devra être faible :
 - Pour une opération (identification de l'utilisateur, prêt, retour, affichage du dossier d'abonné, prolongation...), pas plus de 0,25 seconde de traitement ajouté par l'automate au délai d'exécution par le SIGB des requêtes SIP2 nécessaires à l'opération.
- Un système de prêt secouru interne aux automates devra permettre à ceux-ci de continuer à fonctionner en cas de panne du réseau informatique ou du SIGB et, cela, de la manière la plus transparente possible pour les usagers.
- Un chargement automatique dans le SIGB des transactions sauvegardées en mode secouru devra être effectué par les automates après la réapparition du SIGB. Un écran destiné au personnel devra

permettre d'afficher les problèmes éventuellement constatés (transactions non acceptées par le SIGB) ; la liste devra être exportable.

- Les IHM proposées aux usagers présenteront au minimum les caractéristiques suivantes :
 - La navigation se fera par interface tactile et devra être intuitive et ergonomique.
 - Les écrans seront en langue française. La disponibilité de langues complémentaires sera appréciée ; les langues complémentaires accessibles aux usagers devront être paramétrables par l'Université.
 - Une personnalisation de l'interface devra être possible (logo, nom de la BU) et les textes (incluant les messages d'erreur) devront être modifiables par le personnel.
 - La possibilité de disposer d'un choix de plusieurs habillages graphiques sera appréciée.
 - L'écran d'accueil des automates devra permettre la diffusion de messages d'information et de communication de l'Université :
 - Gestion d'un cadre permettant d'intégrer du code HTML embed ou bien diffusion d'une série d'images téléchargeables par les administrateurs, etc.
 - Les IHM devront présenter un bouton de demande d'assistance. Celui-ci activera un signal lumineux sur l'automate facilement visible par le personnel et fera apparaître un message (fenêtre pop-up) sur certains postes professionnels (liste paramétrable par automate).
- Aucun système de paiement n'est à prévoir.

5.4.2. Caractéristiques physiques et modèles

- Les automates et notamment les écrans devront présenter des caractéristiques leur permettant de résister à un usage en libre-service par du public.
- Ils devront être résistants à l'utilisation régulière de produits désinfectants.
- L'Université souhaite pouvoir choisir les modèles d'automates à acquérir parmi les modèles suivants :
 - Modèle habillé, prêt à l'emploi, sur pied (borne), non réglable en hauteur
 - Modèle habillé, prêt à l'emploi, sur pied (borne), réglable en hauteur par le public
 - Modèle habillé, prêt à l'emploi, sur pied (borne), 3^e modèle disponible dans le catalogue du titulaire
 - Modèle habillé, prêt à l'emploi, à poser sur du mobilier :
 - Le BPU permet le chiffrage de deux modèles présentant des encombrements différents, un modèle peu volumineux ayant la préférence de l'Université.
 - Modèle à intégrer dans du mobilier sur mesure fourni par l'Université :
 - Ce modèle devra obligatoirement comporter un PC tout-en-un pour éviter d'avoir à masquer une unité centrale indépendante de l'écran (voir le paragraphe « 2.4.2 - Points spécifiques concernant les équipements » pour plus de détails)
- Les automates habillés devront être harmonisables d'un point de vue esthétique avec les choix d'aménagement et de décoration de la BU.
- La possibilité de choisir les matériaux d'habillage, leur coloris ou de pouvoir appliquer des décors sur l'habillage sera appréciée.

5.4.3. Accessibilité

- Les automates devront être « accessibles » :
 - Personnes à mobilité réduite ou de petite taille :
 - Modèle « habillé, prêt à l'emploi, sur pied, réglable en hauteur par le public » :
 - La plage de réglage en hauteur et la manipulation nécessaire pour le réglage devront autoriser son usage par des personnes en fauteuil roulant ou de petite taille sans recours à l'assistance d'une personne tierce.
 - Modèle « habillé, prêt à l'emploi, sur pied, non réglable en hauteur » :
 - Ce modèle devra pouvoir être commandé dans une configuration appropriée à un usage par des personnes en fauteuil roulant ou de petite taille.

- Personnes malvoyantes :
 - Les automates devront proposer un habillage graphique particulièrement adapté aux personnes malvoyantes (son activation devra être extrêmement aisée depuis l'habillage standard).
 - Les interfaces devront être compatibles avec le RGAA 4.1 pour les éléments applicables.

5.4.4. Intégration bâtiment et mobilier

La facilité d'intégration des automates dans le bâtiment et les mobiliers constitue un critère important pour l'Université :

- Distances minimales à respecter entre les différents équipements (notamment les systèmes antivol) suffisamment faibles pour avoir peu d'effet sur les choix d'aménagement
- Respect du règlement de sécurité contre l'incendie relatif aux établissements recevant du public
- Sensibilité raisonnable des équipements vis-à-vis du métal présent dans les structures du bâtiment et des mobiliers
- Facilité et simplicité du raccordement courant fort/courant faible
- Pour les automates à intégrer dans du mobilier sur mesure :
 - PC tout-en-un obligatoire
 - Modalités d'implantation des matériels permettant de proposer des conditions d'utilisation ergonomiques pour le public.

5.4.5. Logiciel de gestion centralisée

- Un logiciel devra permettre d'accéder de manière centralisée à l'ensemble des automates sans qu'il soit nécessaire de se connecter individuellement à chaque automate :
 - Configuration de tout ou partie des automates en une seule opération, la configuration individuelle restant possible
 - Tableaux de bord synthétiques reflétant l'état de fonctionnement des automates
 - Accès à l'ensemble des transactions de prêt-retour (avec possibilité de filtre par date, automate, inscrit SIGB, type de transaction, résultat de la transaction...) ; il devra être aisé de retrouver une transaction en cas de litige avec un inscrit SIGB (dans la limite des obligations légales concernant les données personnelles)
 - Accès à différentes statistiques d'usage : nombre et type des transactions, nombre de consultations du dossier d'inscrit SIGB, nombre de prolongations de prêt... sur une période
 - Pour toutes ces données et informations, possibilité de générer des rapports et exportations au format Excel, Word ou PDF.
- Les interfaces du logiciel de gestion centralisée seront de type Web et toutes disponibles en français.
- L'accès sera nominatif. Des droits d'accès devront être gérés afin de pouvoir limiter les actions possibles pour l'utilisateur (par exemple, pas de changement de configuration autorisé).

5.5. Système de retour

- La BU SHS restructurée devra être équipée d'un système de retour RFID comportant :
 - 1 boîte de retour intérieure
 - 1 robot de tri à 7 bacs
 - 2 bacs supplémentaires pour remplacement immédiat d'un bac plein par un bac vide.

Aucun point d'insertion de documents situé dans le local du robot et destiné au personnel n'est nécessaire.

Voir le paragraphe « 2.4.2 - Points spécifiques concernant les équipements » pour le plan d'implantation.

