

1 Contraintes techniques

L'ensemble des composants de l'architecture technique nécessaire au bon fonctionnement du logiciel de gestion documentaire pour le Campus Paramédical du CHU Dijon Bourgogne devra suivre les contraintes techniques détaillées ci-après.

1.1 Serveurs

1.1.1 Serveurs d'applications et serveurs web

Les serveurs seront exclusivement des machines virtuelles hébergées sur l'infrastructure de virtualisation VMware du CHU de Dijon.

Toutefois, si pour le projet un serveur doit comporter des composants spécifiques (cartes d'acquisition, cartes audio, ...) ou s'il doit être connecté à un appareil biomédical autrement qu'en TCP/IP, le candidat précisera alors le type, la marque et les caractéristiques techniques des machines proposées. Il fournira également la méthodologie de sauvegarde adaptée.

Les systèmes d'exploitation des serveurs sont exclusivement basés sur Windows Server ou Red Hat Entreprise Linux en 64 bits et dans des versions dont le support est encore disponible pour les trois années suivant leur installation.

Si la solution implique d'importantes ressources d'archivage (plusieurs Téraoctets) pour des documents ou des images, un serveur spécifique ou un partage (CIFS ou NFS) adossé à l'infrastructure de stockage capacitif sera proposé. Cette machine exposera des partages CIFS ou NFS aux autres serveurs de la solution.

1.1.2 Base de données

Les Systèmes de Gestion de Bases de Données utilisés au CHU de Dijon sont par ordre de préférence :

- Oracle
- SQL Server
- MySQL

La base de données choisie devra être installée dans une version dont le support est encore disponible pour trois années.

Bases Oracle

Les bases Oracle sont installées exclusivement sur des serveurs virtuels dédiés sous Red Hat Entreprise Linux selon une méthodologie définie par le CHU de Dijon. La sauvegarde est assurée par Veeam Backup ou RMAN. Les bases sont obligatoirement en ARCHIVELOG.

Les objets de bases de données seront regroupés dans un ou plusieurs schémas dédiés à l'application. Les utilisateurs Oracle n'auront pas les droits DBA mais disposeront des autorisations adaptées (GRANT). Les DB Link sont à éviter.

Bases SQL Server

Les bases SQL Server sont installées exclusivement sur des serveurs virtuels sous Windows. Le serveur peut soit être dédié, soit mutualisé avec d'autres composants applicatifs. Les fichiers de données, journaux et backup seront séparés sur des disques distincts.

Les objets de bases de données seront regroupés dans un ou plusieurs schémas dédiés à l'application. Le compte SA ne sera pas utilisé directement par l'application.

Quelle que soit la base de données mise en œuvre, le candidat proposera son plan de maintenance et de sauvegarde.

1.1.3 Installation des composants applicatifs

Pour Microsoft

Les installations des différents composants logiciels devront suivre la démarche suivante :

- Intégration des serveurs dans le domaine Active Directory du CHU de Dijon,
- Utilisation d'un compte de domaine administrateur du serveur (pas de comptes locaux),
- Installation des composants sur le disque D (rien sur C),
- Les applications doivent impérativement être installées sous forme de services exécutés par des comptes de service.
- Aucun programme ne doit tourner en session ouverte,
- Les partages de fichiers ne seront jamais « en contrôle total à tout le monde » mais limités à des groupes d'utilisateurs définis depuis l'AD

Pour Linux

Les installations des différents composants logiciels devront suivre la démarche suivante :

- Les applications doivent fonctionner dans un environnement « utilisateur sans droit » (exclusion de root),
- Les processus doivent démarrer sous forme de services correspondant au standard du système,
- Aucun répertoire ou fichier ne doit porter des droits de type 777,
- Pour les serveurs exposés en DMZ, SE Linux sera activé et les mises à jour de sécurité seront automatiques et systématiques.

Le candidat précisera les prérequis à son installation et leur version (JDK, Framework .NET, ...).

