DEPARTEMENT DE L'ESSONNE

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

Acquisition, mise en œuvre, maintenance, assistance et évolution d'un progiciel de gestion des courriers pour le Département de l'Essonne

SOMMAIRE

GLOSSAIRE

AD : Active Directory (Annuaire Microsoft)

CPSI : Chef de Projet Informatique Système d'Information

CD91 : Conseil Départemental de l'Essonne

DBA : Administrateur Base de Données

DGA : Direction Générale Adjointe

DGME : Direction Générale de la Modernisation de l'Etat

DGS : Direction Générale des Services

DRM : Direction des Ressources Mutualisées

DSI : Direction des Systèmes d'Information

ISIM : Ingénieur Système d'Information Métier

MDS : Maison Départementale des Solidarités

NOTRe : Nouvelle Organisation Territoriale de la République

PMI : Protection Maternelle et Infantile

SI : Système d'information

RSSI : Responsable Sécurité Système d'Information

Acronymes techniques standards

EIS : Executive Information System

EIGRP : Enhanced Interior Gateway Routing Protocol

ETL : Extract Transform Load

FQDN: Fully Qualified Domain Name

GED : Gestion Electronique de Documents

HSRP : Hot Standby Router Protocol

HTTP : Hypertext Transfer Protocol

HTTPS : Hypertext Transfer Protocol Secured

LAD : Lecture Automatique de Documents

LAN : Local Area Network

LDAP : Lightweight Directory Access Protocol

LDIF : Ldap Data Interchange Format

MAN : Metropolitan Area Network

NTLM : NT Lan Manager

OCR : Optical Character Recognition

RAD : Reconnaissance Automatique de Documents

1. ENVIRONNEMENT ET OBJECTIFS DU MARCHE

1.1. L'environnement du projet

1.1.1. Le Conseil départemental de l'Essonne

Le Conseil départemental de l'Essonne, collectivité territoriale et service public de proximité, est, selon la loi, chargé de « régler par ses délibérations les affaires du département ».

Ses compétences ont été définies par les lois de décentralisation adoptées en 1982 et 1983, puis élargies notamment par la loi du 13 août 2004 relative aux libertés et responsabilités locales ainsi que récemment par la loi NOTRe. Elles couvrent entre autres l'action sociale, l'éducation et l'aménagement du territoire. La politique du Conseil départemental est définie au sein de l'assemblée départementale, composée de 42 conseillers départementaux, et qui se réunit au moins une fois par trimestre. L'instance est dirigée par un président élu, chargé de fixer l'ordre du jour, de diriger les débats et de faire adopter les délibérations.

Pour mettre en œuvre la politique définie par cette assemblée, le Président s'appuie sur :

- un Cabinet, qui aide le Président à gérer au mieux les affaires du département, en apportant une expertise sur des questions précises
- une Direction Générale des Services (DGS) qui, en relation directe avec le Président, assume des fonctions :
    - de coordination et d'animation des équipes de direction,
    - de pilotage stratégique de la mise en œuvre et de l'évaluation des politiques décidées par les élus.

  Sous son autorité, les services départementaux sont organisés autour de grands secteurs d'intervention, structurés en Directions Générales Adjointes (DGA) :
    - DGA Territoires et mobilités,
    - DGA aux Solidarités,
    - DGA Education, Citoyenneté, Culture et Sports,
    - DGA Equipements et Environnement,
    - DGA Accompagnement et Ressources

Chaque DGA s'appuie sur un Secrétariat Général Ressources lequel a pour principal mission de coordonner les actions de ses directions opérationnelles avec la DGAAR, les directions ressources.

Enfin des directions à missions transversales sont directement rattachées au Directeur général des services :

- le secrétariat général,
- l'inspection générale.

Le Conseil départemental de l'Essonne est composé de plus de quatre mille agents répartis pour moitié environ sur les cinq principaux sites administratifs à Evry et pour l'autre moitié dans plusieurs dizaines de sites distants.

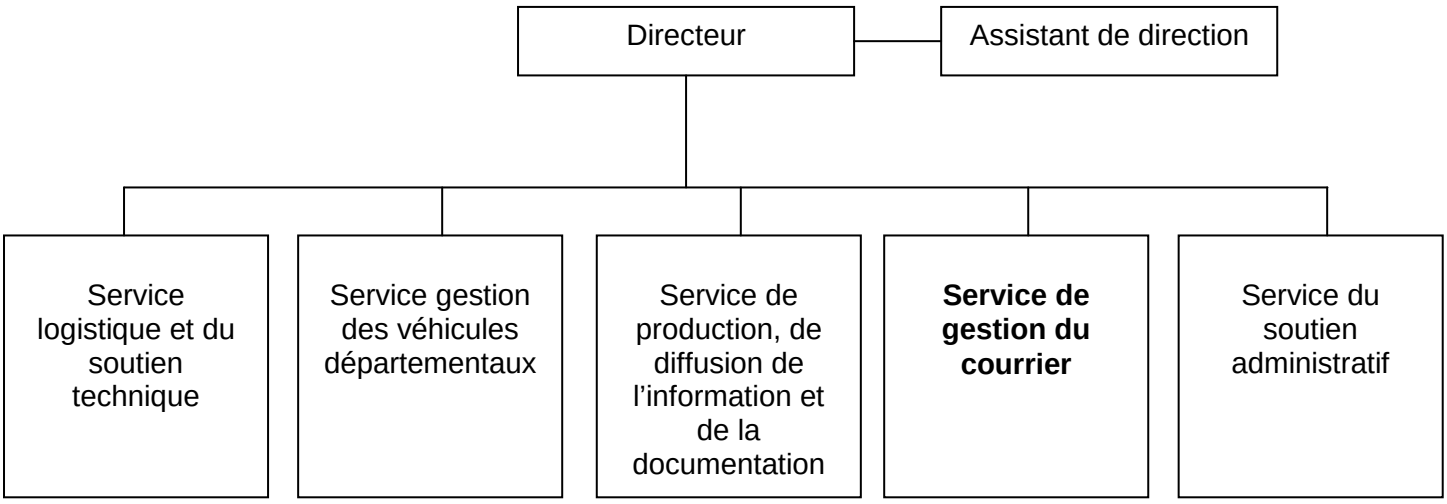
1.1.2. La Direction des Ressources Mutualisées (DRM)

1.1.2.1. Les missions de la DRM

La Direction des Ressources Mutualisées est la maîtrise d'ouvrage de la transformation digitale du processus métier de la gestion du courrier. Elle dépend de la DGA Accompagnement et Ressources. Elle est direction d'accompagnement, de régulation des ressources techniques et administratives, de logistique, d'information et de documentation des directions métiers.

1.1.2.2. Les fonctions des services de la DRM

La DRM s'appuie sur 5 services. La Direction compte 92 agents, dont 8 au **service de gestion du courrier**. Ce service, dédié au traitement et à l'acheminement du courrier, optimise la gestion du suivi du courrier interne, extérieur et électronique avec un suivi de ces derniers et un contrôle des délais de réponse.



Organisation de la DRM

1.1.3. La Direction des Systèmes d'Information (DSI)

1.1.3.1. Les missions de la DSI

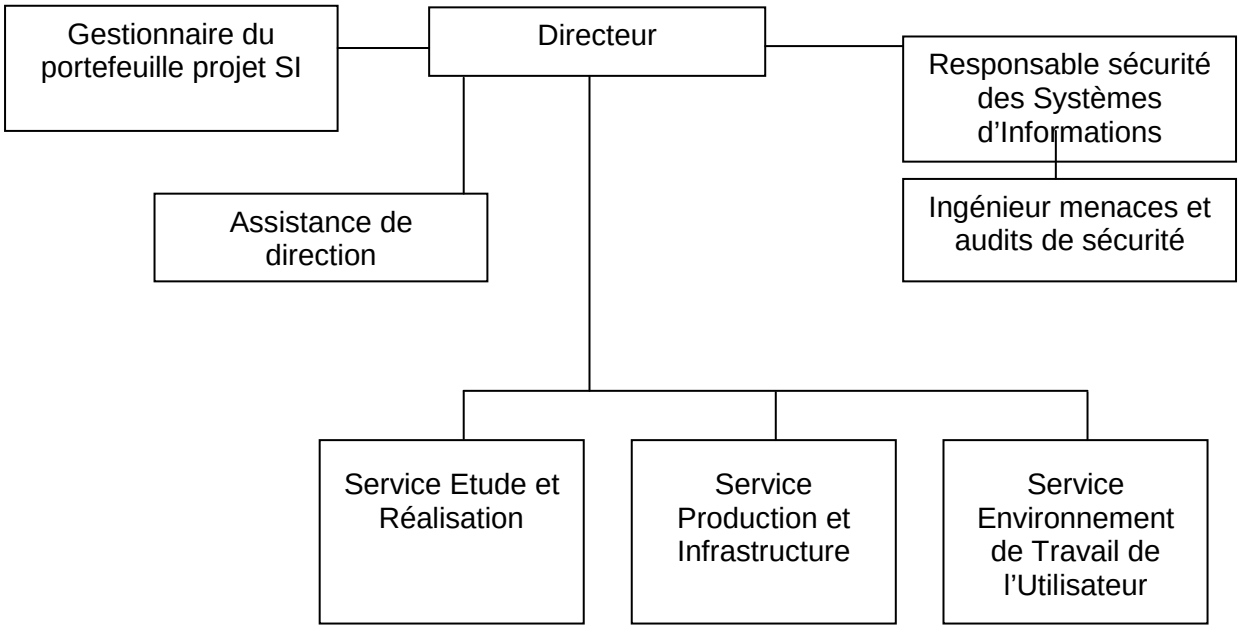
La Direction des Systèmes d'Information (DSI) est la maîtrise d'œuvre de la dématérialisation du courrier. Elle joue également le rôle d'assistance à maîtrise d'ouvrage comme dans la quasi-totalité des projets d'informatisation des directions. Elle dépend de la DGA Accompagnement et Ressources.

La DSI est donc maître d'œuvre et assistance à maîtrise d'ouvrage sur :

- La gestion du référentiel SIG et progiciels,
- La téléphonie,
- La transmission de données,
- L'intégration de solutions,
- Les développements spécifiques et l'open source,
- L'infrastructure informatique,
- L'interopérabilité,
- La sécurité informatique,
- Le déploiement des logiciels et des postes,
- L'évolution du Système d'Information pour s'aligner sur les besoins métiers

1.1.3.2. Les fonctions des services de la DSI

La DSI s'appuie sur 3 services. La Direction compte 65 agents.



Organisation de la DSI

Service Production et Infrastructure (SPI)

- Gestion opérationnelle des infrastructures systèmes et réseau du département,
- Définition des standards techniques,
- Architecture et urbanisation de l'infrastructure SI,
- Exploitation au quotidien des plateformes techniques,
- Gestion de la téléphonie fixe,

Service Etude et Réalisation (SER)

- Analyse et définition des besoins (AMOA),
- Architecture et Urbanisation du SI
- Qualification en environnement de test des solutions,
- Développements spécifiques et open source,
- Paramétrage technique applicatif,
- Support technique logiciel métier de second niveau,
- Pilotage opérationnel des projets,
- Gestion des plannings, des ressources et des marchés,
- Responsable du Pôle SIG,

Service Environnement de Travail de l'Utilisateur (SETU)

- Acquisition et déploiement des postes et logiciels informatique,
- Maintien en conditions opérationnelles,
- Support 1er et 2ème niveau utilisateur,
- Attribution des accès réseau,

- Gestion de la téléphonie mobile,
- Intégrations applicatives/bureautiques dans l'environnement de travail de l'utilisateur

En parallèle de ces trois services opérationnels, la DSI gère également la sécurité du système d'information..

1.1.3.3. Les chantiers actuels du SI

- Urbanisation,
- Optimisation des ressources,
- Dématérialisation des processus métiers (AMOA)
- Sécurité,
- Virtualisation,
- Gestion du nomadisme,
- Interopérabilité,
- Modélisation processus métiers.

1.1.3.4. L'environnement informatique DRM

Tous les courriers sont actuellement traités manuellement au sein du service courrier. Au sein du service, 8 postes informatiques sont comptabilisés en 2016. Les postes informatiques sont principalement utilisés pour la bureautique. Ils sont connectés entre eux et permettent ainsi le travail en réseau. Des équipements supplémentaires pourront être déployés pour les besoins du projet lié à la dématérialisation du courrier.

L'essentiel des agents de service courrier sont peu formés à l'informatique, d'où la nécessité de mettre en place des solutions ergonomiquement intuitives et agréables à utiliser ainsi qu'un accompagnement au changement important et adapté à la situation.

Dans ses prestations d'accompagnement, le titulaire devra respecter notamment les orientations techniques définies par la Direction des Systèmes d'Information pour interfacer certaines des briques fonctionnelles dans le système d'information du Conseil départemental de l'Essonne.

1.2. Le projet

1.2.1. L'objectif du projet

Le Conseil départemental de l'Essonne souhaite moderniser et rendre plus efficiente la gestion des courriers entrants et sortants au sein de chacune de ses directions. Ainsi, ce projet a pour objectif d'informatiser les courriers ainsi que les données recueillies sur ces derniers : factures, lettres personnelles, recommandées, tout en intégrant la production des statistiques d'activité.

Le projet représente, de plus, une opportunité pour la DRM du Conseil départemental de l'Essonne :

- d'améliorer les conditions d'exercice du travail administratif,
- de fiabiliser et sécuriser les courriers, et les statistiques d'activité qui en sont extraites,
- de tracer les courriers pendant leur instruction,
- de mieux suivre les délais de réponse pour chacun des types de courriers reçus,
- de contribuer à l'amélioration des processus métiers liés à la facturation en gérant en central l'ensemble des factures adressées à la collectivité,
- d'archiver les courriers dans un système fiable et pérenne.

1.2.2. Eléments de volumétrie

Le Conseil départemental de l'Essonne reçoit en moyenne 800 courriers par jour sur son site central d'Evry. Il faut ajouter à ce chiffre les différents courriers envoyés directement dans les sites distants comme les Maisons Départementales des Solidarités (MDS), les centres de Protection Maternelle et infantile (PMI)…Le volume est aujourd'hui difficile à estimer.

Toutes les directions de la collectivité, au nombre de 30 sont concernés par la dématérialisation du courrier. Le nombre d'utilisateurs estimés est environ de 500. Ce nombre pourra évoluer tout au long du projet en fonction des nouveaux enjeux qui pourront être donnés par la Direction générale.