5.5.1. Boîte de retour SIP2

- La boîte de retour sera intérieure.
 - Elle devra autoriser les usagers à réaliser de manière autonome le retour de tous les types de documents proposés par les BU/Learning center de l'Université et équipés d'étiquettes RFID (imprimés, périodiques, CD, DVD et plus généralement documents multimédias et multiéléments).
 - La boîte dialoguera avec le SIGB par l'intermédiaire du protocole SIP2. Si cela s'avère nécessaire, toute fonctionnalité définie par ce protocole et supportée par Alma devra pouvoir être mise en œuvre.
 - La boîte sera équipée d'un écran.
 - En complément des informations affichées sur l'écran, un signal lumineux (vert, rouge...) pour indiquer aux usagers la bonne prise en compte des documents déposés ou, au contraire, le refus de prise en compte des documents sera apprécié.
 - Les IHM proposées aux usagers sur l'écran présenteront au minimum les caractéristiques suivantes :
 - La navigation se fera par interface tactile et devra être intuitive et ergonomique.
 - Les écrans seront en langue française. La disponibilité de langues complémentaires sera appréciée ; les langues complémentaires accessibles aux usagers devront être paramétrables par l'Université.
 - Une personnalisation de l'interface devra être possible (logo, nom de la BU) et les textes et messages devront être modifiables par l'Université.
 - L'écran d'accueil de la boîte devra permettre la diffusion de messages d'information et de communication de l'Université :
 - Gestion d'un cadre permettant d'intégrer du code HTML embed ou bien diffusion d'une série d'images téléchargeables par les administrateurs, etc.
 - Aucune fonctionnalité nécessitant l'identification de l'utilisateur ne sera mise en œuvre :
 - La boîte sera uniquement utilisée pour le retour des documents.
 - Aucun lecteur de carte CMS ni aucun lecteur de cartes code à barres ne sont donc requis.
 - La fonction d'identification par saisie manuelle du numéro lecteur devra pouvoir être désactivée si elle est disponible.
 - La boîte devra offrir les fonctionnalités suivantes pour les transactions de retour effectuées par les usagers :
 - La boîte devra identifier les documents à partir de leur étiquette RFID.
 - Les usagers devront pouvoir retourner des documents sans s'identifier.
 - La boîte devra activer la protection antivol RFID des documents acceptés en retour.
 - La boîte devra traiter spécifiquement les documents non reconnus et les transactions de retour refusées :
 - suite à une anomalie détectée par la boîte au niveau d'un document :
 - Document non reconnu
 - Code RCR présent dans la ou les étiquettes absent d'une liste de codes autorisés (liste modifiable par l'Université ; la liste devra permettre de gérer le cas « code RCR absent de la puce »)
 - Document multiélément avec élément manquant ou étranger
 - Etc.
 - sur réponse négative du SIGB (dossier de l'inscrit en litige, document ne pouvant être retourné à la BU SHS ou par l'intermédiaire de la boîte, etc.).
- Pour chaque grand type d'anomalie, le système devra être paramétrable pour rejeter le document (par exemple, document non reconnu) ou le diriger vers le bac spécifique aux erreurs (par exemple, document incomplet).

- La boîte devra :
 - Afficher tous les messages d'anomalies et tous les messages de circulation transmis par le SIGB.
 - Délivrer un reçu aux usagers (identification de l'utilisateur, liste des documents rendus). Le reçu devra être paramétrable par l'Université. Les usagers devront pouvoir choisir :
 - De ne recevoir aucun reçu
 - De le recevoir par mail à l'adresse présente dans leur compte SIGB
 - De le charger sur leur smartphone par l'intermédiaire d'un QR code affiché sur l'écran de la boîte
 - D'imprimer le reçu sur l'imprimante à ticket qui équipera la boîte.
- La boîte retour devra présenter des caractéristiques lui permettant de résister à un usage en libre-service par du public.
- La boîte devra être activable/désactivable :
 - À partir d'un calendrier horaire
 - En permanence (en cas de panne, par exemple).
- La boîte sera dotée d'une trappe qui sera fermée lorsque la boîte sera désactivée. Un message adéquat sera affiché sur l'écran. Les usagers ne devront pas pouvoir ouvrir la trappe.
- Il devra être possible de désactiver automatiquement la boîte de retour lorsqu'un ou plusieurs bacs du robot de tri seront pleins.
- Le temps de traitement par la boîte des informations transmises par le SIGB devra être faible :
 - Pour une opération de retour, pas plus de 0,25 seconde de traitement ajouté par la boîte au délai d'exécution par le SIGB des requêtes SIP2 nécessaires à l'opération (hors transport par le robot de tri).
- Une fonction de retour secouru interne à la boîte de retour devra lui permettre de continuer à fonctionner en cas de panne du réseau informatique ou du SIGB et, cela, de la manière la plus transparente possible pour les usagers :
 - Les documents seront envoyés vers le bac « erreurs ».
 - Un chargement automatique dans le SIGB des transactions sauvegardées en mode secouru devra être effectué par la boîte après la réapparition du SIGB. Un écran destiné au personnel devra permettre d'afficher les problèmes éventuellement constatés (transactions non acceptées par le SIGB) ; la liste devra être exportable.
- Accessibilité :
 - La boîte de retour devra être « accessible » :
 - Pour les personnes à mobilité réduite en fauteuil roulant ou de petite taille
 - Pour les personnes malvoyantes :
 - La boîte devra proposer un habillage graphique particulièrement adapté aux personnes malvoyantes (son activation devra être extrêmement aisée depuis l'habillage standard).
 - Les interfaces devront être compatibles avec le RGAA 4.1 pour les éléments applicables.

5.5.2. Robot de tri

- La boîte de retour sera reliée à un robot de tri à 7 bacs.
- Le bac cible pour un document sera calculé par l'intermédiaire d'une matrice de tri interne à la boîte de retour à partir des informations retournées par le SIGB pour le document ou bien en utilisant le « sort bin » s'il est calculé par le SIGB. Un bac sera affecté aux documents en erreur.

- Lorsqu'un bac sera plein, un « push » automatique d'un avertissement vers des postes professionnels associés au système de retour devra être réalisé (fenêtre pop-up, éventuellement mail...).
- Si possible, le mécanisme utilisera une cellule détectant physiquement que la hauteur maximale de documents est atteinte et non un simple comptage du nombre de documents déposés dans le bac.
- Le robot de tri devra être évolutif et supporter l'ajout de bacs supplémentaires.
- Les bacs seront dotés d'un fond mobile s'enfonçant sous le poids des livres ou de tout autre mécanisme équivalent afin d'éviter que les documents ne subissent des chocs trop violents lors de leur arrivée dans le bac et afin que la récupération des documents par le personnel soit la plus aisée possible.
- Les bacs seront dotés de roulettes multidirectionnelles avec freins.
- Le BPU permet le chiffrage de quatre modèles de bacs ayant des caractéristiques et des capacités différentes. **Les candidats doivent obligatoirement chiffrer au moins 2 modèles distincts.**

5.5.3. Autres équipements

Les coûts portés dans le BPU devront intégrer toutes les alimentations, tous les boîtiers électroniques et tous les équipements informatiques nécessaires au fonctionnement, au paramétrage et à la surveillance du système de retour.

5.5.4. Intégration bâtiment

Contraintes incendie

- Le système de retour devra respecter le règlement de sécurité contre l'incendie relatif aux établissements recevant du public.

Raccordement courant fort et courant faible

- Les candidats décriront avec précision les modalités de raccordement courant fort/courant faible du système de retour.

Contraintes esthétiques

- L'habillage de la boîte de retour devra être harmonisable d'un point de vue esthétique avec les choix d'aménagement et de décoration faits pour la BU SHS.

Positionnement du robot dans la salle dédiée

- Voir le paragraphe « 2.4.2 - Points spécifiques concernant les équipements » pour le plan d'implantation.

Contraintes sonores

- Dans les espaces publics et dans la salle du robot où le personnel interviendra fréquemment, le système de retour devra présenter un niveau sonore raisonnable.