1.1.4 Sauvegarde

Les sauvegardes des serveurs et des bases de données sont assurées par l'infrastructure de sauvegarde du CHU conformément au PRA en vigueur. Le candidat précisera la volumétrie initiale à prendre compte ainsi qu'une projection de croissance par année.

De plus, le candidat fournira, si nécessaire, les scripts ou les commandes nécessaires pour garantir la cohérence applicative d'une sauvegarde.

Le candidat doit indiquer s'il existe des spécificités dans le processus de restauration.

1.1.5 Sécurité et réseau

Les serveurs seront intégrés au réseau conformément au plan d'adressage en vigueur au CHU, dans des VLAN routés dédiés aux serveurs. Les serveurs auront une IP fixe et une entrée DNS statique.

Tous les serveurs ayant des services ouverts vers l'extérieur seront isolés dans une DMZ, laquelle est coupée du LAN par des firewalls. Aussi, le candidat listera les ports à ouvrir tant vers l'extérieur que vers l'intérieur. En aucun cas un serveur du LAN n'ouvrira de service directement sur Internet. Tous les accès Internet en tant que client se feront via un Proxy.

Pour les applications Web ouvertes sur Internet, seul le protocole HTTPS est autorisé. Le candidat précisera le type de certificat à utiliser et les modalités d'installation.

Tant pour Microsoft que pour Linux, le candidat précisera s'il a des réserves quant à l'application régulière des patches de sécurité.

Les systèmes ayant besoin de ressources réseau particulières (Broadcast, Multicast, NAT, ...) devront faire l'objet d'une expression de besoins détaillée.

Accès distant

Le CHU permet aux prestataires de prendre la main à distance sur des serveurs ou des PC via un accès au Bastion CHU. Aucune autre solution de prise de main à distance n'est admise au CHU. Selon le nombre d'intervenants possibles sur les machines, le prestataire disposera soit de plusieurs comptes individuels, soit d'un compte générique si plus de 50 utilisateurs nommés sont susceptibles d'intervenir.

1.2 Postes de travail et périphériques

1.2.1 Postes de travail

Les postes clients sont fournis avec l'antivirus Sophos (incluant le module d'analyse comportementale). L'antivirus est obligatoire.

Les postes clients du CHU sont installés avec soit :

- Windows 11,
- VMware Horizon.

L'installation des logiciels du candidat devront prendre en compte les restrictions suivantes :

- Les utilisateurs des PC sont des utilisateurs standards Windows (et non pas administrateur du poste),
- L'UAC (User Account Control) est activée,
- Les paramètres de restriction et configuration sont appliqués via GPO, pour Windows, Edge et pour Office. Ces paramètres sont disponibles sur demande,
- Les applications sont à installer dans les répertoires programmes files ou programme files x86 uniquement (pas à la racine du disque),
- Les utilisateurs ne doivent pas pouvoir écrire dans les répertoires d'installation de programmes,
- Les données locales des applications sont soit stockées dans les profils des utilisateurs (soit %APPDATA% soit %LOCALAPPDATA%), soit stockées dans %ProgramData%
- Pour les données temporaires, il convient d'utiliser %temp%

Si les logiciels utilisent Java, le candidat précisera la version nécessaire.

Dans le cas d'un logiciel sous forme de client Web, le candidat doit fournir tous les éléments de configuration du navigateur internet (ActiveX, paramètres de sécurité, ...). L'application devra alors fonctionner sous Edge, navigateur officiel de l'Institution CHU de Dijon.

Dans le cas d'un client lourd à installer sur les postes informatiques, le candidat doit fournir une solution d'installation en mode silencieux et à défaut l'ensemble des éléments permettant une installation manuelle du logiciel afin que le CHU puisse packager et déployer le logiciel via les outils de gestion de Parc sur CHU.

1.2.2 Impressions

Le candidat précisera si des files d'impressions sont à créer localement sur ses serveurs. A défaut, les impressions s'appuieront sur le serveur d'impression du CHU.