En moyenne, 1000 courriers arrivent chaque jour au Conseil départemental de l'Essonne.

1.2.3. Stratégie de déploiement

Le département de l'Essonne souhaite déployer progressivement la future solution au sein de ses directions. Cette stratégie permettra entre autre à la DRM, la DSI et le cas échéant aux directions pilotes de vérifier que le progiciel est apte à répondre aux besoins fonctionnels et techniques de la collectivité. Cette aptitude sera donc évaluée tout au long du déploiement de la solution. Tout lancement de phase sera conditionné par l'aptitude de la phase précédente.

6 phases fonctionnelles ont été identifiées en l'occurrence :

Phase 1 : Indexation automatique des courriers (hors factures) préalablement numérisés, traités et vidéo-codés (solution LAD, RAD, OCR) dans la future solution de gestion de courrier puis distribution automatique dans les directions via cette même solution

- Phase 1.1 : Traitement des courriers sensibles par les directions métiers
- Phase 1.2 : Traitement des courriers non sensibles par les directions métiers

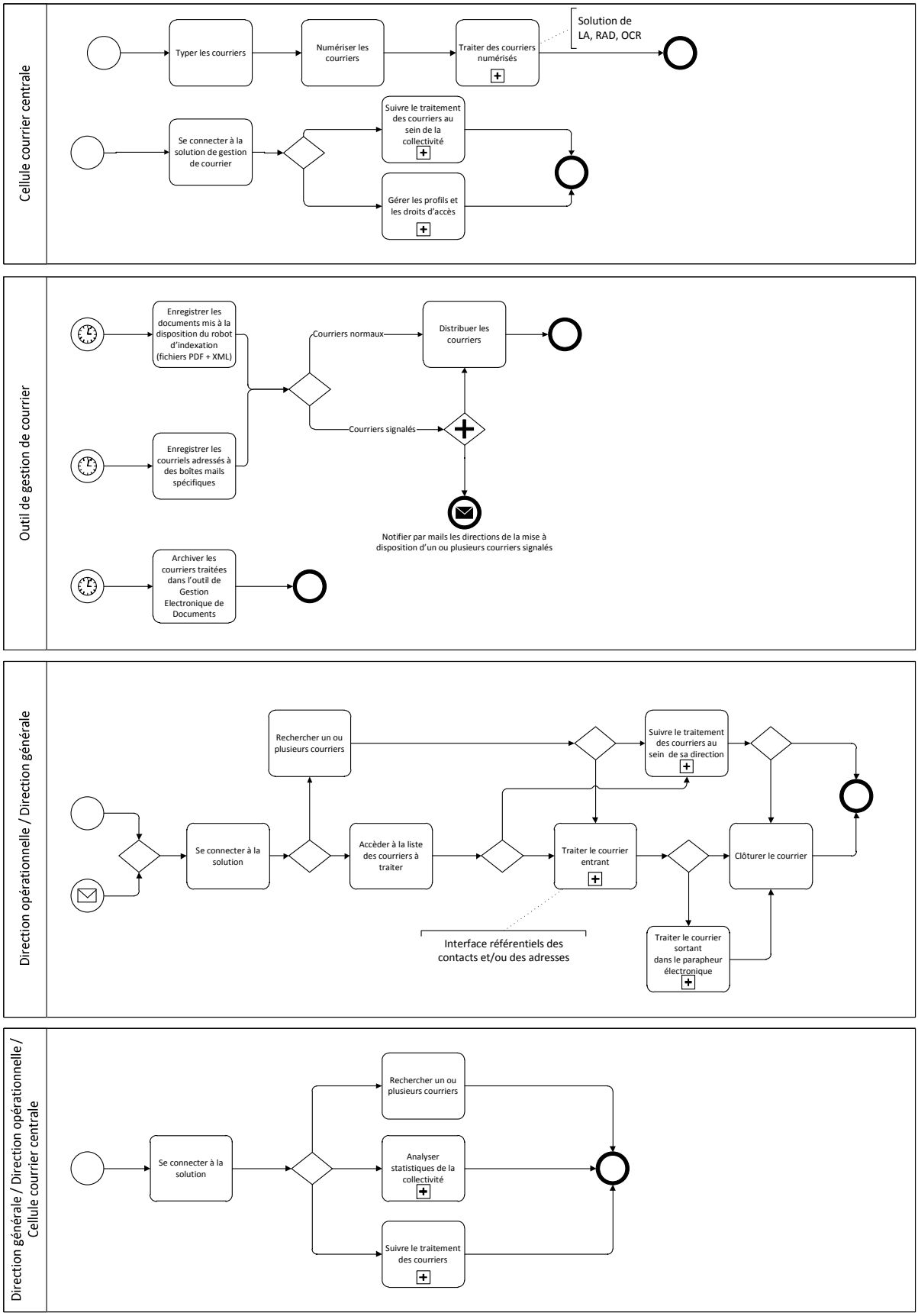
Phase 2 : Dématérialisation des courriers arrivant dans les sites distants (MDS, PMI…)

Phase 3 : Gestion des courriers sortants

- Phase 3.1 : Courriers sortants sans utilisation du parapheur électronique
- Phase 3.2 : Interface avec le parapheur électronique

Phase 4 : Gestion des courriers internes

2. MACRO PROCESSUS ENVISAGE POUR LA GESTION DU COURRIER



3. LES BESOINS FONCTIONNELS

3.1. Gestion des profils et des droits

La gestion du courrier au sein du département de l'Essonne représente dans un premier temps plus de 500 professionnels répartis autour d'une trentaine de directions toutes concernées par la dématérialisation des courriers. Chaque personne en fonction de sa direction, service et fonction aura donc des droits personnels et potentiellement différents des autres utilisateurs.

La prise en charge d'un courrier est pluridisciplinaire au sein d'une direction. Les données seront donc partagées pour une partie d'entre elles entre tout ou partie des professionnels. Des droits doivent donc être partagés.

Id	Fonctionnalités obligatoires	Commentaire
FP1	Gérer des profils / des groupes	Définir des profils : par direction, service, fonction
FP2	Gérer des droits sur le courrier	Les administrateurs fonctionnels peuvent donner des droits d'accessibilités sur un document, un formulaire (lecture, modification, pas d'accès) voire une donnée de ce formulaire
FP3	Gérer des droits pour un utilisateur en particulier	Pouvoir affecter à un utilisateur en particulier des droits de lecture, modification, suppression sur les différents volets d'un courrier entrant ou sortant
FP4	Gérer des délégations de droits	Pouvoir transférer temporairement ses niveaux de droits d'utilisation à une autre personne
FP5	Gérer automatiquement les droits d'accès à partir de l'organigramme de la collectivité	Interrogation de l'annuaire d'entreprise pour attribuer automatiquement des droits à un utilisateur au sein de sa nouvelle direction ou de son nouveau service. A l'inverse retirer automatiquement les droits d'accès en cas de départ de la direction et/ou d'un service

3.2. Gestion des courriers entrants

Le courrier arrive au département :

- Par voie postale (courrier papier)

  L'enregistrement de ce courrier dans le progiciel de gestion du courrier sera automatisé (indexation et distribution). Chaque courrier sera, préalablement à son enregistrement dans l'outil, numérisé puis traité à l'aide d'un outil de LAD, RAD et OCR dont l'acquisition est en cours au sein de la collectivité. Le courrier sera mis à la disposition de la future solution sur un serveur de fichiers constitué d'un ou plusieurs répertoires (1 par direction par exemple) selon un format standard restant à définir (TIFF, PDF, JPEG…).

- Par voie électronique (par mail adressé à une boîte générique telle que contact@cd-essonne.fr par exemple ou par mail adressé directement à un agent de la collectivité)

  Ce type de courrier sera automatiquement intégré dans la future solution à l'aide d'une synchronisation entre le serveur de messagerie et cette dernière.

Id	Fonctionnalités obligatoires	Commentaire
CE1	Enregistrer manuellement un courrier	
CE2	Enregistrer automatiquement un courrier	Courriers, courriels ou notes selon la procédure décrite ci-dessous
CE3	Horodater un courrier	Permettre lors du traitement du courrier de savoir

Id	Fonctionnalités obligatoires	Commentaire
		quand le courrier a été enregistré dans le logiciel et par qui
CE4	Enregistrer différents types de courrier	Permettre de typer les courriers pour associer à chaque type de courrier un processus métier (destinataires, délai de réponse, niveau de priorité…)
CE5	Enregistrer/ Modifier les informations ou métadonnées associées à un courrier	Automatique dans le cadre d'une indexation automatique ou manuellement dans le cas contraire
CE6	Compléter les métadonnées d'un courrier à partir d'informations issues des autres bases de données de la collectivité	Exemple : récupérer automatiquement le canton de l'expéditeur du courrier à partir de son code postal lors de l'indexation automatique Exemple 2 : faire appel à des référentiels du département dans le formulaire d'enregistrement d'un courrier (liste…)
CE7	Réorienter le courrier manuellement vers la bonne direction en cas d'erreur d'aiguillage	Permettre à un utilisateur de réorienter le courrier en cas d'erreur lors de la distribution automatique
CE8	Positionner des alertes dès qu'un ou plusieurs courriers sont enregistrés dans la solution	Permettre à une secrétaire de direction par exemple d'être notifié lorsqu'un ou plusieurs courriers sont disponibles dans la boîte aux lettres de sa direction
CE9	Gérer les recommandés	Permettre la saisie manuelle ou à l'aide d'une douchette des informations liées à un recommandé (Numéro, niveau….)
CE10	Attribuer automatiquement un numéro d'enregistrement unique du courrier dans la solution et afficher ce dernier dans le cadre d'un enregistrement manuel du courrier	

Id	Fonctionnalités optionnelles	Commentaire
CE11	Enregistrement direct d'un courriel depuis Microsoft Outlook vers la future solution de gestion de courrier	Permettre à un agent d'enregistrer dans la future solution un courriel depuis sa boîte électronique (mail adressé directement au Président par exemple….)
CE12	Mise à jour de la base de contact lors de l'enregistrement automatique du courrier dans la solution et traçabilité de cette mise à jour	Permettre la mise à jour de la base de contacts gérée par le département le cas échéant
CE13	Intégrer des données externes lors de l'enregistrement du courrier dans la solution	Lors de l'indexation d'un courrier, interrogation d'une source externe (base de données, fichiers…) afin de compléter automatiquement des métadonnées au courrier entrant
CE14	Imprimer depuis la fiche du courrier le numéro d'enregistrement du courrier sous forme de code barre ou de flash code	Permettre à la cellule courrier de coller le code barre ou le flash code sur le courrier

3.3. Gestion du cycle de vie des courriers

Directement ou en partenariat avec les autres collectivités ou l'Etat, le Conseil départemental intervient dans de nombreux aspects de la vie quotidienne. Différents types de courriers peuvent donc lui être envoyés (factures, demande de subvention, déclaration d'une situation préoccupante, demande de travaux…). La future solution de gestion du courrier doit donc permettre d'associer un processus métier à chaque type de courrier afin de permettre à ses directions de les instruire dans les meilleures conditions (rapidité, traçabilité…).

Id	Fonctionnalités obligatoires	Commentaire
CV1	Modéliser un processus métier pour chacun des types de courrier identifiés (entrants et sortants)	Définir automatiquement les destinataires du courrier tout au long du processus associé à ce dernier, définir les délais de réponses, les alertes si retard dans le traitement, les délais d'archivage…
CV2	Gérer plusieurs versions de processus métier pour un type de courrier en particulier	Lors de la modification d'un processus métier ne pas bloquer les courriers associés à la version -1 du processus
CV3	Transférer manuellement et automatiquement les courriers vers outil de GED après traitement	Pré-archiver les courriers et ne conserver dans la solution de gestion de courrier que le courrier en cours de traitement et traités depuis moins de N mois
CV4	Consulter l'historique des actions réalisées sur un courrier pendant son instruction	Savoir qui a fait quoi et quand
Id	**Fonctionnalités optionnelles**	**Commentaire**
CV5	Exporter/importer des processus	Permettre de travailler sur des processus BPMN2 générés via l'outil de modélisation transverse de la collectivité (exemple BONITA)
CV6	Enregistrer directement le courrier entrant ou sortant dans la GED de la collectivité	

3.4. Traitement des courriers

Id	Fonctionnalités obligatoires	Commentaire
TC1	Accéder à la liste des courriers du jour	Permettre à un agent d'une direction de connaître le nombre de courrier du jour et d'accéder directement à ces derniers
TC2	Consulter la fiche courrier et le courrier sur une même page	
TC3	Enregistrer une note privée sur la fiche courrier	Seul le créateur de la note privée aura accès à cette information tout au long du traitement du courrier
TC4	Enregistrer une note publique sur la fiche courrier	Toutes les personnes devant intervenir sur le traitement du courrier pourront accéder à l'information
TC5	Classer les courriers en fonction d'un plan de classement paramétrable et propre à la collectivité	Classer le courrier et préparer le pré-archivage (cf CV3)

Id	Fonctionnalités obligatoires	Commentaire
TC6	Modifier les informations (méta données) relatives à un courrier	Permettre à un agent de changer manuellement les délais de traitement d'un courrier ou de modifier son type
TC7	Permettre à un utilisateur en fonction de ces droits de suivre les délais de traitements des courriers en cours de traitement pour sa direction, son service…	Permettre à un ou plusieurs agents (en fonction de leur droit d'accès) de suivre les délais de traitement du courrier à tout moment
TC8	Identifier tous les courriers en retard via une vue (interface) dédiée	Permettre à un agent en fonction de ses droits de lister tous les courriers en retard d'une direction en particulier ou d'un service en particulier
TC9	Relance manuelle d'un utilisateur ou d'un groupe d'utilisateurs concernant le traitement d'un courrier en particulier	Permettre à un administrateur fonctionnel de relancer par mail un utilisateur en cas de retard de traitement sur un courrier
TC10	Notification électronique automatique en cas de retard sur les délais de traitement du courrier	Permettre à un agent ou un groupe d'agents d'être alertés par mail lorsque le traitement d'un courrier arrive à échéance ou si le délai de traitement est dépassé
TC11	Proposer à un utilisateur une page d'accueil spécifique à son contexte et paramétrable	Permettre à un utilisateur dès sa connexion au logiciel de prendre connaissances des informations essentielles à une gestion du courrier efficiente
Id	**Fonctionnalités optionnelles**	**Commentaire**
TC12	Ajouter une note directement sur l'image du courrier (PDF, TIFF…)	Permettre à un agent d'ajouter un commentaire directement sur le courrier PDF