Contraintes de poids

- **Les candidats préciseront la charge minimale par m² que le plancher doit supporter.**

Contraintes de dimensions pour la livraison

- Les différents éléments à assembler pour constituer la boîte de retour et le robot de tri devront emprunter les portes extérieures et intérieures du bâtiment. Les contraintes de taille ne sont pas encore connues.
- Même si le local du système de retour est situé en rez-de-forum, l'utilisation d'un monte-charge pourrait être nécessaire si les livraisons doivent arriver par les niveaux inférieurs.
- **Les candidats préciseront les dimensions minimales attendues pour les portes et le monte-charge.**

5.5.5. Logiciel de gestion centralisée

- Un logiciel devra permettre la gestion de la boîte et de son robot :
 - Configuration de la boîte et du robot de tri
 - Tableaux de bord synthétiques reflétant l'état de fonctionnement de la boîte de retour et du robot de tri associé
 - Accès à l'ensemble des transactions de retour (avec possibilité de filtre par date, inscrit SIGB, résultat de la transaction...) ; il devra être aisé de retrouver une transaction en cas de litige avec un inscrit SIGB (dans la limite des obligations légales concernant les données personnelles)
 - Liste des documents présents dans le bac « Erreurs » et raison de leur transfert dans ce bac
 - Accès à différentes statistiques d'usage complémentaires : taux horaire de transaction, nombre de refus d'ouverture de la trappe, nombre de documents rejetés (donc non transférés dans un bac), nombre de documents transférés dans chaque bac, nombre de débordements de chaque bac, etc.
 - Pour toutes ces données et informations, possibilité de générer des rapports et exportation au format Excel, Word ou PDF.
- Si possible, ce logiciel prendra également en charge les automates et permettra d'obtenir des vues consolidées sur l'ensemble des transactions de prêt-retour réalisées par le public à partir des équipements d'automatisation.
- Les interfaces du logiciel d'accès centralisé seront de type Web et toutes disponibles en français.
- L'accès sera nominatif. Des droits d'accès devront être gérés afin de pouvoir limiter les actions possibles pour l'utilisateur (par exemple, pas de changement de configuration autorisé).

5.5.6. Chiffrage dans le BPU

- Le BPU demande le chiffrage d'une configuration comportant :
 - La boîte de retour intérieure avec un robot de tri à 7 bacs sans les bacs
- Des postes supplémentaires permettent de chiffrer 4 modèles de bacs :
 - 2 doivent être chiffrés obligatoirement ; ces 2 bacs doivent avoir des capacités différentes.

5.6. Terminaux RFID mobiles

5.6.1. Inventaires, recherches, modification des données

Les terminaux devront permettre la lecture et l'écriture des puces RFID des documents sans avoir besoin de manipuler individuellement les documents. Ils devront permettre de réaliser les opérations suivantes :

- Inventaires :
 - Pause possible pendant un inventaire (de quelques minutes à plusieurs jours)
 - Génération de la liste des documents inventoriés
 - Chargement de la liste dans le SIGB (identifiant des documents)
 - Affichage de la liste sur le terminal pendant l'inventaire (y compris s'il est en pause) et une fois l'inventaire terminé :
 - Affichage a minima de titre, auteur, identifiant, cote, statut (disponible, prêté, réservé, perdu...), statut antivol, complétude, bibliothèque et localisation d'appartenance
 - Tri et filtrage de la liste par statut, complétude, bibliothèque et localisation d'appartenance
- Vérification du classement des documents
- Recherche de documents particuliers (pendant ou hors inventaire) :
 - Documents particuliers (saisie des identifiants au début de la recherche)
 - Documents perdus
 - Documents prêtés ou réservés
 - Documents avec un statut antivol particulier (activé ou non activé)
 - Documents n'appartenant pas à des bibliothèques ou des localisations précisées au début de la recherche

- Documents appartenant à une liste spécifique créée par les bibliothécaires dans le SIGB et chargée dans le terminal au début de la recherche.
- Modification des données des étiquettes :
 - Réencodage (changement de norme, inscription de données complémentaires)
 - Activation ou désactivation systématique du statut antivol
- Dialogue en temps réel avec le SIGB par l'intermédiaire du protocole SIP2 pour l'obtention des informations sur les exemplaires : titre, auteur, identifiant, cote, statut (disponible, prêté, réservé, perdu...), bibliothèque et localisation d'appartenance...
 - Un fonctionnement dégradé sans liaison avec le SIGB devra être possible.

Lors d'une recherche ou lors de la vérification du classement, les lecteurs devront signaler en temps réel la détection d'un problème ou de l'un des documents objet de l'opération ; l'opérateur ne devra pas avoir à examiner plus de 30 cm linéaires des derniers documents inventoriés.

5.6.2. Prêts et retours

Dans la mesure du possible, en lien avec le SIGB, les terminaux mobiles proposeront des fonctionnalités permettant d'effectuer le prêt et le retour des documents, d'accéder au dossier de l'adhérent et de prolonger les prêts :

- Identification de l'adhérent (numéro lecteur) :
 - À partir de la carte multiservice (CMS) de l'Université (si possible)
 - À partir de la carte code à barres dont sont dotés les lecteurs extérieurs
 - À partir d'un code à barres affiché dans une application pour smartphone (par exemple, une application dédiée au stockage dématérialisé de cartes)
 - À partir de la saisie manuelle directe du numéro lecteur de l'abonné
- Identification des documents à partir de leur étiquette RFID
- Outre les prêts, retours et prolongations unitaires (un document à la fois), possibilité d'effectuer les mêmes transactions par lot (par exemple, pour une rangée de documents)
- Dialogue en temps réel avec le SIGB par l'intermédiaire du protocole SIP2
- Activation ou désactivation du statut antivol en fonction de la transaction réalisée
- Si possible, impression d'un ticket de transaction (prêt ou retour) par l'intermédiaire d'une imprimante Bluetooth (la fourniture de l'imprimante Bluetooth est hors accord-cadre).

5.6.3. Caractéristiques générales

Les terminaux mobiles seront dotés :

- d'un écran tactile permettant le pilotage du terminal mobile
- d'une connexion Wi-Fi
- d'une connexion Bluetooth
- d'un navigateur Internet récent (si possible).

Les terminaux seront légers et dotés d'une batterie disposant d'une bonne autonomie. Celle-ci devra permettre le travail d'inventaire sur une plage de 7 heures ; si nécessaire, une pause méridienne d'une heure au maximum pourra être ajoutée afin d'assurer une recharge de la batterie.

Les terminaux devront pouvoir être facilement tenus d'une seule main par une personne se déplaçant dans les espaces publics ou les magasins.

5.7. Remarque générale concernant l'alimentation PoE des matériels d'automatisation

Pour chaque équipement pouvant être alimenté par l'intermédiaire de sa connexion Ethernet (PoE), le prix porté dans le BPU doit obligatoirement inclure un injecteur PoE afin que l'alimentation de l'équipement puisse être éventuellement réalisée à partir d'une prise 220 V installée à proximité si cela s'avère nécessaire.

6. Prestations de services attendues pour la mise en œuvre

6.1. Prestations de conduite de projet - Calendrier

6.1.1. Calendrier prévisionnel des prestations

Les informations données dans ce paragraphe sont indicatives et pourront être modifiées par l'Université.

Le titulaire doit prévoir une réalisation en trois phases :

- Phase 1 : élaboration du plan d'implantation
 - Voir « 6.3 - Prestations de conseil pour l'implantation des équipements d'automatisation dans la BU SHS restructurée et l'aménagement des espaces »
 - Cette phase sera lancée dès l'attribution de l'accord-cadre.
- Phase 2 : spécifications de la configuration et du paramétrage
 - Cette phase inclura le maquetage « automates et système de retour »
 - Voir « 6.4 - Prestations de spécifications de la configuration et du paramétrage des équipements d'automatisation »
 - Réalisation de septembre 2025 à décembre 2025
- Phase 3 : installation des équipements dans la BU SHS restructurée :
 - La BU SHS restructurée ouvrira ses portes à la rentrée de septembre 2026.
 - L'installation des équipements RFID est prévue au 1^{er} trimestre 2026.

Hors formations, les opérations de vérification suivront les étapes MOM, VA et VSR définies par le CCAG-TIC. La VSR aura une durée de 3 mois après la mise en production.