1.2.3 Smartphone, tablettes

Le candidat détaillera les caractéristiques techniques des équipements de type Smartphones ou tablettes compatibles avec sa solution. Il fournira un guide d'installation et décrira les différents modes d'intégration avec sa solution.

Dans le cas de terminaux mobiles, ceux-ci doivent être compatibles avec les outils de gestion de flottes de terminaux (VMWare Workspace One, MobileIron ou Microsoft Intune).

1.3 Plateforme envoi de sms

Le CHU dispose d'une plateforme d'envoi de SMS via la solution Orange Business Service. Cette solution constitue le seul vecteur d'envoi de SMS admis par le CHU. Le candidat devra s'interfacer via l'utilisation de Web services dont le WSDL est disponible via le lien : « <https://www.contact-everyone.fr/orange-business.com/ContactEveryone/services/MultiDiffusionWS?wsdl> »

Orange Business Services s'est assuré de l'interopérabilité de son Web Service avec les moteurs de Web Services pour les solutions Java Axis (Environnement J2EE) et .NET (Microsoft). Il est recommandé d'utiliser la librairie Axis au-dessus des serveurs d'application J2EE tels que WebSphere, WebLogic, Jonas ou Tomcat. Il est également possible, dans un autre environnement supportant l'approche Web Service, de générer les classes/proxys permettant l'appel du Web Service à partir du contrat d'interface WSDL fourni.

1.4 Interfaces avec d'autres applications

Les interfaces entre les applications sont pilotées par l'EAI du CHU de Dijon (Enovacom). Ce dernier fonctionne dans une logique de « pull and forward » ce qui induit que les connecteurs d'interfaces sortantes doivent produire les messages localement sur le serveur, l'EAI assurant le routage.

Pour les flux sortants, l'application soumettra les messages soit :

- Via des fichiers déposés dans un répertoire du serveur. L'application procédera à un renommage du fichier une fois celui-ci écrit pour éviter les collisions entre les processus d'écriture et de prise en charge par l'EAI (cf descriptif ci-dessous)
- Via une table de SAS qui sera lue par l'EAI

Pour les flux entrants, l'application recevra les messages, par ordre de préférence :

- Via un dépôt de fichier dans un répertoire
- Via une table de SAS qui sera alimentée par l'EAI,
- Via un processus d'écoute de socket (MLLP),

Cependant le mode d'échange de données à privilégier est le « mode fichier » selon les consignes et protocoles suivants :

- Un fichier porte un numéro unique, purement incrémentale.
- A la fin de l'écriture du fichier par le processus de sortie un fichier portant le même nom mais avec l'extension .ok est généré pour signifier qu'il n'existe plus de blocage sur le fichier de donnée qui peut être consommé librement.
- Pour un processus entrant le même fonctionnement est réalisé : l'EAI dépose un fichier avec un numéro unique purement incrémentale, lorsque le fichier .ok est écrit le fichier peut être lu. Le destinataire est chargé de la suppression du fichier de donnée et .ok à la fin de sa consommation
- Un fichier .log doit être alimenté pour superviser l'activité de consommation des messages (quels fichiers sont lues, intégrés, consommés) et doit remonter clairement les données provoquant des erreurs d'intégration.

Concernant les formats de données, il sera préféré l'utilisation de normes comme HL7. Si la nature des échanges ne fait l'objet d'aucune norme, les formats seront transformés par l'EAI. Le candidat fournira alors une spécification de la structure de ses messages.

1.5 Construction des rapports

Deux besoins pourraient apparaître :

1.5.1 Rapports BO :

Les données sont proposées aux utilisateurs dans Business Object (SAP), dans la version BI 4.3 SP2. Les univers BO seront donc livrés sous la forme de fichiers lcbiar.

L'ensemble des données fonctionnelles de l'outil doivent être disponible aux utilisateurs, dans un ou plusieurs univers.

Le cas échéant, les informations nécessaires seront :

- Définition et règles de calcul des indicateurs s'il y en a
- Restriction d'usage de l'univers : quelles données sont compatibles...