3.5. Gestion des courriers sortants

Id	Fonctionnalités obligatoires	Commentaire
CS1	Enregistrer manuellement un courrier sortant	
CS2	Utiliser des modèles de documents pour générer automatiquement le courrier ou le squelette du courrier (adresse destinataire = adresse expéditeur…)	
CS3	Gérer des notes personnelles au courrier sortant	
CS4	Gérer des notes publiques au courrier entrant	
CS5	Positionner des alertes (alerte dès que courrier sortant est associé à un courrier entrant par exemple)	
CS6	Interroger la base de contact de la solution ou autre (référentiel annexe) pour récupérer automatiquement les informations concernant le destinataire si pas de courrier entrant associé	
CS7	Interface avec le i-Parapheur de l'ADULLACT (circuit de validation du courrier sortant le cas échéant))	Transfert du document dans le parapheur électronique directement depuis le logiciel de gestion de courrier

Id	Fonctionnalités optionnelles	Commentaire
CS8	Enregistrer manuellement un courrier sortant depuis les outils d'éditions tels que Microsoft Word par exemple	
CS9	Enregistrer manuellement un courriel depuis le client de messagerie d'un agent (Microsoft Outlook)	
CS10	Interroger la base de contact de la collectivité pour récupérer automatiquement les informations concernant le destinataire si pas de courrier entrant associé	

3.6. Recherche des courriers

Id	Fonctionnalités obligatoires	Commentaire
RC1	Rechercher une donnée textuelle au sein d'un courrier entrant et/ou sortant	
RC2	Rechercher une donnée issue de la fiche descriptive du courrier entrant et/ou sortant (métadonnées) via un formulaire de recherche multicritères	
RC3	Afficher le résultat d'une recherche sous forme de liste et accéder à la fiche du courrier depuis cette liste	
RC4	Enregistrer des requêtes personnelles	
Id	**Fonctionnalités optionnelles**	**Commentaire**
RC5	Afficher simultanément plusieurs fiches courrier sur une même page (fiche du courrier entrant et fiche du courrier sortant liés à ce dernier)	
RC6	Exécuter des requêtes proposées par les administrateurs fonctionnels	

3.7. Statistiques

Id	Fonctionnalités obligatoires	Commentaire
ST1	Afficher en fonction des droits de l'utilisateur des statistiques mensuelles concernant les courriers entrants (Répartition mensuelle des courriers entrants par direction, répartition mensuelle des courriers entrants par type de courrier, Délai de traitement moyen des courriers en fonction de la direction...)	Permettre aux utilisateurs, aux administrateurs fonctionnels, aux dirigeants de la collectivité de suivre le traitement du courrier
ST2	Afficher en fonction des droits de l'utilisateur des statistiques mensuelles concernant les courriers sortants (Répartition mensuelle des courriers sortants par direction, répartition	Permettre aux utilisateurs, aux administrateurs fonctionnels, aux dirigeants de la collectivité de suivre le traitement du courrier

Id	Fonctionnalités obligatoires	Commentaire
	mensuelle des courriers sortants par type de courrier, Délai de traitement moyen des courriers en fonction de la direction… .	
ST3	Extraire des données d'activité et de description des courriers entrants et sortants	Extraction de données sous différents formats (Excel, PDF…)
ST4	Générer des tableaux de bord récurrents de base	
ST5	Extraire des données sous différents formats	
ST6	Générer de nouvelles statistiques	
Id	**Fonctionnalités optionnelles**	**Commentaire**
ST7	Extraire les données de la base dans un univers BO	Permettre de déléguer la production de statistiques à l'outil Business Object
ST8	Générer un PDF de synthèse concernant un courrier entrant ou sortant	Traçabilité de toutes les opérations réalisées (qui, quand, quoi)

3.8. Fonctionnalités autres

Id	Fonctionnalités obligatoires	Commentaire
FD1	Extraire des tableaux de synthèse par type de courrier, par date d'enregistrement…	Permettre aux utilisateurs, aux administrateurs fonctionnels, aux dirigeants de la collectivité d'éditer depuis le progiciel des états

4. URBANISATION ET ARCHITECTURE

4.1. Généralités

Le titulaire devra respecter les orientations techniques définies d'un commun accord entre la Direction des Systèmes d'Information (DSI) du département de l'Essonne et le titulaire pour s'insérer dans l'architecture générale.

D'une façon générale, la future solution doit être ouverte aux technologies Intranet ou Client / Serveur. Les propositions d'architecture technique peuvent être dans l'une de ces 2 technologies ou un mixte.

Les futurs services pouvant être acquis pendant la durée du marché nécessiteront :

- La mise en place d'un protocole d'échanges d'informations entre eux et les applications constituant le système d'information du département de l'Essonne
- Un renforcement et une prise en compte en amont des règles de sécurité,
- Le respect par le titulaire des préconisations techniques du département de l'Essonne définies par sa Direction des Systèmes d'Information.

4.2. Référentiels et standards d'accessibilité

Afin de garantir la sécurité et l'accessibilité des systèmes d'information, le département de l'Essonne se conforme aux référentiels généraux élaborés par la DGME en lien avec les ministères

- le Référentiel Général de Sécurités (RGS),
- le Référentiel Général d'Interopérabilité (RGI),
- le Référentiel Général d'Accessibilité des Administrations (RGAA),

- **Le référentiel général de sécurité (RGS)** définit un ensemble de règles et de bonnes pratiques en matière de sécurité des systèmes d'information applicables par les autorités administratives dans la sécurisation de leurs systèmes d'information. Le RGS a pour principal objectif de développer la confiance des usagers et des administrations dans leurs échanges numériques. Il contient un ensemble de règles de sécurité, fixées dans le corps du document RGS ou dans les documents annexés, qui s'imposent aux autorités administratives et aux prestataires qui les assistent. Le décret n° 2010-112 du 2 Février 2010 porte création du Référentiel Général de Sécurité (RGS).
  Comme toute collectivité territoriale, le département se doit donc de respecter ces exigences.
  La version en cours du RGS (Version 2.0) est applicable depuis le 1er Juillet 2014, suite à la publication au journal officiel de l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité.

  http://references.modernisation.gouv.fr/rgs-securite

- **Le référentiel général d'interopérabilité (RGI)** est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration. Il fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. L'arrêté du 9 novembre 2009 porte approbation du référentiel général d'interopérabilité

  https://references.modernisation.gouv.fr/sites/default/files/RGI_Version1%200.pdf

- **Le référentiel général d'accessibilité des administrations (RGAA)** complétera, dans le cas où le titulaire propose une architecture N-tiers, les référentiels précédents en ce qui concerne les règles fondées sur les standards internationaux, mais aussi sur les conditions et méthodes d'évaluation des services pour permettre l'accès – notamment des personnes handicapées – aux voies électroniques d'information et télé services publics. L'approche multi canal permet de traiter tant l'Internet que le téléphone ou l'accès via la télévision.

  https://references.modernisation.gouv.fr/rgaa-3-0

- **Le référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (Cloud computing) –** référentiel d'exigences définit un ensemble d'exigences et recommandations qu'un prestataire proposant une offre sécurisée de service d'informatique en nuage doit respecter, afin de garantir des niveaux de compétence, de qualité et de confiance qui permettent de lui confier des données.

  http://www.ssi.gouv.fr/uploads/IMG/pdf/cloud_referentiel_exigences_anssi.pdf

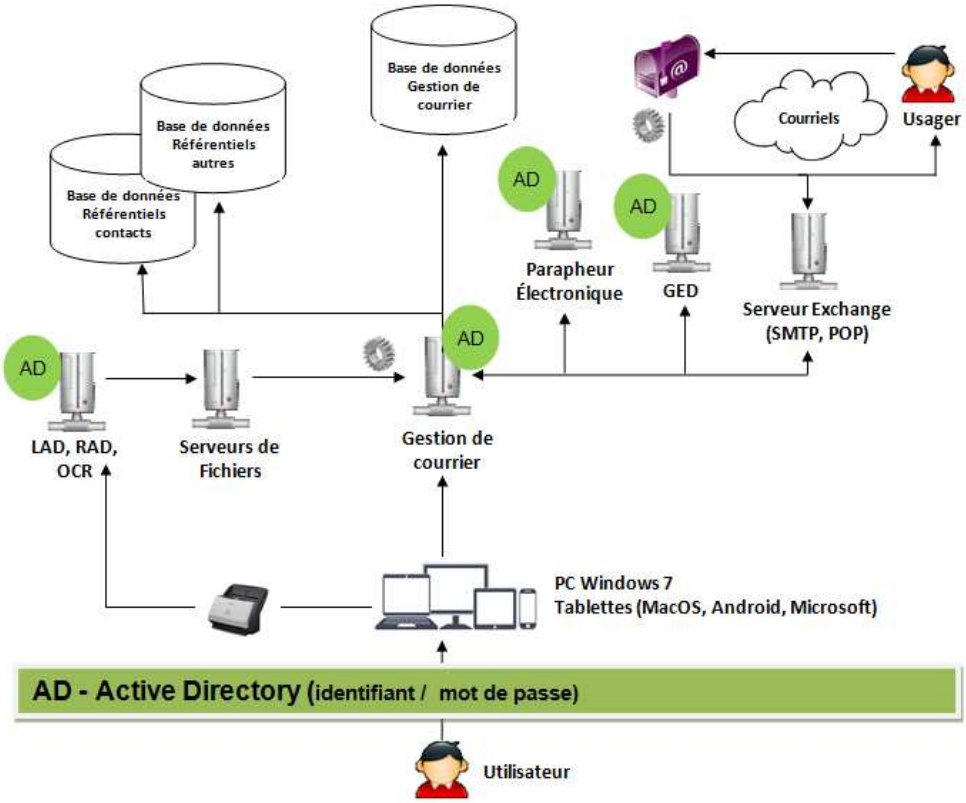
4.3. Interopérabilité, urbanisation du système d'information (SI)

Assurer l'interopérabilité des briques logicielles est essentiel pour le département. Pour cela le département de l'Essonne a fait le choix de s'appuyer sur les principaux standards ouverts du marché (W3C …).

Si le titulaire propose une architecture N-tiers, la solution devra reposer sur un standard ouvert au sens de l'art 4 de la loi n°2004-575 du 21 juin 2004 (loi pour la confiance dans l'économie numérique), afin de garantir l'interopérabilité effective entre les systèmes actuels et à venir.

5. CARTOGRAPHIE APPLICATIVE

5.1. Cartographie applicative envisagée



5.2. Annuaire technique

Le système se connectera obligatoirement à l'annuaire Microsoft Active Directory (AD) du département de l'Essonne pour authentifier un utilisateur au système. Le titulaire proposera un système d'authentification conforme aux exigences décrites dans le paragraphe 6.3.2 du CCTP et l'annexe 4 (10.4).

La mise en œuvre de cette interface pourra faire l'objet d'un bon de commande aux tarifs visés au bordereau des prix. Cette interface devra être opérationnelle dès la phase 1 du projet (voir ci-dessus)

5.3. Outil de LAD, RAD, OCR

Comme le montre le macro-processus du paragraphe 2 et l'annexe 5 (10.5) de ce CCTP, la future solution devra pouvoir indexer et transmettre automatiquement à une direction les courriers qui seront préalablement numérisés par le service courrier puis traités à l'aide d'un outil de LAD, RAD, OCR. Cet outil est actuellement en cours d'acquisition par le département.

La mise en œuvre de cette interface pourra faire l'objet d'un bon de commande sur la base d'un devis défini aux tarifs de prestations du bordereau des prix. Cette interface devra être opérationnelle dès la phase 1 du projet (voir ci-dessus).

5.4. Messagerie

Le conseil départemental de l'Essonne souhaite que la future solution récupère automatiquement les courriels envoyés à une adresse générique comme contact@cg91.fr par exemple. Le Conseil départemental de l'Essonne souhaiterait également qu'un agent puisse, s'il en a les droits, enregistrer depuis son client de messagerie (Microsoft Outlook) un ou plusieurs courriels (avec le(s) pièce(s) jointe(s)) directement dans la future solution.

De la même manière, la future solution devra pouvoir, en fonction du processus métier associé au courrier traité, envoyer des courriels (accusé de réception…) aux personnes ayant écrit au département et ce quel que soit le format de ce dernier (papiers, mail…)

5.5. Outil de gestion électronique de Documents

Dans le cadre du cycle de vie d'un courrier, le conseil départemental de l'Essonne souhaite pouvoir déplacer les courriers et leurs métadonnées du progiciel de gestion de courrier vers son outil de gestion de documents (GED) Alfresco. Ce processus devra pouvoir être automatisé et s'adaptera au plan de classement de la collectivité actuellement en cours de définition.

La mise en œuvre de cette interface pourra faire l'objet d'un bon de commande sur la base d'un devis défini aux tarifs de prestations du bordereau des prix.

5.6. Parapheur électronique

Dans le cadre d'un processus de gestion des courriers sortants ou des notes internes par exemple, la progiciel de gestion de courrier devra obligatoirement pouvoir s'interfacer avec le parapheur électronique de la collectivité en l'occurrence le libriciel i-Parapheur proposé sous licence libre par l'ADULLACT.

5.7. Référentiel des contacts

Le département travaille actuellement sur son référentiel des contacts. La future solution devra pouvoir s'interfacer avec ce référentiel lors du processus de gestion des courriers entrants et sortants. Si la future solution propose son propre référentiel des contacts, ce dernier pourra être maintenu pour le bon fonctionnement de la solution mais devra être mise à jour via des web services ou autres.

La mise en œuvre de cette interface pourra faire l'objet d'un bon de commande sur la base d'un devis défini aux tarifs de prestations du bordereau des prix. Le calendrier de mise en œuvre de cette interface est fonction du calendrier lié au projet référentiel des contacts.

6. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DU CONSEIL DEPARTEMENTAL

6.1. Contexte technique du département

Qu'il s'agisse d'extension du périmètre fonctionnel ou de migration technique de modules existants, le titulaire devra prendre en compte les attendus techniques décrits ci-dessous.

D'une manière générale, le département a pour stratégie de suivre les évolutions techniques de ses partenaires (Oracle, Microsoft, …) et de développer les applications en mode web afin de répondre aux besoins de mobilité et de télétravail.

L'annexe 2 résume et complète ce qui suit.

6.1.1. Les postes de travail

Les postes de travail sont des micro-ordinateurs dont la configuration minimale est composée d'un processeur multi cœurs, 128Go sur disque dur et 4Go de mémoire centrale, fonctionnant avec le système d'exploitation Windows 7 Pro 64 bits.