6.1.2. Conduite de projet et équipe proposée

Organisation de l'Université

- Un groupe projet assurera le suivi la mise en œuvre. Il sera constitué :
 - MOA :
 - De représentants de l'Université
 - De représentants de l'assistance technique à maîtrise d'ouvrage (ATMO société Mupy Conseil)
 - MOE :
 - De représentants du groupement attributaire du marché global de performance (mandataire société Rabot Dutilleul) et notamment de la société en charge des aspects VDI/RFID (société Savoir Sphère).

Conduite de projet

Le titulaire devra assurer la conduite de projet associée aux services et fournitures de l'accord-cadre :

- Il devra fournir un document décrivant l'organisation du projet (plan qualité succinct).
- Il devra organiser des réunions de suivi de projet et produire les ordres du jour et les comptes rendus. Doivent être prévus :
 - Un comité de pilotage de lancement en présentiel
 - Des réunions plénières régulières de suivi de projet avec le groupe projet en présentiel (fréquence à définir par le titulaire)
 - Des points rapides avec le groupe projet en distanciel :
 - La durée de chaque point n'excédera pas une heure.
 - Par défaut, ces points rapides auront lieu toutes les deux semaines ; dans les périodes moins chargées, sur décision du groupe projet, ils pourront avoir lieu à une fréquence moindre.

- Des comités de pilotage en présentiel (réunion de lancement incluse) :
 - Le titulaire aura la charge d'élaborer et de communiquer l'ordre du jour, de fournir l'ensemble des éléments nécessaires à son bon déroulement (suivi des actions complété, planning mis à jour, points d'alertes à remonter...) et de rédiger le compte rendu.
 - Le titulaire devra assurer jusqu'à 3 comités de pilotage en plus de la réunion de lancement.
 - Le titulaire devra tenir à jour le calendrier projet au fur et à mesure de l'avancement de la mise en œuvre.
 - Il devra produire des notes techniques ou projet sur tout sujet le nécessitant.
 - Il devra assurer un suivi des actions et des risques.
 - Il devra offrir une plate-forme de gestion de projet accessible depuis Internet et permettant au groupe projet :
 - d'accéder à tous les documents du projet et au planning
 - de déclarer et suivre les anomalies lors des opérations de vérification
 - de suivre les tâches affectées aux membres du groupe projet.
- La gestion des accès devra être nominative.

Les réunions en présentiel pourront avoir lieu dans tout bâtiment situé sur le Campus Pont de Bois à Villeneuve-d'Ascq. Exceptionnellement et uniquement après accord du groupe projet, des réunions prévues en présentiel pourront avoir lieu en distanciel.

Structure de l'équipe proposée

Le titulaire devra fournir une équipe dont la structure et les membres présenteront toutes les compétences nécessaires au suivi et à la réalisation des différents types de prestations de services décrites dans le présent chapitre.

6.2. Prestations concernant l'équipement des collections

Aucune prestation concernant l'équipement des collections n'est attendu de la part du titulaire :

- La BU SHS poursuivra la politique d'équipement déjà en place.
- Aucune collection n'est à équiper spécifiquement en lien avec le présent accord-cadre.

6.3. Prestations de conseil pour l'implantation des équipements d'automatisation dans la BU SHS restructurée et l'aménagement des espaces

Le titulaire aura une mission de conseil importante concernant les aménagements nécessaires aux équipements RFID.

- **Contraintes d'environnement et règles de sécurité :**
Le titulaire devra prodiguer tous les conseils nécessaires concernant les contraintes d'environnement :
 - Sensibilité des équipements proposés à l'environnement métallique lié aux bureaux, aux étagères, aux huisseries, à la structure du bâtiment...
 - Règles d'implantation des équipements et distances minimales à respecter entre deux platines, entre une huisserie métallique et un portique antivol, etc.
 - Respect des règles de sécurité dans les établissements recevant du public
- **Aménagement des espaces :**
À la fois sous l'angle « usagers » et sous l'angle « documents », le titulaire donnera tous les conseils utiles concernant l'organisation des espaces d'un point de vue technique et ergonomique et en termes de gestion des flux.

- **Plan d'implantation et validation des travaux :**

Le titulaire élaborera un plan d'implantation précis des différents équipements détaillant les câblages et fourreaux requis ainsi que les attendus pour tous les travaux préparatoires à réaliser. Ce plan sera réalisé en collaboration avec la MOA et avec la MOE en charge de la structuration du bâtiment. Le plan d'implantation devra obligatoirement être validé par la MOA et la MOE.

Le titulaire devra réceptionner officiellement les travaux d'aménagement réalisés par la MOE.

Le titulaire devra émettre toutes les réserves qu'il jugera nécessaires lors de la réception de ces travaux dans la mesure où des éléments ne seraient pas conformes à la solution retenue et validée conjointement par le titulaire, la MOA et la MOE.

Toute modification sur les aménagements qui sera due au non-respect par le titulaire de la solution validée initialement ou qui portera sur un élément n'ayant pas fait l'objet de réserve à la réception des travaux sera à la charge financière du titulaire.

Le titulaire devra participer à des réunions de chantier. Cinq réunions sont à prévoir au maximum.

- **Intégration des équipements RFID dans la BU SHS :**

Le titulaire prodiguera tous les conseils et livrera tous les documents nécessaires ;

- À l'harmonisation avec les choix d'aménagement et de décoration décidés pour la BU SHS :
 - Présentation des possibilités d'habillage des équipements RFID
- À l'intégration de ses équipements dans les mobiliers :
 - Intégration des platines et des automates
 - Conseils concernant les structures et éléments métalliques des mobiliers
 - Respect des règles d'ergonomie
- À l'accessibilité :
 - Pour les personnes à mobilité réduite et de petite taille
 - Pour les personnes malvoyantes.

6.4. Prestations de spécifications de la configuration et du paramétrage des équipements d'automatisation

Le titulaire devra élaborer un dossier complet de configuration et de paramétrage du système d'automatisation qui sera remis au groupe projet.

Les besoins de l'Université devront être recueillis au cours de réunions d'instruction spécifiques.

Préalablement à l'instruction, une session de présentation de la solution RFID du titulaire sera organisée afin que le groupe projet et le personnel de la BU SHS puissent en prendre connaissance (cf. « 6.7.2.1 - Présentation de la solution du titulaire »).

Le dossier de configuration et de paramétrage devra notamment prendre en compte :

- L'intégration avec le SIGB Alma :
 - Le titulaire devra participer aux réunions ou échanges qui pourraient s'avérer nécessaires avec le fournisseur de ce SIGB et le groupe projet afin de mettre en place un interfaçage optimal entre les équipements d'automatisation et ce SIGB.
- L'intégration avec la solution Affluences.

Par ailleurs, le groupe projet mettra en place un groupe de travail dédié pour le paramétrage des automates et du système de retour (maquettage). Ce groupe de travail étudiera l'adaptation éventuelle des règles de circulation du SIGB, le calcul du « sort bin » par le SIGB pour le robot de tri, la définition du paramétrage des matériels d'automatisation, l'adaptation éventuelle des messages du SIGB et des matériels d'automatisation, etc. :

- Le titulaire devra participer au travail de spécifications réalisé par le groupe de travail (au moins 3 réunions d'une demi-journée sur site).
- Pour les automates, le travail sera réalisé sur un automate acquis de manière anticipée par l'Université.

Les candidats préciseront comment pourra être réalisé le travail sur le système de retour et son robot de tri, ce travail allant débiter avant la livraison des équipements.