1.5.2 Extraction de données dans l'entrepôt de données de santé

Afin de pouvoir extraire certaines informations pertinentes dans un entrepôt de données de santé (traitement de nuit via ETL), nous avons besoin de documentation du modèle de données

Le candidat fournira :

- Définition et schéma des entités principales (Tables) et des liens entre les entités principales
- Le catalogue de données : le dictionnaire avec la définition des données, exemples de valeurs

2 CONFIDENTIALITE – MESURES DE SECURITE

Le candidat est tenu à la confidentialité des informations, auxquelles il aurait accès dans le cadre de l'exécution du présent marché. Il s'engage à faire respecter ces dispositions par son personnel et par ses éventuels sous-traitants. Il assure également la confidentialité des données patients auxquelles il aurait accès lors de l'exécution du présent marché.

2.1 Obligation de confidentialité

Le candidat et le pouvoir adjudicateur qui, à l'occasion de l'exécution du marché, ont connaissance d'informations ou reçoivent communication de documents ou d'éléments de toute nature, signalés comme présentant un caractère confidentiel et relatifs, notamment, aux moyens à mettre en œuvre pour son exécution, au fonctionnement des services du candidat ou du pouvoir adjudicateur, sont tenus de prendre toutes mesures nécessaires, afin d'éviter que ces informations, documents ou éléments ne soient divulgués à un tiers qui n'a pas à les connaître.

Une partie ne peut demander la confidentialité d'informations, de documents ou d'éléments qu'elle a elle-même rendus publics.

Ne sont pas couverts par cette obligation de confidentialité les informations, documents ou éléments déjà accessibles au public, au moment où ils sont portés à la connaissance des parties au marché.

2.2 Protection des données à caractère personnel

Chaque partie au marché est tenue au respect des règles relatives à la protection des données nominatives, auxquelles elle a accès pour les besoins de l'exécution du marché.

Notamment, toute intervention effectuée par les agents préposés du candidat ou agissant pour son compte et mettant ces derniers en situation de pouvoir accéder à des données médicales nominatives, doit se faire dans le respect le plus strict de leur confidentialité.

Les parties se conformeront à l'annexe relative à la protection des données à caractère personnel, le candidat s'engage à compléter cette annexe.

2.3 Accès distant au SI

Chaque intervention sur place ou à distance par télémaintenance ne peut être réalisée qu'à la demande ou avec l'accord préalable de la DSN. L'intervention fait en outre l'objet d'un compte rendu détaillé comportant l'identification de l'intervenant et sa signature ; ce compte rendu est adressé à la DSN.

Et conformément aux recommandations du CERT SANTE, le candidat devra respecter les exigences suivantes :

- a. Utilisation de l'accès VPN proposé par l'établissement(s) pour réaliser ses actions.
- b. Ne pas utiliser des outils de prise en main à distance accessibles par une connexion tierce (ex: TeamViewer, AnyDesk, ...).
- c. Utilisation du bastion d'administration proposé par l'établissement(s) qui permet une traçabilité forte des actions réalisées (enregistrement vidéo des sessions).
- d. Le candidat s'engage à fournir la liste des adresses IP publiques qui pourront se connecter à l'accès VPN, afin que l'établissement(s) puisse mettre en place un filtrage sur ces adresses IP.
- e. Utilisation d'un compte nominatif pour chaque intervenant du candidat qui ne sera créé sur les systèmes d'information de l'établissement(s) qu'après signature individuelle de la charte dédiée aux administrateurs.