Les logiciels retenus par la DSI sont :

- Prioritairement la suite MS Office 2010 32 bits et, à défaut, la suite bureautique OpenOffice v4,
- La messagerie Exchange 2013 et le client Outlook de la suite Office 2010
- Le navigateur Internet Explorer IE10.
- Acrobat Reader version 11 minimum,
- PDFCreator V1.7.0
- L'outil de déploiement sur les postes SCCM,
- L'antivirus McAfee VirusScan 8.8 et le pare-feu McAfee HIP 8.0 pour les postes fixes et les portables (migration à venir)

Les équipements connectés au poste de travail peuvent être :

- Imprimantes/copieurs lasers Canon ou autres constructeurs (réseau ou local), A3/A4, couleur et/ou noir et blanc, recto verso,
- Scanners compatible TWAIN (HP ou équivalents)

Afin de sécuriser le SI du département, les utilisateurs disposent de droits restreints sur les postes de travail. Ainsi, les utilisateurs ne peuvent pas installer de logiciels (aucun droit administrateur) et les programmes ne peuvent pas apporter de modifications à l'ordinateur ou au système lors de leur exécution (contrôle de compte utilisateur UAC au niveau 4).

6.1.2. Les équipements nomades

Les tablettes sont de la marque APPLE et de type IPAD sous IOS 7 minimum et de capacité 16, 32 ou 64 Go. Les tablettes sont compatibles Wifi et 3G. D'autres tablettes peuvent être déployées en fonction du projet (fonction du type de connexion réseau requise).

Les ordinateurs portables sont des micro-ordinateurs dont la configuration minimale est composée d'un processeur multi cœurs Intel ou AMD, 250Go sur disque dur et 4Go de mémoire centrale, fonctionnant avec le système d'exploitation Windows 7. Connexion réseau filaire et/ou sans fil.

Les logiciels retenus par la DSI sont identiques à ceux retenus pour les postes de travail. Les droits administrateurs locaux sont retirés afin que les utilisateurs ne puissent installer des produits.

6.1.3. Les serveurs WEB

Les serveurs WEB installés sont :

- IIS7 ou IIS7.5 pour la gestion des transferts de documents HYPERTEXT selon le protocole http et TLE 1.2 minimum pour le mode sécurité
- Apache 2.2
- Tomcat 6

6.1.4. Les SGBDR

Dans le cadre des progiciels hébergés par le département de l'Essonne, les SGBDR retenus par la DSI sont prioritairement :

- PostgreSQL 9.4 sous Linux CENTOS 7.2,
- MySQL v5.7,
- Oracle 11G ou 12C sous Windows 2012/R2 64 bits en version serveur standard (et non entreprise), Client Oracle 11.2.0.4.32 bits sur le poste de travail (version engagée)
- SQL Serveur 2012

Afin de garantir l'archivage des données, l'interopérabilité et plus généralement d'urbaniser le système d'information du département, le titulaire s'engage à communiquer à chaque mise à jour, les différents modèles de données de la base de production et de son infocentre :

- Le macro modèle en cas de modélisation complexe,
- Le modèle conceptuel et logique de données au sens UML,
- Le schéma et descriptif des interfaces, connecteurs, web services

La personne publique s'engage à ne pas communiquer ces éléments à un tiers externe à la DSI conformément aux clauses telles que définies dans le CCAG TIC

6.1.5. Les protocoles et logiciels systèmes

Les standards définis par la DSI sont :

- Oracle11.2.0.4 32 bits pour la couche de communication et d'accès aux bases de données Oracle,
- ODBC V2 32 bits,
- ADO (interface standard Microsoft d'accès aux données),

- Annuaire Active Directory 2012 R2 pour les identifications internes
- DNS Microsoft 2012 R2
- Serveur Exchange 2013 / Client Outlook de la suite Office 2010

6.1.6. Les systèmes d'exploitation

Les systèmes serveurs pourront être installés sur des machines virtuelles utilisant la technologie RDS. Les standards actuels définis par la DSI sont :

- Windows 2012 R2 64 bits pour les serveurs hébergeant les bases de données Oracle,
- Linux CentOS 7.2 et de bases de données PostgreSQL,
- Windows 2012 R2 pour les serveurs de taille moyenne hébergeant les applications ou la bureautique, Windows 2012 R2 pour les serveurs d'accueil WEB ou TSE, ou Linux ES5 / CentOS 6.2 pour les serveurs d'applications WEB,
- WINDOWS 7 64 bits pour les postes de travail. Stratégies de groupes à droits restreints.

6.1.7. Les outils d'exploitation

Les applications devront pouvoir s'intégrer dans l'environnement d'exploitation en production suivant :

- Le logiciel d'ordonnancement ITPAM de l'éditeur AVANTAGE PRODUCTION
- Le logiciel de sauvegarde – restauration TIME NAVIGATOR v4.3 de l'éditeur ATEMPO,
- Le logiciel de supervision WHAT'S UP PRO v16.4.1 ou supérieur,
- Les logiciels antivirus de McAfee VirusScan pour Windows, LinuxShield, Netshield, MOVE pour les environnements virtuel
- Le logiciel WSUS 2012 pour les mises à jour Microsoft

Le titulaire sera amené à préciser de quelle façon la solution intégrera les possibilités d'utilisation des logiciels ci-dessus

6.1.8. Les outils d'édition, décisionnels, d'extraction et d'infocentre

La DSI a retenu la constitution d'un infocentre alimenté par les données utiles de certaines applications de production.

La mise à disposition d'un infocentre dédié à l'application avec ses mécanismes d'extraction est souhaitée ;

Les outils d'extraction et d'EIS (Executive Information System) retenus par la DSI sont :

- Talend open Studio 5.2.1
- Décisionnels : Business Object XI 3.1.SP5
- Editions : elles devront pouvoir être créées et maintenues par les utilisateurs, de préférence sur la base d'une solution de type bureautique.

Dans le cas où le système proposé nécessiterait le recours à des logiciels spécifiques, le titulaire est tenu de préciser les composants de base nécessaires à l'exécution de ses produits (outil d'alimentation de l'infocentre, moteur d'analyse multidimensionnelle, licences bureautiques ou éditiques...).

6.1.9. Le réseau

Le réseau du Conseil départemental de l'Essonne (voir annexe 3 (10.3) de ce CCTP) est constitué d'un MAN d'une dizaine de sites situés à Evry dont la DSI-RIA, l'Hôtel Du Département (HDD), les bâtiments France Evry, France Essonne, Centre Evry et Europe2. Une boucle optique dotée d'une bande passante de 1Gbits/s relie ces sites via les commutateurs de backbone. Les communications inter-sites sont gérées par un protocole de routage dynamique.

Les serveurs de production et de développement sont installés majoritairement à la DSI, avec des serveurs de secours sur le site France Essonne. Ces deux sites constituent le cœur du réseau.

Les sites distants (106) d'une taille de 1 à 100 postes informatiques et répartis sur l'ensemble du département, y sont connectés avec une solution VPN/MPLS opérateur redondée. Le LAN de chaque site est constitué d'un routeur de l'opérateur et de commutateurs Cisco ou basiques. Les liaisons VPN sont

soient de type SDSL avec des débits jusqu'à 4 Mbit/s ou des ADSL avec des débits jusqu'à 1Mbit/s. Un projet de déploiement en très haut débit fibre opérateur est en cours sur l'année 2016 permettant des débits compris entre 4Mo et 10 Mo selon les sites.

Toutes les adresses réseau de type publiques seront implémentées avec un FQDN et toutes les adresses réseaux privées du CD91 seront implémentées en nom DNS relatif.

6.2. Sécurité

6.2.1. Généralités

La sécurité du système d'information est un aspect important du projet.

Lors de ses développements, le titulaire doit se conformer au RGS (voir ci-dessus). Il définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Il propose également des bonnes pratiques en matière de sécurité des systèmes d'information que les autorités administratives sont libres d'appliquer. Cinq fonctions de sécurité sont retenues :

- Le traitement des vulnérabilités
- L'authentification,
- La signature électronique,
- La confidentialité,
- Le cachet,
- L'authentification serveur

Suivant le niveau souhaité s'appliquant à l'une de ces fonctions de sécurité, le RGS définit les exigences techniques et les moyens de protection pertinents en termes de produits de sécurité et d'offre de service de confiance.

Les fonctions impliquées dans le dispositif de chiffrement devront être conformes aux standards de cryptographie à clé publique : Public Key Crypto Standards (PKCS) et aux API de signature recommandées par l'administration selon le référentiel général de sécurité et le référentiel général d'interopérabilité (voir ci-dessus).

La sécurité physique (réseau, stations de travail, plates-formes) est du ressort de la collectivité et n'entre pas dans le périmètre du projet. Les éléments exposés dans les sous paragraphes suivants sont en revanche pris en compte par le titulaire.

La couverture des objectifs de sécurité, décrits ci-dessous, devra être garantie dans le produit final proposé par le titulaire.

Une revue formelle du respect des spécifications de sécurité sera réalisée, lors des recettes et des mises en exploitation. Elles seront vérifiées lors de la vérification d'aptitude et de la vérification de service régulier par le RSSI ou son représentant.

6.2.2. Traitement des vulnérabilités

En cas de vulnérabilité technique ou de faille de sécurité sur un composant de la solution ou suite à la parution de la nouvelle version d'un composant de la solution, le fournisseur doit vérifier la compatibilité du correctif ou de la nouvelle version de composant avec sa solution, la non régression suite à application du correctif et fournir dans un délai fixé contractuellement une procédure de mise à jour, un correctif ou une nouvelle version packagée pour la solution.

En particulier, le fournisseur doit proposer une version compatible avec des versions de composants ayant au plus un écart de 2 versions majeures avec la version la plus récente.

Ce suivi des correctifs et des évolutions concerne tout particulièrement Java et FlashPlayer pour les postes de travail ; Java, Tomcat ou OpenSSL pour les serveurs.

6.2.3. Authentification

La gestion des comptes d'accès doit être intégrée à l'annuaire AD du département de l'Essonne, via le protocole LDAPv3, NTLM ou Kerberos. Dans le cas du protocole LDAP, les échanges entre la future solution et cet annuaire devront être sécurisées via les protocoles SSL V3 ou TLS.

Dans le cas d'une architecture Web, la valeur saisie dans le champ mot de passe du formulaire ne doit pas être visible des personnes environnantes. Le mot de passe ne doit pas non plus être pré-rempli par le navigateur.

La durée de vie de la session ne doit pas par défaut être équivalente à la durée de vie de la fenêtre du navigateur. Il est raisonnable de clore la session après 10 minutes d'inactivité.

Une déconnexion explicite par l'utilisateur doit toujours être possible. Il faut donc fournir à l'utilisateur la possibilité d'utiliser un bouton « se déconnecter » afin d'écourter sa session.

Dans tous les cas :

- La connexion de la future solution à l'AD ne doit pas être anonyme (connexion anonyme non autorisée)
- Les données relatives à l'authentification des utilisateurs ne doivent pas être interceptées en clair
- Les mots de passe locaux, s'ils existent, doivent être stockés chiffrés en base,
- Tous les accès à l'application seront tracés et les données de connexions conservées pendant un an

6.2.4. Habilitations

Le système d'habilitation des utilisateurs (notion de profil relative aux droits d'accès aux services et aux données) doit permettre de répondre aux contraintes de fonctionnement de la collectivité.

Le cloisonnement des traitements impose de donner aux utilisateurs des accès différenciés au système d'information en fonction de leur droit d'en connaître. Le produit final inclura donc un outil permettant dans la mesure du possible :

- de gérer les droits de création, modification, suppression et lecture sur les données (et ce pour chaque donnée ou groupe de données),
- de créer et d'administrer différents profils d'accès,
- d'affecter un ou plusieurs profils à un utilisateur,
- de mettre à jour les profils (création, modifications, suppression) dynamiquement avec prise en compte "à chaud" des modifications intervenues,
- de tracer les opérations de gestion des droits d'accès,
- les sessions utilisateurs ne doivent pas pouvoir être rejouées,
- certains traitements ne servent aux personnes habilitées que ponctuellement dans des phases d'étude ou de simulation avant validation. Le système doit garantir la destruction de ces traitements et des données qui en résultent.

6.2.5. Gestion des droits d'accès systèmes, bases de données et progiciel

Pour des raisons de sécurité, tous les comptes par défaut associés aux systèmes d'exploitation, à la base de données, au serveur d'application et au progiciel doivent pouvoir être modifiés par le département. De nouveaux comptes disposant des mêmes droits seront créés par le titulaire à partir d'une liste communiquée par le chef de projet de la collectivité.

6.2.6. Confidentialité des données

La confidentialité des données justifie un certain degré de sécurité :

- les transactions doivent être sécurisées par l'utilisation de procédés chiffrant les données et réputés sûrs comme SSL (V3 128 bits minimum) ou TLS (préférence du département). Ce mécanisme doit être aisément déconnectable par des personnes habilitées,
- ces procédés doivent pouvoir être mis en œuvre sur tous les protocoles utilisés par le système pour la transmission de données sensibles (HTTPs, LDAPs, etc.),
- le produit final doit permettre le chiffrement et le déchiffrement des données en base et le cas échéant des fichiers,

- le produit final doit pouvoir empêcher la mise en cache des données et donner la possibilité du masquage (ou non-affichage) des URL,
- le produit final doit pouvoir empêcher de rejouer une session (impossibilité de rejouer une URL avec des droits différents capture de paquets réseaux, technique de « man in the middle »).

6.2.7. Intégrité des données

La base de données de la future solution est l'unique source d'information des agents et se doit d'être totalement fiable.

Il est souhaité que les sessions soient journalisées et archivées. Des fonctionnalités de traçabilité des opérations seront implémentées ainsi que des mécanismes "d'accounting" (notion de journaux de connexions)

- Le titulaire doit proposer un processus de contrôle d'intégrité des flux d'interopérabilité entrant pouvant être mis en œuvre,
- Les accès directs aux données autrement que par l'applicatif doivent être impossibles, pour les utilisateurs de l'applicatif. Les seuls pouvant bénéficier de cet accès seront les logiciels interopérables (exemple : Business Object) et les administrateurs ;
- La gestion de la multisession devra garantir l'intégrité de toutes les données manipulées dans les transactions considérées. En cas de conflit entre deux sessions, un message clairement défini devra alerter l'utilisateur.