6.5. Prestations d'installation des matériels, de déploiement des logiciels et de réalisation des paramétrages

Installation et mise en ordre de marche des matériels dans la BU SHS restructurée

Le titulaire de l'accord-cadre devra assurer la livraison et l'installation physique de l'ensemble des équipements dans la BU SHS restructurée. Les prix portés dans le BPU doivent donc intégrer tous les frais associés.

Doivent être notamment prévus par le titulaire :

- Le raccord courant fort et courant faible de tous les équipements incluant la mise en place éventuelle d'injecteurs PoE (cf. « 5.7 - Remarque générale concernant l'alimentation PoE des matériels d'automatisation »)
- L'installation du portique antivol incluant les perçages dans le sol, la fixation des panneaux et l'installation éventuelle d'un passe-câble métallique
- L'installation des systèmes de comptage par caméra incluant les perçages dans le plafond ou les cloisons et la fixation des systèmes
- L'installation des automates incluant l'intégration éventuelle dans un meuble en collaboration avec le fournisseur de mobilier
- L'installation de la boîte de retour incluant les perçages et fixations requis ainsi que l'étanchéification avec la mise en place de joints ad hoc entre la boîte et la cloison.

Le titulaire devra installer ses équipements selon les règles de l'art et en coordination avec les entreprises réalisant les travaux.

Après chaque installation, le titulaire assurera le nettoyage du chantier qui devra rester libre de tous déchets et emballages. Les déchets laissés sur place par le titulaire seront évacués par l'Université à ses frais. En cas de dégradation des locaux, les travaux de remise en état seront également effectués aux frais du titulaire.

Le titulaire devra s'adapter au calendrier d'intervention qui sera définie par la MOE. Ce calendrier respectera les durées minimales d'intervention qui seront fournies par le titulaire.

Déploiement des logiciels sur les postes professionnels de la BU SHS

Le titulaire devra fournir les packages permettant le déploiement silencieux des logiciels d'automatisation sur les postes professionnels.

Le titulaire devra réaliser une première installation sur un poste professionnel, fournir la documentation d'installation associée et effectuer un transfert de compétence vers l'équipe infodoc de la DGDNum qui se chargera du déploiement sur l'ensemble des professionnels.

Réalisation des paramétrages – Fourniture clés en main

Le titulaire réalisera la totalité des paramétrages à partir du dossier de paramétrage validé par l'Université. La configuration initiale du système d'automatisation est totalement à la charge du titulaire qui devra effectuer une livraison « clés en main » pour l'ensemble des équipements et logiciels commandés.

Fourniture des dossiers techniques

Le titulaire devra livrer les documents suivants :

- Un dossier d'architecture technique qui intégrera notamment :
 - Un schéma des flux de données entre le SIGB, les postes professionnels de la BU SHS, les équipements fournis par le titulaire, les plates-formes extérieures et tout autre élément pertinent.
- Un dossier d'installation décrivant pas à pas :
 - La procédure d'installation et de configuration détaillée d'un poste professionnel incluant
 - Les logiciels pour l'utilisation des platines (encodage, prêt-retour, etc.)
 - L'utilisation des terminaux RFID mobiles (si nécessaire)

- La gestion centralisée du portique antivol, des systèmes de comptage, des automates, du système de retour, etc.
 - La procédure de configuration des différents matériels.
- Un dossier d'exploitation décrivant, notamment :
 - Les procédures de surveillance des équipements
 - Les vérifications de premier niveau à exécuter dans différents cas de dysfonctionnement
 - Les procédures d'arrêt/démarrage ainsi que les consignes pour un redémarrage régulier de certains éléments
 - Les procédures éventuelles de sauvegarde et restauration de données.
- Un dossier « sécurité » :
 - Le plan d'assurance sécurité (PAS) de l'entreprise
 - La politique de sécurité du système d'information (PSSI) de l'entreprise
 - Le plan de continuité d'activité (PCA) de l'entreprise
 - Document montrant la conformité du système installé au RGS version 2.0 pour les éléments relevant de sa responsabilité (donc hors éléments strictement dépendants de l'infrastructure informatique et réseau de l'Université).
 - Documents concernant le site d'hébergement de la plate-forme extérieure du titulaire si celui-ci propose une telle plate-forme :
 - Le plan d'assurance sécurité (PAS) de l'hébergement
 - La politique de sécurité du système d'information (PSSI) de l'hébergement
 - Le plan de reprise d'activité (PRA) appliqué en cas de perte du site de production.
- Un dossier « protection des données à caractère personnel » :
 - Politique de sécurité des données à caractère personnel de l'entreprise (complément éventuel au PAS et au PSSI si ces documents ne traitent pas du sujet)
 - Registre des catégories d'activités de traitement
 - Liste des sous-traitants ultérieurs
- Ces documents devront être mis à jour à chaque nouvelle installation de matériels.

6.6. Prestations liées à la protection des données personnelles

Voir le paragraphe « 4 - Protection des données à caractère personnel » et plus particulièrement le paragraphe « 4.6.1 - Prestations de services attendues pour la mise en œuvre ».

6.7. Prestations de formation

6.7.1. Modalités de formation

Toutes les formations liées à la mise en œuvre des équipements d'automatisation seront dispensées par le titulaire en présentiel. La liste des formations attendues en présentiel est détaillée ci-dessous. Les nombres de sessions sont estimatifs.

Les formations proposées par les candidats doivent couvrir l'ensemble des fonctionnalités demandées dans ce CCTP. Les candidats proposant des formations particulières doivent obligatoirement les rattacher à l'une des formations listées ci-dessous.

6.7.2. Liste des formations attendues

6.7.2.1. Présentation de la solution du titulaire

- Personnes concernées :
 - Groupe projet
 - Personnel de la BU SHS
 - Administrateurs fonctionnels de la BU SHS
 - Administrateurs techniques
- Nombre maximum de personnes par session : pas de limite
- Nombre prévisionnel de sessions : 1

- Contenu :
 - Présentation de la solution RFID au groupe projet, au personnel de la BU SHS et aux administrateurs fonctionnels et techniques.
 - Cette présentation devra permettre au personnel d'acquérir et de comprendre les notions et problématiques associées à la mise en œuvre de la RFID ; pour le groupe projet et les administrateurs, cette présentation devra permettre de mieux suivre et gérer le projet de mise en œuvre.

6.7.2.2. Formation à l'équipement des documents avec des étiquettes RFID

- Personnes concernées :
 - Personnel de la BU SHS
 - Administrateurs fonctionnels de la BU SHS
- Nombre maximum de personnes par session : 10
- Nombre prévisionnel de sessions : 2
- Contenu :
 - Cette formation devra permettre au personnel de maîtriser l'équipement des documents avec les logiciels fournis par le titulaire.
 - Elle devra entraîner le personnel à l'utilisation des platines RFID et des logiciels associés dans une optique « encodage et gestion des collections ».
 - La session intégrera une information précise des personnels sur les rayonnements électromagnétiques émis par les différents matériels faisant l'objet de la formation.

6.7.2.3. Formation à l'utilisation des platines (prêt-retour), du portique antivol, des compteurs de passage et des automates

- Personnes concernées :
 - Personnel de la BU SHS
 - Administrateurs fonctionnels de la BU SHS
 - Administrateurs techniques
- Nombre maximum de personnes par session : 10
- Nombre prévisionnel de sessions : 3
- Contenu :
 - Cette formation sera donnée au personnel une fois les matériels installés sur site :
 - Platines RFID : formation complémentaire éventuelle pour les fonctionnalités liées au prêt-retour.
 - Portique antivol, compteurs de passage : fonctionnement, administration non technique courante (utilisation du logiciel de gestion centralisé, statistiques, etc.).
 - Automates de prêt-retour : fonctionnement et administration non technique courante (utilisation du logiciel de gestion centralisé, statistiques, mode dégradé, changement du mode de fonctionnement - prêt, retour, prêt-retour - accès aux différents logs, etc.).
 - La session intégrera une information précise des personnels sur les rayonnements électromagnétiques émis par les différents matériels faisant l'objet de la formation.