- f. Le candidat informe l'établissement(s) de tout départ de collaborateur (congés longue durée) ou mouvement en interne pour révocation des accès. Cette déclaration doit se faire dès que la société en a connaissance.
- g. Utilisation de l'authentification deux facteurs via l'envoi d'un OTP (One Time Password) sur une boîte mail professionnelle qui est mise en œuvre par l'établissement(s). Ce mode d'authentification deux facteurs peut être amené à évoluer.
- h. Les intervenants du candidat utilisent des postes dédiés à l'administration lors de l'intervention. Ces postes ne doivent pas réaliser des tâches bureautiques (office, courriel, ...) ou toutes autres tâches à risque.
- i. Les intervenants du candidat utilisent exclusivement un poste d'administration professionnel avec un antivirus à jour – l'usage d'un poste personnel est interdite même pour établir une connexion VPN sur le poste d'administration.
- j. Le candidat s'engage à ne pas mettre en place d'outil de prise en main à distance (ou toutes autre solution générant un "tunnel" de contrôle) pour contourner le VPN de la structure.
- k. Si le candidat a besoin d'avoir une supervision sur les serveurs concernés par la prestation de télémaintenance, le candidat doit fournir la matrice de flux vers internet (hostname/ip publique, port, protocole). Les métriques seront poussées de l'établissement(s) vers le candidat sans jamais que la solution utilisée ne puisse permettre une prise de contrôle/exécution par ce canal. La configuration de l'agent de supervision doit être statique et le serveur de supervision ne doit pas être en capacité de modifier la configuration de l'agent, ou de transmettre un argument pris en compte dans l'exécution des commandes de l'agent.
- l. En cas de cyberattaque côté établissement(s), le lien internet pourrait être amené à être couper les premiers jours / semaines. Dans ce cadre la télémaintenance ne pouvant être assurée, une intervention sur site doit être prévue par le candidat avec un engagement de service qui doit être proposé.

2.4 Gestion des secrets

La notion de secret d'authentification englobe les mots de passe, clef privée SSH, code PIN ... plus globalement tout élément secret permettant l'authentification. Sauf mention contraire et par souci de simplicité, la notion de « mot de passe » fera référence à un secret d'authentification dans le reste du document.

Conformément aux recommandations du CERT SANTE, le candidat devra respecter les exigences suivantes :

- a. Les mots de passe de l'établissement(s) sont conservés dans une solution sécurisée (exemple : KeePass).
- b. Les mots de passe de l'établissement(s) ne sont jamais enregistrés dans les applications utilisées pour l'administration du SI (ex: navigateur, consoles d'administration comme par exemple PuTTY, ...).
- c. Les mots de passe de l'établissement(s) sont changés tous les ans afin de limiter le risque qu'un mot de passe puisse être réutilisé indéfiniment par un ancien employé.
- d. Les mots de passe de l'établissement(s) sont générés avec un générateur de mot de passe (exemple : KeePass) sur un alphabet au minimum alphanumérique et avec pour longueur minimum 14 caractères.
- e. Les mots de passe de l'établissement(s) sont uniques : ils ne peuvent pas être réutilisés pour d'autres clients.
- f. Les mots de passe de l'établissement(s) sont différents pour chaque environnement (production, qualification...).

2.5 Sous-traitance

Le candidat doit informer ses sous-traitants des obligations de confidentialité et des mesures de sécurité qui s'imposent à lui pour l'exécution du marché. Il doit s'assurer du respect de ces obligations par ses sous-traitants.

2.6 Contrôles et sanctions

L'établissement(s) a la possibilité, à ses frais, d'auditer ou de faire auditer le respect des exigences précédentes mis en place par le candidat une fois par an, afin de vérifier la conformité du candidat vis-à-vis des exigences. Le candidat s'engage dans un délai raisonnable à mettre à la disposition de l'établissement(s) toutes les informations nécessaires pour démontrer le respect de ses obligations ou des obligations de ses sous-traitants.

Le non-respect d'au moins une partie de ces règles du candidat ou d'un de ses sous-traitants expose le candidat à une ou plusieurs des sanctions suivantes à l'appréciation de l'établissement(s) selon la gravité du manquement et le contexte :

1. Révocation immédiate des accès informatique du personnel du candidat ou de ses sous-traitants.
2. Exclusion immédiate des locaux de l'établissement(s) pour le personnel du candidat ou de ses sous-traitants.