Le titulaire offrira un outil pour vérifier l'intégrité des données de la base le cas échéant. Le produit final doit disposer d'un outil de roll-back ou d'un mécanisme de reprise en cas de coupure de session lors des télétransmissions.

6.2.8. Contraintes pour certains sites

Les flux générés par l'application doivent traverser différents réseaux (dont notre plateforme de sécurité et un VPN Opérateur, MPLS). Certaines contraintes doivent être prises en compte :

- Utiliser des ports de communications fixes et interdire l'utilisation de ports dynamiques. Cette restriction vaut pour toutes les communications entre toutes les parties constitutives du système,
- Indiquer exhaustivement les ports utilisés dans sa documentation,
- Les ports utilisés peuvent être éventuellement modifiables par le propriétaire,
- Eviter dans les transactions les protocoles propriétaires, qui seront systématiquement bloqués. Tous les flux devront être identifiés et, s'il y a lieu, documentés.

En particulier, la politique de filtrage réseau devrait limiter les flux des clients Web vers les serveurs aux ports standard 80 et 443.

6.2.9. Applications web et/ou accessibles depuis internet

Lorsque les fonctionnalités ou les modules mis en œuvre s'appuient sur des technologies WEB et plus particulièrement lorsqu'elle est accessible depuis Internet, les risques pesant sur la sécurité sont augmentés. Afin de les réduire, les règles de l'art et les recommandations habituelles en la matière devront être suivies. A ce titre, le titulaire devra se référer notamment aux documents suivants :

- Le guide OWASP Testing guide, téléchargeable sur le site OpenWeb Application Security Project (http://www.owasp.org/index.php/Category:OWASP_Testing_Project), ou à celui dédié au développement (http://www.owasp.org/index.php/Category:OWASP_Guide_Project).
- Les recommandations de l'ANSSI sur la sécurisation des flux HTTPS (Recommandations de sécurité concernant l'analyse des flux HTTPS – N°DAT-NT-19/ANSSI/SDE/NP) et la sécurisation des sites web (Recommandations pour la sécurisation des sites web – N° DAT-NT-009/ANSSI/SDE/NP)

Sécurisation de la session utilisateur

Les sessions utilisateurs sont des espaces de travail dans le temps utilisant un espace de stockage d'informations. Cet espace de travail est privé et lié à un utilisateur particulier. Afin de garantir la sécurité de l'emploi de ces sessions utilisateurs, un certain nombre de précautions sont indispensables de la part du développeur de l'application web. Il se doit ainsi de respecter les bonnes pratiques sur le sujet.

L'utilisation du protocole HTTPS au lieu de HTTP permet de se prémunir contre une écoute du trafic entre le client et le serveur. Ainsi, tout espace privé doit être protégé par le protocole HTTPS. Si toutefois cette précaution est trop pénalisante en terme de performance du serveur, il faut s'assurer que au minimum les cookies soient échangés en SSL afin d'assurer la confidentialité de leurs contenus et d'éviter toute interception par écoute du trafic. Les cookies de session doivent donc toujours être définis avec les attributs Secure et http-only.

La valeur saisie dans le champ mot de passe du formulaire ne doit pas être visible des personnes environnantes. Il est donc nécessaire d'utiliser le type d'input password plutôt que text. Le mot de passe ne doit pas non plus être pré-remplissable par le navigateur. Les développeurs doivent donc utiliser l'attribut autocomplete à off.

Tous les paramètres fournis par l'utilisateur ou obtenus par l'URL doivent être systématiquement contrôlés et les paramètres interdits expurgés. Les messages d'erreurs ne doivent pas afficher le détail des fonctions employées, ni leurs valeurs ou les requêtes adressées aux bases de données. Aucune information relatives aux droits d'accès d'un utilisateur ne doit être passée en paramètre à l'URL, afin d'éviter une modification frauduleuse de ces paramètres par l'utilisateur dans le but d'accroître son niveau d'habilitation.

Recommandations

- Filtrer les entrées utilisateurs.
- Interdire la consultation des répertoires présents sur le site Web en définissant une page par défaut.
- Prévoir des pages d'erreurs personnalisés afin d'éviter d'afficher les pages bannières.
- Mettre en place le paramètre autocomplete=off sur tous les formulaires contenant un mot de passe.
- Mettre en place un mécanisme de challenge-response pour l'authentification des utilisateurs.
- Ajouter les attributs HttpOnly et Secure aux cookies de session.

6.2.10. Navigateurs Internet

Afin d'optimiser la gestion de la sécurité des navigateurs Internet (Internet Explorer, Firefox,…), il est préféré d'éviter des technologies discriminantes (ActiveX, Applets Java, ASP, Flash,...). Si toutefois ces technologies sont utilisées, leur paramétrage, et/ou leur développement, seront effectués selon les recommandations de sécurité des concepteurs (Microsoft, SUN,…) de celles-ci ou d'un organisme de sécurité comme le CERTA par exemple. Le code développé pourra être signé par un certificat à des fins de contrôle de non modification dans le temps.

Il est rappelé que le navigateur privilégié au sein du département de l'Essonne est IE version 10. Le titulaire rendra compatible sa solution lors de toute montée de version des navigateurs et communiquera à la collectivité ses tests de non régression. Toutes les modifications induites par les montées de version devront restées compatibles avec la ou les versions antérieures des navigateurs retenus par la collectivité.

6.2.11. Journaux d'événements, traçabilité et conservation des logs

La solution doit intégrer le traçage de toutes les opérations effectuées (nature de l'opération, utilisateur, valeur de la donnée, date et heure). Ces logs devront être facilement exploitables pour permettre une recherche efficace des informations.

Le titulaire doit garantir la conservation et l'archivage des traces d'accès aux progiciels et des traces d'accès des flux échangés, en accord avec les exigences de conformité avec les réglementations et lois en vigueur.

6.2.12. Niveau de sécurité

Conformément au référentiel de sécurité (RGS V2.0), le Conseil départemental de l'Essonne doit décider du niveau de sécurité à mettre en œuvre après avoir effectué une analyse de risques (voir tableau ci-dessous). Cette analyse permet de définir le niveau de sécurité choisi parmi les trois niveaux de sécurité (élémentaire *, standard ** ou renforcé ***)

Critères	Niveau de sécurité
Fiche courrier	Standard **

Fiche contact	Standard **
Interfaces SI département de l'Essonne	Standard **

Afin de respecter la démarche d'amélioration continue de la sécurité initiée au sein du département de l'Essonne, les différentes étapes du management du risque lié à ce projet devront être revues régulièrement. L'avancement puis le suivi du projet permettront de mieux caractériser les actifs à protéger, d'identifier les menaces et vulnérabilités s'y appliquant afin d'estimer chaque risque sous forme d'impact et de probabilité d'occurrence.

L'évaluation du risque incombe au département de l'Essonne. Elle doit lui permettre d'identifier à tout moment les risques liés au projet. Le département peut les accepter en l'état ou souhaiter les réduire en mettant en œuvre des mesures de sécurité ou en améliorant celles existantes.

La mise en œuvre de nouvelles mesures de sécurité pourra faire l'objet d'un bon de commande sur la base d'un devis définis aux tarifs de prestations du bordereau des prix.

7. EXIGENCES DU DEPARTEMENT

7.1. Les environnements de qualification, de formation et de production

Les progiciels livrés par l'éditeur sont intégrés, industrialisés, testés et validés dans un environnement de qualification par les équipes en charge du projet. Lors des tests de qualification de l'application et pour des modifications majeures, la DSI réalisera un audit réseau pour s'assurer du bon fonctionnement protocolaire et du comportement des machines impliquées. La collectivité s'assurera également qu'il n'y a aucun flux parasite ou mal implémenté.

Lorsque la recette est effectuée, le progiciel est déployé dans un environnement de production et dans un environnement de formation.

Cette démarche impose une gestion de ces environnements :

- plusieurs installations,
- des procédures de passage d'un environnement vers un autre (rechargement de base, initialisation de paramètres).

Dans le cadre de nouveau modules ou nouvelles fonctionnalités, l'installation dans l'environnement de qualification est à la charge du titulaire accompagnée d'un transfert de compétences vers l'équipe informatique.

L'installation dans les environnements de formation et de production est effectuée par la DSI : afin de faciliter le passage d'un environnement à l'autre, il est demandé au titulaire de fournir des procédures de transfert total ou partiel des paramètres et des tables de référence de l'environnement de qualification vers celui de production ou de formation.

7.2. Le déploiement

Pour tous les logiciels (applicatifs et utilitaires) proposés à installer, le titulaire précisera les versions et tout particulièrement les prérequis nécessaires au fonctionnement des produits.

Pour chacun des logiciels applicatifs le prestataire fournira un guide et une procédure automatique ou sinon manuelle en cas de soucis. Chacune des procédures sera documentée.

L'installation du logiciel métier sera réalisée sur un serveur et un poste de référence unique et/ou des serveurs et postes selon l'architecture proposée. Les équipes de la DSI prendront en charge le déploiement, réaliseront la télédistribution à partir de cette référence à l'aide des outils adéquats.
Avant toute livraison d'une nouvelle version, le titulaire devra s'assurer que celle-ci n'engendrera aucune régression fonctionnelle ou technique dans les environnements du département. Le département pourra le cas échéant demander au titulaire de fournir son cahier de recette s'il constate une régression au niveau de sa qualification.

7.3. Installations et paramétrages

7.3.1. Installations et paramétrages

Cette prestation est réalisée en deux temps

Tout d'abord, le titulaire identifie et fournit les licences applicatives de la solution ainsi que de l'ensemble des éléments logiciels nécessaires à son fonctionnement puis, procède à l'installation des applications dans l'environnement de qualification. La procédure d'installation est documentée afin de permettre des réinstallations ultérieures dont, entre autres, la livraison de nouvelles versions de la solution.

Après recette du système par le titulaire et la collectivité, les applications sont installées dans l'environnement de production par la DSI, avec l'assistance du titulaire.

Puis, le titulaire finalise avec les utilisateurs les spécifications liées à l'usage des applications. Il rédige le cahier de paramétrage qui synthétise les choix faits et les caractéristiques des paramètres à définir dans les applications. Dans la mesure du possible, le titulaire propose un mécanisme d'initialisation ou de configuration automatique de ces paramètres. Il procède aux paramétrages avec transfert de compétences vers les équipes de la DRM et de la DSI en charge du projet.

7.3.2. Livraison et installation

Le titulaire devra identifier et fournir les licences applicatives de sa solution ainsi que l'ensemble des éléments logiciels nécessaire à son fonctionnement. Le titulaire procède à l'installation des applications dans l'environnement de validation. La procédure d'installation est documentée (voir § documentation à fournir) afin de permettre des Installations ultérieures, des changements de version et la mise en œuvre de l'environnement de production par les équipes de la DSI.

7.3.3. Spécifications du paramétrage

La prestation consiste à spécifier les fonctions attendues de la solution sur la base du CCTP. Cette étude doit permettre de rédiger un dossier de paramétrage de la solution à mettre en œuvre pour une entité. Le titulaire doit réaliser les prestations suivantes :

- effectuer une prise de connaissance préalable du contexte du projet
- formaliser les fonctions sous la forme d'un dossier de paramétrage faisant clairement apparaitre les fonctions déjà développées et les personnalisations nécessaires afin de répondre aux exigences du CCTP Le titulaire aura une mission d'analyse et d'assistance à l'expression des besoins en vue de l'écriture du dossier de paramétrage. Cette expression des besoins peut s'effectuer sous la forme d'ateliers organisés avec les chefs de projets ou experts métiers.

7.3.4. Paramétrages

Le titulaire doit effectuer le paramétrage de la solution en environnement de validation et définir les scénarios de test du système afin d'établir la démonstration du bon fonctionnement du système. Le dossier de paramétrage finalisé est remis aux administrateurs fonctionnels et techniques. Le titulaire fournit la procédure de bascule du paramétrage validé en environnement de production.

7.4. Développements – Intégrations

Le titulaire fournit sa méthodologie de développement et d'intégration de logiciel pour tout ce qui a trait aux développements spécifiques ou à l'intégration avec des logiciels existants.

Il réalise les développements des fonctions qui ne sont actuellement par couvertes par les solutions qu'il propose.

Il intègre sa solution dans l'environnement technique du Conseil départemental en respectant les exigences qui ont été définies.

7.5. Aide au démarrage

Une assistance sur site pourra être demandée lors du démarrage de chaque direction. Cette assistance nécessitera la présence du prestataire sur le site central du département (EVRY) ou sur les sites distants (répartis sur le territoire essonnien).

7.6. Fourniture de modules ou évolutions

7.6.1. Modalités

Des modules supplémentaires du (des) progiciel(s) ou des développements spécifiques pourront être acquis dans le cadre du présent marché sur la base du bordereau des prix et/ou du catalogue des prix.

Qu'il s'agisse d'extension du périmètre fonctionnel ou de migration technique de modules existants, la mise en œuvre de tout nouveau module devra être traitée en mode « projet » sur la base d'un cahier des charges techniques et/ou fonctionnelles chiffré dans un devis.

Le devis fourni par le titulaire précisera le cas échéant :

- les fonctionnalités,
- les interfaces,
- les procédures de traitement,
- les éditions,
- les livrables,
- le modèle de données cible,
- les modalités de la gestion de projet,
- le planning de mise en œuvre : livraison, installation technique, vérifications,
- les modalités de vérification,
- les transferts de compétence technique,
- à titre indicatif, les formations utilisateurs qui ne sont pas intégrées au présent marché,
- les contraintes et risques associés,
- le coût,
- les frais annuels de maintenance,
- les délais associés,

ou tout autre élément indispensable à la prise de décision de la personne publique pour engager l'évolution.

7.7. Garantie de bon fonctionnement

Le titulaire est tenu à une obligation de résultats sur le fonctionnement de la solution pendant toute la durée du marché. Cette garantie porte sur le service fourni, les logiciels, et toutes les prestations associées (études, développements, intégration, mise en œuvre), tels que décrits dans ce cahier des charges.

La garantie engage le titulaire à remédier gracieusement à tout vice de fonctionnement provenant d'une mauvaise conception ou réalisation du logiciel.

7.7.1. Performance de l'application

La mesure de performance est le temps d'affichage exigé selon la nature de la page à afficher. La solution doit supporter jusqu'à 120 connexions simultanées sans dégradation des performances.