6.7.2.4. Formation à l'administration et à l'exploitation techniques et fonctionnelles des platines, du portique antivol, des compteurs de passage, des automates

- Personnes concernées :
 - Administrateurs fonctionnels de la BU SHS
 - Administrateurs techniques
- Nombre maximum de personnes par session : 10
- Nombre prévisionnel de sessions : 1
- Contenu :
 - Cette formation devra permettre l'examen des dossiers d'architecture, d'installation, d'exploitation et d'administration du système d'automatisation concernant les platines, le portique antivol, les compteurs de passage et les automates. Cette formation inclura les composants installés sur les postes professionnels. Elle présentera notamment :
 - L'architecture

- Les procédures d'installation
- Les éléments de paramétrage réservés aux administrateurs fonctionnels et techniques
- Les procédures de surveillance des équipements
- Les vérifications de premier niveau à exécuter dans différents cas de dysfonctionnement
- Les procédures d'arrêt/démarrage
- Les procédures éventuelles de sauvegarde et restauration de données.

6.7.2.5. Formation à l'utilisation du système de retour

- Personnes concernées :
 - Personnel de la BU SHS
 - Administrateurs fonctionnels de la BU SHS
 - Administrateurs techniques
- Nombre maximum de personnes par session : 10
- Nombre prévisionnel de sessions : 3
- Contenu :
 - Utilisation et administration non technique courante du système de retour :
 - Utilisation de la boîte de retour
 - Changement des bacs du robot de tri
 - Utilisation du logiciel de gestion centralisé, statistiques, résolution de problèmes courants, accès aux différents logs
 - Etc.

6.7.2.6. Formation à l'administration et à l'exploitation techniques et fonctionnelles du système de retour

- Personnes concernées :
 - Administrateurs fonctionnels de la BU SHS
 - Administrateurs techniques
- Nombre maximum de personnes par session : 10
- Nombre prévisionnel de sessions : 1
- Contenu :
 - Cette formation devra permettre l'examen des dossiers d'architecture, d'installation, d'exploitation et d'administration du système RFID concernant le système de retour (incluant les composants installés sur les postes professionnels) ; elle présentera notamment :
 - L'architecture
 - Les procédures d'installation
 - Les éléments de paramétrage réservés aux administrateurs fonctionnels et techniques
 - Les procédures de surveillance des équipements
 - Les vérifications de premier niveau à exécuter dans différents cas de dysfonctionnement
 - Les procédures d'arrêt/démarrage

6.7.2.7. Formation à l'utilisation et à l'administration technique et fonctionnelle des terminaux RFID mobiles

- Personnes concernées :
 - Personnel de la BU SHS
 - Administrateurs fonctionnels de la BU SHS
 - Administrateurs techniques
- Nombre maximum de personnes par session : 10
- Nombre prévisionnel de sessions : 1
- Contenu :
 - Cette formation portera sur l'utilisation des terminaux RFID mobiles et des logiciels associés.
 - Elle inclura également l'administration des terminaux ainsi que les procédures d'installation et de configuration des éventuels logiciels associés.

6.7.3. **Déroulement des formations - Supports**

- Les formations auront lieu en présentiel dans la BU SHS ou dans tout autre bâtiment situé sur le Campus Pont de Bois à Villeneuve-d'Ascq.
- Le titulaire devra fournir un support de formation spécifique à chaque session qu'il remettra sous forme dématérialisée.
- Les formations ne seront pas utilisées pour spécifier ou mettre en place certains paramétrages.
- Les formations feront l'objet d'un PV d'approbation de la part de l'Université, PV qui devra être obtenu pour le déclenchement du paiement.

6.8. **Fourniture de la documentation**

- Outre les documents qui viennent d'être énumérés dans la description des prestations de service, le titulaire devra fournir les documentations d'administration, les documentations d'utilisation et les documentations techniques de l'ensemble des matériels et logiciels qu'il aura fournis.
- Ces documentations feront l'objet d'une livraison sous forme de fichiers PDF.
- Toutes les documentations seront rédigées en langue française.
- La qualité, l'exactitude et l'exhaustivité des documentations feront l'objet d'un point soumis à vérification d'aptitude.

Sont attendus au minimum :

- Dossiers techniques listés dans le paragraphe « 6.5 - Prestations d'installation des matériels, de déploiement des logiciels et de réalisation des paramétrages »
- Supports de formation
- Manuels d'utilisation
- Manuels d'administration
- Documentations techniques

6.9. **Assistance au démarrage**

Le titulaire devra apporter une assistance au démarrage lorsque le système d'automatisation commencera à être utilisé par le public à la réouverture de la BU SHS.

Cette assistance au démarrage est un complément à l'assistance générale due par le titulaire dans le cadre de la garantie et de la maintenance.

6.10. **Vérification des prestations**

Par défaut, les opérations de vérification des prestations suivront le mécanisme « Mise en ordre de marche (MOM) / Vérification d'aptitude (VA) / Vérification de service régulier (VSR) » dont le détail est décrit dans le CCAP.

Les candidats doivent prévoir les journées nécessaires à la gestion des opérations de vérification et notamment à l'assistance du groupe projet lors des opérations de recette (VA) :

- Réponses aux questions
- Le cas échéant, assistance à la réalisation de certains tests.

Le titulaire devra fournir les cahiers de recette nécessaires aux opérations de MOM et de VA.

7. Prestations de services attendues pour la garantie et la maintenance

7.1. Présentation générale

Les matériels et logiciels livrés par l'intermédiaire du présent accord-cadre devront faire l'objet d'une garantie de la part du titulaire :

- Cette garantie sera organisée en fonction des différentes opérations de vérification qui seront réalisées au cours de l'accord-cadre.
- Le point de départ de la garantie des matériels et logiciels associés à une opération de vérification sera la notification de la décision positive d'admission (donc après la VSR pour les vérifications de type MOM/VA/VSR).
- Les matériels et logiciels devront être garantis au moins 1 an.

Coût de la garantie :

- Le coût de la garantie, incluant la correction des anomalies du lundi au vendredi de 9h00 à 18h00, doit être compris dans le coût d'acquisition des matériels et logiciels y compris si certains de ces éléments sont proposés avec un coût nul par le titulaire. Cette garantie ne pourra donc faire l'objet d'aucune redevance de la part du titulaire.
- L'extension de la garantie au samedi de 9h00 à 18h00 et au dimanche de 9h00 à 18h00 fera l'objet d'un chiffrage par les candidats par l'intermédiaire des postes prévus à cet effet dans le BPU.

L'accord-cadre inclut également la maintenance des matériels et logiciels qui sera appliquée à l'issue de chaque période de garantie :

- Les clauses correspondant à la maintenance corrective devront s'appliquer du lundi au vendredi de 9h00 à 18h00.
- Par l'intermédiaire des postes prévus à cet effet dans le BPU, les candidats chiffreront en sus l'application de la maintenance corrective au samedi de 9h00 à 18h00 et au dimanche de 9h00 à 18h00.

Les prestations fournies par le titulaire pendant la période de garantie devront être les mêmes que celles fournies pendant la période de maintenance.

7.2. Besoins concernant la garantie et la maintenance

7.2.1. Objet de la garantie et de la maintenance

Le titulaire mettra à la disposition de l'Université un service qui devra :

- résoudre les dysfonctionnements techniques et fonctionnels (traitement correctif) constatés par l'Université
- fournir un traitement préventif pour réduire les risques de dysfonctionnement (incluant une visite annuelle)
- assurer un traitement évolutif et adaptatif permettant à l'Université de bénéficier des dernières versions des logiciels installés
- fournir une assistance téléphonique en français pour répondre aux questions que l'Université pourra se poser sur les matériels et logiciels et pour lesquelles la documentation fournie par le titulaire donne une réponse imprécise, incomplète ou non conforme aux résultats constatés.

La garantie et la maintenance s'appliqueront à l'ensemble des matériels et logiciels fournis par le titulaire par l'intermédiaire du présent accord-cadre, qu'ils soient construits ou édités ou non par le titulaire. Cela inclut donc notamment :

- Les systèmes d'exploitation, les SGBD, les serveurs Web, les logiciels libres, les modules sous licence, etc. installés sur les matériels fournis par le titulaire et les postes professionnels appartenant à la BU SHS
- Les équipements entièrement fournis par des sociétés tierces
- Les matériels tiers utilisés à l'intérieur de certains équipements (par exemple, le poste inclus dans chaque automate et le système de retour, la « box » éventuellement nécessaire pour le portique antivol, le périphérique de type grand smartphone/petite tablette éventuellement fourni avec chaque terminal RFID mobile...)
- Toute plate-forme extérieure appartenant au titulaire et nécessaire au fonctionnement du système d'automatisation fourni.

Le titulaire prendra toutes les dispositions pour maîtriser l'ensemble de l'environnement technique qu'il aura fourni.

Tout problème survenant sur un équipement ou composant dont le titulaire n'est pas le constructeur ou l'éditeur devra néanmoins être pris en compte et résolu par lui, sous sa responsabilité exclusive :

- La résolution pourra être limitée à la mise en place d'une solution de contournement du problème. Cette solution devra être stable, ne pas provoquer de perte fonctionnelle pour les utilisateurs et ne pas dégrader les performances.
- L'Université ne devra pas avoir à contacter une société tierce. Le titulaire prendra à sa charge tous les contacts nécessaires avec ces sociétés.

Le titulaire n'utilisera que des composants logiciels que l'éditeur s'engage à maintenir pendant la durée de l'accord-cadre. Si la durée de l'accord-cadre dépasse la durée pendant laquelle un éditeur s'engage à maintenir un composant logiciel, le titulaire opérera une migration vers des systèmes maintenus.

Les traitements correctifs et la maintenance évolutive et adaptative s'appliqueront également à la documentation.

7.2.2. Accès au service de garantie et de maintenance par l'Université

Le titulaire devra fournir :

- Une hotline téléphonique avec un numéro non surtaxé disponible (jours fériés exclus)
 - du lundi au vendredi de 9h00 à 18h00
 - ainsi que le samedi de 9h00 à 18h00 et le dimanche de 9h00 à 18h00 si l'Université commande l'extension de garantie et de maintenance correspondante.
- Un système de gestion des anomalies accessible par Internet 24 heures sur 24 et 7 jours sur 7 avec gestion nominative des accès.

Les anomalies et dysfonctionnements pourront être signalés, selon le choix de l'Université, par l'un ou l'autre de ces moyens ; dans tous les cas, le suivi de leur traitement devra pouvoir être réalisé par l'intermédiaire du système de gestion des anomalies.

L'assistance téléphonique sera disponible par l'intermédiaire de la hotline.

7.2.3. Accès au système par le titulaire

Le titulaire pourra intervenir sur le système installé par l'intermédiaire du présent accord-cadre :

- À distance, en télémaintenance :
 - Le titulaire pourra accéder en télémaintenance à ses équipements en appliquant une procédure fournie par l'Université.
 - L'accès pourra être permanent par l'intermédiaire d'un système VPN appartenant à l'Université, sans nécessité d'une validation préalable par l'Université. Le titulaire devra néanmoins prévenir la BU si son intervention provoque l'indisponibilité de certains équipements. Les comptes d'accès au VPN sont nominatifs ; le titulaire devra préciser la liste des intervenants possibles et avertir l'Université de tout changement dans cette liste.

- En se déplaçant dans la BU SHS sous réserve que l'intervention soit planifiée et accompagnée par un agent de la BU SHS :
 - Cette procédure ne sera enclenchée que si l'assistance téléphonique ou l'accès par télémaintenance ne permet pas les actions nécessaires.
 - Les interventions sur site seront à la charge exclusive du titulaire, sans possibilité de facturation complémentaire.

Toute intervention, en télémaintenance ou sur place, fera l'objet d'un rapport ou d'une fiche d'intervention et sera transcrite dans le système de gestion des incidents accessible par Internet.

7.2.4. Traitement préventif

Dans le cadre de la garantie et de la maintenance, le titulaire devra réaliser de manière régulière et préventive toutes les opérations nécessaires pour conserver les matériels et logiciels dans un état de performance et de fonctionnement optimal.

Le titulaire effectuera obligatoirement une visite annuelle :

- Pour vérifier le bon fonctionnement des matériels incluant une vérification mécanique du système de retour
- Pour vérifier le bon fonctionnement des logiciels, par exemple, en examinant les logs générés par ces logiciels
- Pour procéder à un dépoussiérage et à un nettoyage des équipements qui le nécessitent
- Pour vérifier les connectiques
- Etc.

Lors de cette visite, il corrigera tout problème constaté.

Les rapports de visites préventives seront répertoriés dans le système de gestion des incidents accessible par Internet.

7.2.5. Traitement correctif

Chaque anomalie constatée dans le fonctionnement des matériels et logiciels devra être corrigée par le titulaire dans le cadre de la garantie et de la maintenance, sous réserve que l'anomalie se soit produite dans des conditions d'usage normal du matériel ou du logiciel et conformes aux recommandations du titulaire.

Chaque anomalie fera l'objet d'un rapport ou d'une fiche d'intervention qui sera transcrite dans le système de gestion accessible par Internet.

Les anomalies seront classées selon deux catégories, laissées à l'appréciation finale de l'Université en cas de désaccord :

- Anomalies mineures (non bloquantes) :
Une anomalie mineure n'interdit l'accès qu'à des fonctions peu importantes des logiciels ou matériels concernés et ne perturbe pas de manière importante les performances ; le fonctionnement habituel de la BU SHS n'est pas ou est peu affecté par une anomalie mineure.
- Anomalies majeures (bloquantes) :
Une anomalie majeure interdit l'accès à une ou plusieurs fonctions importantes des matériels ou logiciels concernés et/ou perturbe fortement les performances ; une anomalie majeure affecte de manière importante le fonctionnement habituel de la BU SHS.

L'accumulation d'anomalies mineures pourra être considérée comme une anomalie majeure.

Seront notamment considérés comme « anomalies majeures », les cas suivants :

- Dysfonctionnement du portique antivol (plus d'alarme pour tout ou partie des unités de passage)
- Dysfonctionnement de la moitié ou plus des automates libre-service de la BU SHS (prêts et/ou retours en libre-service impossibles)
- Dysfonctionnement du système de retour (retours impossibles)

- Dysfonctionnement simultané d'au moins deux postes professionnels équipés d'une platine dans la BU SHS si le dysfonctionnement est en lien avec la platine ou les logiciels fournis par le titulaire.