Les temps de réponse sont évalués lors de l'étape de test en environnement de développement isolé afin qu'il n'ait aucune interférence. Ils ont pour objet d'évaluer la capacité de la solution à résister à une montée en charge proche des conditions de production. Le titulaire fournit les moyens de vérifier les mesures de ces temps de réponse (log ou autre système). Les scénarios de tests des interfaces Web seront impérativement automatisés via un outil libre au choix du titulaire.

Le Conseil départemental prêtera une attention particulière à la performance mesurée pour les pages suivantes :

Fonctionnalités	temps maximum en seconde
Accès page d'accueil	1
Authentification	1
Recherche mots clés	2
Afficher le fiche courrier	1
Administrateurs	**temps maximum en seconde**
Recherche simple (2 critères) avec environ 100 lignes de résultat (affichage 1er page)	2
Recherche Complexe (5 critères) avec environ 100 lignes de résultat (affichage 1er page)	3
Validation d'une saisie	2
Affichage de l'arborescence	2
Déploiement d'une arborescence	1
Supprimer un objet	2

Utilisateurs	Temps maximum en seconde
Afficher la page d'accueil (non authentifié)	1
S'authentifier et afficher la page d'accueil	3
Revenir sur la page d'accueil	1
Afficher une page intermédiaire	2
Afficher une page rédactionnelle	2
Recherche	2
Affichage du plan de l'arborescence	2
Déploiement d'une arborescence	2

Un protocole avec étalon de mesure adapté à la plateforme du CD91 et des outils de tests seront fournis par le titulaire pour s'assurer du bon fonctionnement des composants. Si ces temps de réponse se sont subitement dégradés après la mise à jour d'un composant, un test dans la version antérieure sera réalisé.

7.8. Convention de service entre les parties

Les prestations de maintenance et d'assistance portent sur l'application en environnement de production installée ou configurée par la DSI sur les recommandations du titulaire.

7.8.1. Accès aux ressources

L'accès distant aux ressources s'effectue en conformité avec les règles de sécurité définies par la DSI.
Le titulaire pourra disposer après accord de la DSI à minima d'un environnement de qualification pour réaliser les tests ou contrôles nécessaires.

Il pourra demander à la DSI de dupliquer l'environnement de production dans l'un de ces environnements pour mener à bien ses opérations de tests ou de contrôle.

7.8.2. Travaux d'administration de supervision et d'exploitation

Certains travaux courants pourront être assurés par la collectivité après avoir défini en commun les procédures et les profils des exploitants.

Il appartient au titulaire de définir les comptes et profils des exploitants de la collectivité afin de délimiter leur intervention aux seuls travaux définis.

Les travaux assurés par la collectivité sur l'environnement de production seront les suivants :

- Les sauvegardes des plateformes,
- L'administration de la base de données,
- Les exports logiques des bases de données,
- Les lancements de traitements différés (batchs) définis par le titulaire,
- La supervision de la plateforme sur la base d'indicateurs définis par le titulaire,
- L'administration du logiciel (au sens technique et fonctionnel).

7.8.3. Identification des responsabilités

En cas d'indisponibilité partielle ou totale du périmètre fonctionnel de l'application, un diagnostic préalable sera réalisé par la collectivité afin d'exclure toute cause exogène.

Elle sera enrichie sur la base des procédures et délégations confiées par le titulaire à la collectivité.

Temps de réponse non conforme au CCTP

Pour retirer l'hypothèse d'un engorgement du réseau LAN ou WAN les accès à la solution seront réalisées à partir des mêmes postes de travail.

Un monitoring du réseau LAN et WAN sera réalisé par la collectivité si les tests en environnement dédié (serveurs, postes de travail sur un réseau non partagé) ont révélé des temps de réponses non conformes.

Si ces temps de réponse se sont subitement dégradés après la mise à jour d'un composant, un test dans la version antérieure sera réalisé.

Accès au logiciel ou un module impossible

Vérification par la collectivité de la bonne activation des services. Application éventuelle de procédures d'arrêt/redémarrage définis par le titulaire.

Dysfonctionnement applicatif

Vérification par la collectivité de la bonne activation des services. Si ces dysfonctionnements surviennent après la mise à jour d'un composant, un test dans la version antérieure sera réalisé.

7.9. Maintenances et support

7.9.1. Maintenance évolutive

La maintenance évolutive concerne les améliorations des fonctionnalités existantes des progiciels. La maintenance évolutive porte également sur toute évolution induite par des montées de version ou des changements de système d'exploitation et des logiciels de base.

On peut distinguer les versions mineures et les versions majeures.

Une version mineure n'a pas de conséquences sur le fonctionnement quotidien des progiciels et des utilisateurs. La personne publique doit être informée de la mise en œuvre de cette version mineure au moins **cinq (5) jours ouvrés** à l'avance.

Une version majeure est une version qui peut avoir un impact important sur le système d'information et sur l'utilisation technique et fonctionnelle des solutions. La personne publique doit être informée de la mise en œuvre de cette version **majeure trente jours (30)** calendaires à l'avance.

Lors d'une montée de version, le titulaire s'engage à prendre en compte et ne pas remettre en cause les paramétrages réalisés par et / ou pour le Conseil général de l'Essonne.

Les mises à jour sont accompagnées de leurs procédures d'installation ainsi que de la description détaillée de leur contenu et des impacts sur les procédures d'exploitation

Dans le cadre de la maintenance évolutive le titulaire s'engage à livrer et à mettre en œuvre la totalité des versions majeures et mineures du progiciel acceptées par la personne publique et ce, durant toute la durée du marché.

Dans le cadre de la maintenance évolutive le titulaire s'engage à livrer la totalité des versions majeures et mineures du progiciel acceptées par la personne publique et ce, durant toute la durée du marché. Les prestations de mise en œuvre et de paramétrage des versions majeures feront l'objet d'une prestation spécifique chiffrée au bordereau des prix.

Le département se réserve le droit de refuser l'installation d'une version s'il juge que les nouvelles fonctionnalités apportées par cette dernière n'offrent aucune plus-value à son activité ou à ses agents. Dans ce cas précis, et si le titulaire indique que cette montée de version est nécessaire pour installer les versions futures (non rétroactivité des versions), le titulaire prendra à sa charge, sur site, les installations, le paramétrage de la nouvelle version et des postes utilisateurs le cas échéant ainsi que l'accompagnement des utilisateurs dans la prise en main de cette dernière.

7.9.2. Maintenance réglementaire

La maintenance réglementaire concerne la prise en compte de l'évolution de la législation (maintenance règlementaire du logiciel). Pour ce dernier pan, il est entendu que ladite maintenance est adossée à la notion de périmètre constant, technique et fonctionnel.

Dans le cas de modifications liées à l'évolution dues à la législation, le titulaire s'engage, après validation de la modalité de prise en compte avec la personne publique, à les réaliser dans les **trois mois (3) au maximum** qui suivent la publication législative.

7.9.3. Maintenance corrective

Par maintenance corrective, il faut entendre la prise en compte des modifications ayant pour effet de corriger des anomalies de fonctionnement constatées par la personne publique ou par le titulaire sur les fonctionnalités existantes.

Dans le cadre de la mise en place d'un nouveau développement ou module, la gestion des anomalies devra reposer sur des procédures de traitement simples et rapides. En cas d'incident ou de panne, le prestataire devra, après constatation ou signalement, effectuer un diagnostic et les interventions techniques nécessaires au rétablissement du service dans les délais prévus.

L'identification de la nature de l'anomalie se fait après contact téléphonique auprès du support (confirmé par email) ou par email entre le correspondant informatique du département et le support du titulaire. Il appartient aux administrateurs techniques et fonctionnels du département de l'Essonne de classifier l'anomalie en bloquante ou non bloquante (voir ci-dessous).

Le titulaire s'engage à tout mettre en œuvre pour régler dans les délais prévus les problèmes mettant en cause l'utilisation normale du logiciel.

Ces anomalies peuvent être de deux natures :

L'Anomalie bloquante : c'est une anomalie qui rend indisponible le progiciel du fait de l'impossibilité de son utilisation ou de celle d'une fonctionnalité jugée critique pour la collectivité, incluant les modèles de documents, à l'exclusion des documents bureautiques générés, qui peuvent faire l'objet d'altérations hors de l'utilisation du progiciel. Sa correction nécessite une intervention prioritaire du titulaire.

En cas d'anomalie considérée comme bloquante par la personne publique, le titulaire dispose d'un délai **d'une (1) heure ouvrée** en termes de garantie de temps d'intervention (GTI) et d'une garantie de rétablissement (GTR) de **quatre (4) heures ouvrées** pour la résorber.

Le délai est calculé sur les jours ouvrés (§5.6.4 ci-dessous) à partir de l'heure de réception du signalement écrit de l'anomalie, et jusqu'au déblocage ou à la fourniture d'une solution de contournement par le titulaire, cette dernière étant préalablement validée par la personne publique.

Lorsque le titulaire met en place une solution de contournement, en accord avec la personne publique, l'anomalie bloquante se transforme en anomalie non bloquante avec les délais de rétablissement assortis.

L'Anomalie non bloquante ou mineure : c'est une anomalie qui ne rentre pas dans la catégorie « bloquante ». Sa correction peut être priorisée, toute anomalie mineure de fonctionnement

permettant l'utilisation complète des progiciels dans l'ensemble de leurs fonctionnalités, même si celle-ci se fait au moyen d'une procédure de contournement.

En cas d'anomalie considérée comme non bloquante par la personne publique, le titulaire dispose d'un délai de **quatre (4) heures ouvrées en termes de garantie de temps d'intervention (GTI)** et d'une **garantie de rétablissement (GTR)** de **quatre (4) jours** ouvrés.

Dans tous les cas, le titulaire s'engage à fournir à la DSI au département un rapport détaillé sur les anomalies et les correctifs appliqués dans les mêmes délais.

Toute modification de la qualification apportée par le titulaire à la qualification établie par la personne publique, devra obligatoirement faire l'objet d'une information auprès de la personne publique dans le délai le plus bref. Les motifs de la requalification seront clairement exposés. En cas de désaccord, l'interprétation de la personne publique sera retenue.

7.9.4. Le support

Ce support pourra être sollicité pour des problèmes d'incident (anomalie, panne), pour du conseil ou encore pour une assistance à la mise à niveau de versions progicielles (patch) et de l'assistance dans les procédures d'installation.

Ce service proposera un système d'enregistrement d'incident avec horodatage permettant la traçabilité des ouvertures d'incident par la personne publique. Le titulaire proposera également un dispositif d'historisation des tickets d'incidents ouverts et clôturés. La personne publique pourra demander la réouverture d'un incident clôturé lorsque l'anomalie corrigée réapparaîtra.

L'accueil téléphonique est réservé à un interlocuteur unique (par progiciel) désigné par la personne publique et ayant suivi les sessions de formation 'administrateur' et 'gestionnaire' pour le progiciel ; ce service d'accueil téléphonique est assuré, sauf les jours de fête, du **lundi au vendredi de 8h00 à 12h30 et de 14h00 à 17h30.**

L'appel est enregistré et une fiche décrivant la demande est renseignée. Le dossier est ensuite transmis à un technicien compétent et disponible qui rappelle au plus tôt et de toute façon dans la journée pour tout appel reçu avant 10h00. Un diagnostic est établi qui conduit soit à la solution du problème, soit à la poursuite des investigations, soit à la mise en évidence d'une anomalie ; dans ce cas un scénario de contournement peut être proposé dans l'attente de sa correction prévue dans le cadre de la maintenance.

Si ces horaires devaient être ponctuellement modifiés en raison de situations exceptionnelles, le titulaire en informera la personne publique au plus tard un (1) mois avant la date concernée.

De même, dans le cas d'une intervention exceptionnelle mais programmée nécessitant l'assistance téléphonique du titulaire en dehors des plages horaires indiquées, la personne publique en formulera la demande dans un délai nécessaire et suffisant pour organiser l'intervention, et l'inclura dans le bon de commande correspondant.

Les prestations ne sont pas assurées pendant les jours fériés, ni les week-ends.

7.10. Télémaintenance

En cas de besoin, une télémaintenance pourra être déclenchée d'un commun accord avec la personne publique, suivant une procédure préalablement transmise par le titulaire et validée par le Département. Cette procédure devra respecter des règles de sécurité en vigueur, formalisées dans le document annexé décrivant le protocole d'intervention des sociétés extérieures (Annexe 1); qui explicite les règles à respecter lors d'actions de télémaintenance ainsi que les conditions d'usage de cette infrastructure et en particulier l'accès du titulaire sera restreint à l'équipement concerné par l'intervention

Le Département de l'Essonne dispose d'une plateforme d'accès sécurisé WALLIX AdminBastion pouvant être utilisée pour la télémaintenance. Un accès nominatif adapté aux besoins du titulaire peut y être défini afin d'offrir les accès nécessaires aux différentes actions de télémaintenance.

Si le titulaire souhaite disposer de ses propres moyens pour assurer le service de télémaintenance, ceux-ci garantiront la sécurité du flux de données en assurant un canal chiffré (168 bits minimum) entre le poste de télémaintenance du titulaire et le système d'information du Département de l'Essonne. Ces moyens devront requérir une autorisation explicite de la part de la personne compétente du Département de l'Essonne afin d'accéder au service demandé à un instant donné.

Dans le cas contraire le Département se réserve le droit d'imposer les moyens nécessaires afin de garantir la sécurité d'accès à son système d'information.

7.11. Maintenance sur le site de la personne publique

En cas de non résolution des problèmes signalés, ou d'impossibilité de résolution soit par la maintenance téléphonique soit par télémaintenance la personne publique pourra faire appel à une maintenance sur le site. Ces interventions sont prévues dans le catalogue spécifique des prix du marché. Ces intervention s'effectuent à l'intérieur d'une plage horaire du lundi au vendredi de 09h00 à 18h00, sauf jours fériés.

Dans ce cas, la personne publique et le titulaire s'entendront au préalable et décideront d'un commun accord des modalités techniques et financières et des conditions de l'intervention.

7.12. Evolution du périmètre de maintenance

En cas d'acquisition de nouveaux modules, le périmètre de la maintenance pourra évoluer par le biais d'un bon de commande aux tarifs prévus au bordereau des prix.

7.13. Le périmètre du SI sous la responsabilité du titulaire

Périmètre fonctionnel

Il intègre les progiciels installés, configurés ou gérés par le titulaire ou l'un de ses sous-traitants ainsi que leurs évolutions.