Le délai de correction d'une anomalie correspond à la durée écoulée entre la déclaration de l'anomalie par l'Université et la constatation par l'Université de la résolution ou du contournement du problème constaté. Les délais maximaux de correction ou de mise en place d'une solution de contournement pour une anomalie dépendent de sa catégorie :

- Anomalie majeure ne nécessitant pas la mise en place d'une solution de contournement :
 - Délai maximal de correction par télémaintenance : 13 heures ouvrées.
 - Délai maximal de correction si une intervention sur site est nécessaire : 27 heures ouvrées ; ce délai pourra être étendu si l'intervention est décalée en raison de l'indisponibilité du personnel de la BU SHS pour l'accompagnement du titulaire sur place.
- Anomalie majeure nécessitant la mise en place d'une solution de contournement :
 - Délai maximal pour la mise en place de la solution de contournement par télémaintenance : 13 heures ouvrées.
 - Délai maximal pour la mise en place de la solution de contournement si une intervention sur site est nécessaire : 27 heures ouvrées ; ce délai pourra être étendu si l'intervention est décalée en raison de l'indisponibilité du personnel de la BU SHS pour l'accompagnement du titulaire sur place.
 - Délai maximal de correction définitive et de suppression de la solution de contournement : 14 jours calendaires.
- Anomalie mineure :
 - Le délai de correction pour une anomalie mineure sera convenu au moment de la déclaration de l'incident et ne pourra être supérieur à 90 jours calendaires.

Le titulaire aura une obligation de résultat et pas seulement une obligation de moyens ; l'Université vérifiera les délais de correction (garantie de temps de rétablissement) et non les délais d'intervention (garantie de temps d'intervention).

En cas de non-respect des délais de correction, le titulaire encourra les pénalités prévues dans le CCAP dans le paragraphe « Pénalités d'indisponibilité pour les prestations de garantie et de maintenance ».

Pour les anomalies mineures uniquement, le délai de correction d'une anomalie ne prendra pas en compte les périodes au cours desquelles le titulaire attendra des demandes de précisions de la part de l'Université. Si le problème est aléatoire (pas de reproduction systématique), la fourniture de copies d'écran (ou de photos) montrant le problème et sa répétition sur au moins deux journées différentes pourra être considérée par l'Université comme une information suffisante pour déclencher la mesure du délai de correction.

Les délais ouvrés s'entendent par rapport au type de maintenance qui sera retenue par l'Université :

- du lundi au vendredi de 9h00 à 18h00
- ou bien du lundi au samedi de 9h00 à 18h00 si l'Université passe commande de l'extension au samedi
- ou bien du lundi au dimanche de 9h00 à 18h00 si l'Université passe commande de l'extension au samedi et au dimanche.

Dans les trois cas, les jours fériés sont exclus.

Les candidats s'engageront sur des délais précis de correction des anomalies.

7.2.6. Pièces détachées et livraisons

Pendant la garantie

Les pièces détachées, les matériels et la main d'œuvre nécessaires à la correction des anomalies constatées devront être fournis gratuitement pendant toute la durée de la garantie.

Les frais de port nécessaires à la livraison de ces pièces et matériels dans la BU SHS et au retour des pièces et matériels défectueux chez le titulaire, seront à la charge exclusive du titulaire.

Après la garantie (maintenance payante)

Les candidats préciseront les conditions de fournitures des pièces détachées et des matériels nécessaires à la correction des anomalies constatées et les frais de port associés pour la période qui suivra la garantie :

- En cas de gratuité :
 - Les candidats indiqueront une limite de durée éventuelle.
- En cas de paiement :
 - Les candidats intégreront obligatoirement dans leur réponse un tableau listant les pièces détachées et précisant pour chacune, leur prix HT et TTC ainsi que les frais de port HT et TTC associés.

Dans tous les cas, les coûts liés à la main d'œuvre devront être inclus dans les coûts de maintenance standards (pas de facturation complémentaire).

Lot de pièces détachées et de matériels sur place

Le titulaire pourra constituer un lot de pièces détachées et de matériels stockés dans la BU SHS pour assurer les délais de correction exigés pour le traitement correctif. L'Université offrira l'espace de stockage nécessaire. La constitution du lot de pièces détachées est totalement à la charge du titulaire. Aucune facturation spécifique pour la constitution de ce lot ne sera acceptée et le titulaire ne pourra pas faire valoir l'absence d'un lot sur place pour ne pas respecter les délais de correction des anomalies.

7.2.7. Traitement évolutif et adaptatif

Dans le cadre de la garantie et de la maintenance, le titulaire devra fournir, sans frais supplémentaires, toutes les nouvelles versions mineures et majeures des différents logiciels livrés par l'intermédiaire du présent accord-cadre. Ces nouvelles versions seront accompagnées de l'ensemble des documentations standards mises à jour.

Par « évolutif », on entend les mesures de maintenance visant à faire évoluer une ou plusieurs applications, afin d'intégrer de nouvelles fonctions, d'en améliorer le fonctionnement et l'ergonomie ou de prendre en compte de nouvelles dispositions législatives ou réglementaires.

Par « adaptatif », on entend les mesures d'entretien et de maintenance permettant d'absorber des modifications de l'environnement technique d'exécution, comme les mises à jour ou les changements de systèmes d'exploitation, de bases de données, d'interfaces d'échange ou plus généralement des composants techniques et bibliothèques logicielles.

Dans le cadre de la garantie et de la maintenance évolutive et adaptative, le titulaire aura notamment l'obligation de fournir et d'installer de nouvelles versions mineures ou majeures permettant de résoudre les problèmes constatés ou potentiels dans les cas suivants :

- Correction d'une vulnérabilité connue d'un composant de la solution proposée. La correction devra être installée dans un délai de trois mois après l'émission de la demande par l'Université. Ce point fera l'objet d'une attention particulière de la part de l'Université pour les logiciels libres qui pourraient être inclus dans la solution du titulaire.
- Prise en compte d'une évolution de la réglementation en vigueur :
 - Les adaptations ou évolutions des logiciels dues à des évolutions réglementaires devront être disponibles au plus tard trois mois avant la date de mise en vigueur ou dans le mois qui suit la transmission des instructions par les instances officielles.
 - Le titulaire devra lui-même mettre en œuvre les moyens nécessaires à la connaissance de ces modifications auprès des instances concernées. En aucun cas, l'Université ne sera sollicitée pour en informer le titulaire ; elle ne pourra être tenue pour responsable de la non-information du titulaire.
- Correction nécessaire au support d'une nouvelle version d'un navigateur Internet utilisé de manière préférentielle sur les postes professionnels. La correction devra être installée dans un délai de six mois après l'émission de la demande par l'Université.

En cas de non-respect des délais précisés ci-dessus, le titulaire encourra les pénalités prévues dans le CCAP dans le paragraphe « Pénalités d'indisponibilité pour les prestations de garantie et de maintenance ».

Les prestations d'installation des nouvelles versions mineures (patchs correctifs apportant peu d'évolutions fonctionnelles) devront être réalisées dans leur intégralité par le titulaire, dans le cadre de la garantie et de la maintenance et sans surcoût.

Le titulaire aura également à sa charge, sans frais supplémentaires, la mise à jour régulière des systèmes d'exploitation des postes et boîtiers informatiques fournis par ses soins (automates, système de retour, « box » pour le portique antiviol). La fréquence minimum de mise à jour devra être annuelle. Les patchs de sécurité devront être appliqués au maximum trois mois après leur sortie (sauf si l'Université gère leur application). Le titulaire devra également gérer les mises à jour de l'antivirus (sauf si l'Université le fournit).

Les prestations d'installation des nouvelles versions majeures (évolutions fonctionnelles importantes) pourront être facturées en sus de la maintenance par le titulaire. Le coût d'installation (hors formations) doit être chiffré par les candidats par l'intermédiaire du poste prévu à cet effet dans le BPU.

Les prestations de formations liées aux nouvelles versions (mineures et majeures) pourront être facturées en sus de la maintenance par le titulaire (utilisation des prix de journées et de demi-journées de formation du BPU).

Les installations des versions mineures et majeures devront préserver totalement la configuration et le paramétrage propres à l'Université.

7.2.8. Prestations liées à la protection des données personnelles

Voir le paragraphe « 4 - Protection des données à caractère personnel » et plus particulièrement le paragraphe « 4.6.2 - Prestations de services attendues pour la garantie et la maintenance ».