L'application comprend :

- le cœur du logiciel et de ses évolutions (*),
- ses modules complémentaires liés à la solution de base (modules, composants, plug-in) et de ses évolutions (*),
- les connecteurs, interfaces ou API développés ou qualifiés par le titulaire interagissant entre le cœur du logiciel et ses modules complémentaires,
- les portlets, servlets ou applets développés ou qualifiés par le titulaire interagissant entre le cœur du logiciel et ses modules complémentaires.

(*) Mise à disposition par la communauté ou développés par le titulaire dans le cadre de ce marché

Il exclut :

- les applications métiers pouvant communiquer avec l'application du présent marché définie dans son périmètre fonctionnelle,
- les connecteurs, interfaces ou API non développées ou non qualifiées par le titulaire,
- les portlets, servlets ou applets non développés ou non qualifiés par le titulaire.

Périmètre technique

Le titulaire assure la maintenance de tous les composants techniques nécessaires au bon fonctionnement de l'application et des composants rentrant dans le périmètre fonctionnel. Il intègre notamment :

- Les bases de données et middleware,
- Les serveurs d'applications, serveurs web ou frontaux le cas échéant,
- Les composants du périmètre fonctionnel,
- Les outils d'administration ou de monitoring de l'application,

Il exclut les outils installés par la collectivité :

- Les outils de sauvegarde de la collectivité (Tina de Time Navigator),
- Les sondes de supervision installées par la collectivité,
- Les solutions antivirales,

- L'environnement de virtualisation VMware,
- Le firmware des serveurs,
- Le système d'exploitation des serveurs

7.14. Documentation

Dans le cadre de chaque nouvelle évolution (acquisition, développement ou maintenance évolutive), le titulaire mettra à jour la documentation de référence.

La documentation comprendra, notamment :

- Documentation technique pour les administrateurs et le support de premier niveau
- Documentation technique d'installation des fonctions serveurs
- Documentation d'exploitation (cas général et éléments propres au CD91)
- Documentation technique d'installation des postes utilisateurs et notamment les prérequis techniques
- Documentation fonctionnelle pour les différents utilisateurs (guide d'utilisation précis de la plate-forme avec copie des écrans)
- Manuels de maintenance
- La documentation représentant le modèle de données
- La documentation d'architecture fonctionnelle comprenant la modélisation
- La documentation d'architecture technique propre au CD (rédigée en collaboration avec les équipes techniques de la DSI)
- La documentation des processus métiers et un découpage en couches métier et fonctionnelle

Cette documentation sera rédigée en français.

Elle pourra être reprographiée par la personne publique avec mention du nom du titulaire, à l'attention de ses utilisateurs uniquement. Une version numérique modifiable devra donc être proposée par le titulaire.

En cas d'évolution de la solution, la documentation devra être mise à jour et transmise à la personne publique en même temps que la mise à disposition de la version en environnement de recette.

7.15. Arrêt de la maintenance par le titulaire

Si le titulaire prend la décision d'interrompre la maintenance de la version des progiciels actifs au département de l'Essonne, le titulaire en informe la personne publique par courrier recommandé au moins **dix-huit (18) mois** avant la date d'interruption. A défaut, au terme de son renouvellement, la maintenance pourra être reconduite à la demande de la personne publique pour une durée de **dix-huit (18) mois** minimum sans que le titulaire ne puisse s'y opposer dans la limite de la durée d'exécution du marché et de ses bons de commande.

8. AUTRES PRESTATIONS

8.1. Transfert de compétences et formations

Ces prestations de formation concernent tous les utilisateurs de la cellule courrier de la DRM, estimés à environ 10 personnes ainsi qu'aux agents de la DSI en charge du projet, estimés à 5, aux référents qui assureront les formations de tous les utilisateurs (estimés à 30). Elles sont fournies pendant toute la durée du marché et en particulier durant la période d'installation de la solution

8.1.1. Transfert de compétences

Les prestations de transfert de compétence concernent chaque élément fourni par le titulaire et se déroule lors de l'installation et du paramétrage de la solution. Ces prestations font partie intégrante des prestations de fourniture et ne pourront faire l'objet d'aucune facturation supplémentaire. Elles concerneront notamment :

- Passage des compétences sur l'environnement du produit à la DSI ;

- Passage de compétence aux chefs du projet informatique et utilisateur, sur la structure de l'application et de la base ;
- Passage de compétence aux chefs du projet informatique et utilisateur, sur la partie portail.

Le contenu du transfert de compétence sera défini par le titulaire en accord avec la personne publique, sur la base de la proposition remise par le titulaire. Ces transferts de compétence devront de par leur contenu permettre aux utilisateurs d'utiliser les fonctions avancées de la solution mise à leur disposition.

La documentation fournie dans le cadre de ces transferts de compétence comprendra, notamment :

- Documentation d'architecture technique
- Documentation technique d'installation et de paramétrage pour les administrateurs et le support de premier niveau
- Documentation d'exploitation

8.1.2. Formations

Le contenu et les modalités de la formation sont définis par le titulaire en accord avec la personne publique, sur la base de la proposition remise par le titulaire. Le forfait formation sur site correspond à une session de 10 personnes au maximum, il est récupérable au titre de la formation continue.

D'autres formations peuvent être demandées après le lancement du projet sur la base des tarifs prévus au bordereau des prix et/ou du catalogue. Un cahier des charges de la formation attendue sera envoyé au titulaire qui devra présenter dans un délai de **trois (3) semaines** au maximum à partir de la date d'envoi de ce dernier, un contenu de formation. Celui-ci devra être validé par la personne publique pour être applicable.

La documentation fournie dans le cadre de ces formations comprend, notamment :

- Documentation technique pour les administrateurs et le support de premier niveau
- Documentation fonctionnelle pour les différents utilisateurs (guide d'utilisation de la solution).

Cette documentation doit être fournie à chaque stagiaire lors de la session de formation. La reprographie des documents est à la charge du titulaire.

Cette documentation pourra être reprographiée par la personne publique avec mention du nom du titulaire, à l'attention de ses utilisateurs uniquement.

La formation sera réalisée à partir d'une base de données de courriers fictifs fournie par le titulaire lors de mise en ordre de marche.

Organisation des formations

L'amplitude journalière est de 6 heures de face à face pédagogique à partir de 9 heures, hors pauses déjeuner et intermédiaires.

Les formations se déroulent au sein des locaux du Conseil départemental (au siège et/ou sur les sites du département) excepté les samedis, dimanches, jours fériés et jours de fermeture du Conseil départemental.

Obligations des parties

Le département s'engage à :

- Inscrire et convoquer les stagiaires,
- Transmettre la liste définitive des stagiaires et la feuille d'émargement au formateur au démarrage des sessions (dossier formateur),
- Fournir à chaque stagiaire une fiche d'évaluation de stage à remplir en fin de session dont une copie sera transmise au titulaire du marché s'il le demande,
- Fournir les salles de formation et le matériel nécessaire (tableau blanc, paperboard, papier, feutres, vidéo projecteur, postes de travail connectés au réseau),

Le titulaire s'engage à :

- Garantir la qualité des formateurs dont la compétence technique et fonctionnelle correspond à la formation et fournir les CV de chaque intervenant,

- Proposer un nouvel intervenant à la demande du service formation si la prestation effectuée par l'un de ceux-ci s'avère de qualité insuffisante en cours de session,
- Fournir des supports de cours ainsi que des exercices adaptés aux objectifs des stagiaires; tous les documents pédagogiques doivent être reprographiés pour chaque stagiaire aux frais du prestataire ; dans le cadre du développement durable, les matériaux recyclables ainsi que le recto verso seront privilégiés ; les supports papier sont envoyés au service formation au minimum 15 jours avant chaque séance de cours,
- Remettre en ordre les salles de formation du Conseil départemental à la fin du stage et signaler tout problème matériel,
- Participer à une rencontre avec le Service formation dès la notification du marché afin d'élaborer les modalités d'organisation ; participer aux réunions périodiques organisées par le Service Formation pour le suivi et l'évaluation du dispositif,
- Fournir les attestations de stage en 3 exemplaires, mentionnant la présence réelle des stagiaires, avec la facture

Calendrier définitif

Après notification du marché, un calendrier est établi entre le titulaire et la personne publique sur la base d'un accord commun. Le titulaire s'engage à mettre tous les moyens humains et matériels nécessaires aux besoins de formation du Conseil départemental en application du calendrier établi.

Le titulaire fournira par écrit des dates de sessions dans le délai maximal de trois semaines suivant la demande de la personne publique (par mail, télécopie). Celui-ci devra s'y tenir sous peine de résiliation de présent marché.

En cas de retard ou d'absence de transmission du calendrier dans le délai précité, les pénalités de l'article 6.5.e (Pénalités pour non remise de la documentation ou de devis ou de l'étude de faisabilité du CCAP) pourront être appliquées.

8.2. Assistances ou interventions supplémentaires

D'autres prestations pourront être assurées par le titulaire à titre de prestations supplémentaires et facturées en sus en appliquant le tarif visé au bordereau des prix.

Elles concernent notamment :

- Le développement de fonctions spécifiques. Le cas échéant, il fera l'objet d'un supplément de maintenance selon le pourcentage prévu au bordereau des prix.
- L'actualisation de la charte graphique,
- L'expertise technique ou fonctionnelle,
- La gestion de projet,
- La direction de mission,
- Le transfert de compétences vers les référents,
- Le paramétrage, l'assistance au paramétrage ou l'assistance à la demande de la personne publique.

8.3. Réversibilité

Le transfert de l'ensemble des éléments vers un autre titulaire sera réalisé s'il y a lieu au cours du dernier trimestre de chaque période d'exécution du présent marché ou en cas de résiliation du marché. Cette prestation fait l'objet d'un bon de commande spécifique qui en fixera le délai également.

Le titulaire s'engage à réaliser toutes les actions permettant au Département d'assurer la continuité de service. Cette continuité de service doit expressément être transparente pour les utilisateurs finaux, et n'occasionner aucune perte de données.

Dans ce cadre, le titulaire assure les actions suivantes :

- Assistance et conseil au pouvoir adjudicateur,

- Restitution de tous les documents appartenant au Département,
- Restitution d'une sauvegarde complète des données hébergées sur les serveurs,
- Identification de toutes les procédures et de tous les moyens techniques, juridiques et humains nécessaires à la continuité du service dans des conditions identiques,
- Transfert auprès du pouvoir adjudicateur ou de tout autre organisme mandaté par lui des connaissances nécessaires à la poursuite du service,
- Engagement de répondre sur une période de 6 mois à l'issue de la fin du marché (résilié ou expiré) à toute demande d'assistance ou de conseil formulée par le pouvoir adjudicateur.

Pendant la phase de réversibilité, le titulaire assure le service dans les conditions prévues dans le présent marché. L'organisation concernant cette réversibilité est décrite dans l'Artiche 14 – Réversibilité du AE/CCAP.

Outre les documents qui sont remis lors de l'exécution de chaque prestation, le titulaire doit remettre à son successeur l'ensemble de la documentation des applications :

- Modèle de données,
- Extraction ou fourniture des données (même cryptées).

9. DEROULEMENT DU MARCHE

Le titulaire organisera le déroulement du marché en accord avec la personne publique. Si elle est intégrée au projet d'évolution et prévue au devis et confirmée à la commande, la gestion de projet sera gérée comme décrit ci-dessous.

9.1. Equipe projet, instance de décision et réunions

9.1.1. Equipe projet

L'équipe projet assure la conduite du projet. Elle est pilotée par un directeur de projet MOA, cadre représentant la maîtrise d'ouvrage Métier, et est assistée par une assistance à maîtrise d'ouvrage.

Le principal contributeur est le chef de projet MOE, collaborateur de la Direction des Systèmes d'Information.

L'équipe projet est constituée de contributeurs permanents et ponctuels, comme par exemple des référents (experts) ou des grands témoins (acteur de la collectivité ayant mené un projet équivalent).

L'équipe projet est responsable du suivi des ressources, du planning, des objectifs, du reporting et participe aux phases de vérification contractuelles. Elle assure le respect du plan de management gestion de projet et du guide méthodologique des projets.

Le directeur de projet MOA et de son représentant, le chef de projet MOE et de son représentant seront désignés lors de la réunion de lancement. Il en sera de même avec l'équipe projet du titulaire.

9.1.2. Instance de décision – le comité de pilotage

Ce comité se réunira au lancement du marché et à chaque étape importante où une décision sera requise. Il est composé des personnes suivantes :

- Le directeur de la direction des systèmes d'information (DSI) ou son représentant
- Le directeur de la Direction des Ressources Mutualisées (DRM) ou son représentant en tant qu'également Directeur de projet MOA
- Le chef de projet MOE ou son représentant
- Le représentant de l'AMOA
- Un représentant du titulaire (directeur de projet)
- Et de tout expert désigné par les membres.

Le titulaire présentera lors de chaque comité de pilotage un calendrier du projet et un état d'avancement des prestations commandées.

9.1.3. Réunions de suivi fonctionnel et technique

Elles sont organisées sur le site du Département de l'Essonne ou par visioconférence. Le titulaire devra fournir au chef de projet et au responsable métier par mail :

Avant la réunion : l'ordre du jour

Après la réunion : le compte rendu de la réunion

9.1.4. Réunions de suivi contractuel

Une réunion de suivi contractuel sera programmée sur le site du département selon une fréquence définie lors de la réunion de lancement du marché. Le titulaire devra fournir :

Avant la réunion : l'ordre du jour

Après la réunion : le compte rendu de la réunion

9.2. Organisation

Les éléments pouvant être attendus avant chacune des réunions doivent être présentés par le titulaire pour validation au chef de projet concerné au moins **48 heures** avant la tenue de la réunion.

Les réunions de débriefing doivent avoir lieu sous un délai de **48 heures**.

Les éléments attendus après la réunion sont à livrer par le titulaire sous un délai maximal de **5 jours ouvrés** après chaque réunion.

Tous les livrables sont remis sur support informatique au format Microsoft Office Version 2010 à minima. Les cartographies ou processus reposant sur des outils tiers doivent disposer d'un viewer gratuit téléchargeable librement par le département.

Tous les livrables font l'objet d'une validation écrite du chef du projet, sous délai maximum de **10 jours ouvrés** après livraison des éléments.

Pour tous les documents transmis, le titulaire veille à la qualité rédactionnelle et à la lisibilité des livrables remis faute de quoi le département se réserve le droit d'appliquer les dispositions indiquées dans le CCAP en terme de pénalités (chapitre 6.5.e. Pénalités pour non remise de la documentation ou de devis u de l'étude de faisabilité).

Le département s'engage à transmettre tout document utile au titulaire.

9.2.1. Vérification et Admission des prestations (recettes)

L'organisation concernant cette vérification et l'admission des prestations est décrite dans l'article 7 – Opération de vérification/Admission du CCAP.

9.2.2. Processus d'évolution

Le processus est le suivant :

- Le département décide de lancer l'étude de faisabilité d'une demande,
- Le titulaire réalise une étude de faisabilité et de coût et transmet une proposition, dans un délai convenu avec le département de l'Essonne,

Sur la base de cette proposition (devis), le département décide :

- De donner suite et de passer commande de l'évolution,
- De modifier sa demande et de demander un nouveau devis,
- D'abandonner la demande,

Dès la commande réceptionnée :

- Le titulaire réalise les développements correspondants,
- En fonction du mode de fourniture du progiciel (licence ou hébergé), le titulaire ou le département de l'Essonne installe l'évolution sur le système de pré-production,
- Le département effectue la vérification d'aptitude de l'évolution,

- En fonction du mode de fourniture du progiciel (licence ou hébergé), le titulaire ou le département de l'Essonne installe l'évolution sur le système de production,
- Le département prononce la vérification de service régulier de l'évolution.

9.2.3. Processus de nouveau déploiement

Le processus est le suivant :

- La prestation d'un nouveau déploiement fait l'objet d'un bon de commande que le département passe auprès du titulaire,
- Le chef de projet du département, le responsable fonctionnel et le titulaire fixent au cours de la réunion de lancement un planning et les modalités de déploiement,
- Le titulaire et/ou le département de l'Essonne réalise les opérations nécessaires au déploiement,
- Le département effectue la vérification d'aptitude du déploiement,
- Le département prononce la vérification de service régulier du déploiement.

9.2.4. Niveau de service attendu dans la mise en œuvre des évolutions

Chaque évolution ou nouveau déploiement est géré en mode projet ; le chef de projet du département, le responsable fonctionnel et le titulaire conviennent d'un planning.

Le titulaire est ensuite tenu de respecter les délais des prestations dont il a la charge.

9.2.5. Les livrables attendus

Le tableau ci-dessous donne la liste des livrables en fonction des phases du projet :

Phase	Livrables
Cadrage du projet	- **Planning détaillé,** - **Intervenants du titulaire avec fonctions et rôles dans le déroulement du projet,** - **Estimation de la charge des intervenants du Conseil départemental,** - **Spécifications fonctionnelles détaillées,** - **Descriptif des fonctionnalités proposées, synopsis et scénarisation des écrans (maquettes…),** - **Spécifications techniques détaillées (architecture technique et logique, modélisations des flux entre modules, détails des interfaces ou connecteurs,** - **Dimensionnement de l'architecture technique matérielle, architecture,** - **Schéma d'alimentation des données et documents de validation,** - **Elaboration des plans de tests fonctionnels (scénarii de tests et résultats attendus sous forme de fiche de recette…),** - **Elaboration des plans de tests techniques (intégration avec le SI, gestion des habilitations, répondre au PCA/PRA, montée en charge…)**
Mise en ordre de marche	- **Licences (le cas échéant),** - **Documentation d'Installation et de paramétrages techniques du logiciel,** - **Documentation des architectures fonctionnelles et techniques,** - **Mise à jour Modèle physique des données,**

	- **Mise à jour Manuel d'exploitation,** - **Mise à jour Procédures d'arrêt/redémarrage de la solution,** - **Procédure permettant la modification de l'identifiant et du mot de passe des comptes associés au système d'exploitation et aux bases de données (paragraphe 2.4.4)** - **Procédure de déploiement sur environnement de validation (document de paramétrage fonctionnel complété avec les règles retenues),** - **Procédure de déploiement sur environnement de production (procédure de migration de la plateforme de qualification vers la plateforme de production : rechargement de base, initialisation de paramètres…)**
Vérification d'aptitude	- **Cahier de recette complété sur la base des fiches de recette définies lors de la phase 1 pour validation des paramétrages fonctionnels,** - **Cahier de recette complété sur la base du jeu de tests techniques et d'intégration (validation des éditions, des exports, des interfaces…),** - **Intégration de la charte graphique (logos, modèles courriers…),** - **Bilan installation et axes d'amélioration**
Vérification du service régulier	- **Rapport concernant la mesure des indicateurs**
Formation et déploiement	- **Supports de formations (administrateurs et utilisateurs),** - **Manuel utilisateur (administrateurs fonctionnels & utilisateurs)**

10. ANNEXES

10.1. ANNEXE 1 Protocole d'intervention des sociétés extérieures sur le SI du CD91

Ce protocole vise à fixer les règles que doivent respecter les acteurs de sociétés extérieures lorsqu'ils interviennent sur les systèmes informatiques du Conseil départemental.

Périmètre du protocole

Ce document fixe les conditions d'utilisation et de manipulation des éléments suivants :

Accès en interne au réseau du Conseil départemental
Accès depuis une connexion extérieur au réseau du Conseil départemental (télémaintenance)
Conditions d'utilisation de l'environnement de qualification
Accès et utilisation des bases de données en environnement de production
Accès et modifications des progiciels en environnement de production
Accès et modification des équipements réseau
Accès et modification des systèmes réseau
Intervention de maintenance et de déblocage applicatif

Accès en interne au réseau du Conseil départemental

Sécurité du poste de travail du titulaire

Le titulaire extérieur n'obtiendra l'autorisation de connecter provisoirement son matériel au réseau du Conseil départemental que si les éléments suivants sont remplis :

Présence sur la machine d'un antivirus à jour d'un éditeur reconnu
Présence sur la machine d'un pare-feu activé

Accès à Internet

Aucune authentification n'étant nécessaire pour utiliser les liens Internet, le titulaire s'engage à ne pas tenter de contourner les dispositifs de sécurité et de filtrage mis en place sur le réseau.

Accès au réseau

Si pour des raisons techniques un titulaire doit accéder à un des serveurs (Microsoft ou Novell) où est déployé sa solution au sein du réseau du Conseil départemental, une demande selon la procédure habituelle sera faite à l'initiative de la personne en charge du projet au sein de la DSI. Cette demande devra préciser la durée de validité du compte ainsi que les ressources réseau nécessaires (création d'un compte nominatif avec une date limite de validité obligatoire). Certains titulaires assurant une maintenance durable bénéficient d'un compte nominatif permanent.

En aucun cas un titulaire ne peut utiliser – même provisoirement – le compte d'un agent du département pour effectuer son intervention.

Accès depuis une connexion extérieure au réseau du département (télémaintenance)

Aucun accès en télémaintenance n'est possible pour un intervenant extérieur sans l'accord de l'ISIM ou du CPI en charge de l'application.

L'accès en télémaintenance aux applications et/ou serveurs du Conseil départemental sera possible à partir d'une plateforme de rebond sécurisée et au moyen d'une connexion VPN/SSL.

Cette connexion ne sera établie qu'après autorisation du Conseil départemental et qu'à partir de l'adresse publique du titulaire que ce dernier aura communiqué au préalable au Conseil départemental.

Tout accès par télémaintenance au réseau du Conseil départemental fera l'objet d'une consignation dans un fichier électronique par l'équipe Pupitre qui indiquera :

Le N° de la machine concernée,
Le nom de l'entreprise intervenant,
Le nom de l'intervenant,
L'heure de début et si possible l'heure de fin d'intervention de la société,
Le motif de l'intervention

Conditions d'utilisation de l'environnement de développement

De façon générale les intervenants extérieurs ayant à mettre en œuvre des installations ou des évolutions majeures d'une application ou d'une base de données effectueront toutes les manipulations dans l'environnement de développement.

Toute intervention ou basculement en environnement de production ne sera réalisé par l'intervenant extérieur que s'il est accompagné par les ISIMs, l'équipe réseau/système et/ou les DBA.

Les conditions d'accès à l'environnement de développement pour les intervenants extérieurs sont les mêmes que pour les accès en environnement de production :

Poste de travail protégé par un anti-virus à jour et un pare-feu
Compte et habilitations Novell et AD spécifiques
Compte et habilitations sur les bases de données spécifiques

Une fois l'intervention terminée, les différents comptes créés pour le titulaire seront désactivés ou le mot de passe modifié.

Accès et utilisation des bases de données en environnement de production

Toute intervention programmée sur une base de données de production pour modification du contenu ou modification structurelle doit faire l'objet d'une demande préalable à l'Ingénieur Système d'Information Métier (ISIM) et aux DBA.

Une sauvegarde des bases de données devra être réalisée avant toute modification.

Un programme d'intervention précis, relevant la nature des opérations à réaliser devra être remis aux responsables de l'application (ISIM + DBA) :

Nature de l'opération
Scripts réalisés
Tables modifiées ou impactées
Modifications de structure
Modification affectant les sauvegardes
Modifications affectant les traitements automatisés

A la fin de l'opération un compte-rendu reprenant et commentant les opérations réalisées devra être remis aux responsables de l'application (ISIM + DBA) avant le départ du titulaire du Conseil départemental.

Accès et modifications des progiciels en environnement de production

Les modifications programmées des progiciels sont effectuées par les intervenants extérieurs uniquement dans l'environnement de développement.

Toutes les modifications effectuées en environnement de production sont réalisées par les DBA et/ou l'équipe RESEAU à partir d'une procédure détaillée fournie par l'intervenant extérieur. Cette procédure doit contenir les éléments suivants :

Nature de l'opération
Procédure d'installation
Modifications de l'architecture du logiciel
Modifications des fichiers, des droits
Modification affectant les sauvegardes
Modifications affectant les traitements automatisés

Une sauvegarde complète de la machine de production impactée sera réalisée avant toute modification. Il en va de même pour les bases de données afférentes, si la modification de l'application entraîne une modification de la structure ou du contenu des bases.

L'équipe RESEAU/Système et/ou DBA doivent être informées des interventions programmées sur les machines en production afin de planifier les travaux de sauvegarde.

Intervention de maintenance et de déblocage applicatif

Les dispositions précédentes sont assouplies lors des opérations de maintenance et de corrections applicatives menées en urgence par un titulaire extérieur à la demande du Conseil départemental.

En effet, il est parfois impossible ou trop coûteux de reproduire une anomalie en environnement de développement, de la corriger et d'en reporter les résultats en environnement de développement.

En cas d'intervention pour corriger une anomalie, le titulaire n'obtiendra sur la machine et l'application que les habilitations nécessaires à son intervention, le temps de la correction.

Un rapport détaillé devra être remis par le titulaire au responsable de l'application concernant les points suivants :

Date et durée d'intervention
Nature de l'opération
Modifications apportées à la base de données
Corrections apportées à l'application

Les interventions pourront être menées à partir de la plateforme de rebond en télémaintenance ou lors d'une intervention physique du titulaire.

Pour toute intervention effectuée sur l'environnement de Production, il est impératif que celle-ci s'effectue sous la surveillance active d'un agent du Conseil départemental : CPI, ISIM, DBA, CPU.

10.2. ANNEXE 2 Versions usuelles et évolutions engagées

Qu'il s'agisse d'extension du périmètre fonctionnel ou de migration technique de modules existants, le titulaire devra prendre en compte les attendus techniques décrits ci-dessous.

D'une manière générale, le Conseil départemental a pour stratégie de suivre les évolutions techniques de ses partenaires (Oracle, Microsoft, …) et de développer les applications en mode web afin de répondre aux besoins de mobilité et de télétravail.

Les postes de travail

Les postes de travail sont des micro-ordinateurs dont la configuration minimale est AMD SEMPRON 2700 Mhz, 128Go de disque dur et 4 Go de mémoire centrale.

Os	**Version actuelle**	**Version engagée**
Système d'exploitation	Windows 7 Pro 64 Bits	
Service Pack	1	
Mises à jour Microsoft	Réactualisées via WSUS (Pas en fonction)	
Logiciels (Socle de base)	**Version actuelle**	**Version engagée**
Réseau	Client Microsoft Natif (AD)	
	Agent ZENworks v11.2.3 MU1 et SCCM	
Bureautique	Microsoft Office 2010 32 Bits (Word, Excel, PowerPoint, Outlook)	
	PDFCreator v1.7.0	
Client Messagerie externe	OWA	
Lecteur PDF	Acrobat Reader 11	
Internet	Internet Explorer 10	
Utilitaires	7Zip v9.20	
	Agent OCS v2.1.1.1	
	Agent VUEM v3.0	
Multimédia	Windows Media player 12	
Sécurité	Agent McAfee v4.8	Migration 5.0.2
Antivirus McAfee VirusScan	McAfee VirusScan 8.8	Agent McAfee v4.8 ➔ v5.0.2 qui récupère l'antivirus McAfee VirusScan 8.8 ou supérieur)
Pare-feu HIP McAfee	McAfee HIP 8.0	Station : Windows 7 / portable HIP

Les SGBDR

Les serveurs WEB seront installés sur des machines virtuelles utilisant la technologie VMWARE.

Les serveurs Web installés sont :

Systèmes gestion bases de données	Version actuelle	Version engagée
PostgreSQL sous Linux CENTOS	8.4.8	9.4
MySQL	5.5	5.7
Oracle sous Windows en version serveur standard (et non entreprise),	Edition Version 11.2.0.3 en 64 bit sur serveur Windows 2008 64 Bit	Edition Version 12C 64 bits sur serveur Windows 2012
SQL server	2005	2012

Les protocoles et logiciels systèmes

Les standards définis par la DSI sont :

Protocoles et logiciels système	Version actuelle	Version engagée
ODBC Oracle sur poste de travail	Oracle 11.2.0.4 (32 bits)	
Pour la couche de communication et d'accès aux bases de données Oracle,	Oracle 11.2.0.4 (32 bits)	
Client réseau	Client Microsoft natif (AD) seven 64 bits ou supérieur	
ADO (interface standard Microsoft d'accès aux données),		
Annuaire	Active Directory 2012 R2	
DNS	Microsoft 2012 R2	
AD et DNS MICROSOFT (serveur 2012 R2).		
ASP pour le traitement et l'exécution des applications Intranet.		
PEERLINK	3.5.1.1015	

Les serveurs Web

Les serveurs Web installés sont :

Serveurs web	Version actuelle	Version engagée
IIS pour la gestion des transferts de documents HYPERTEXT selon le protocole HTTP	7 et 7.5	**8.5 (sous W2012R2)**

Pour le mode sécurisé SSL	V3 minimum	
APACHE	2.2	2.4
Tomcat	6	7
JBOSS		

Les communications entre le client et le serveur WWW devront s'effectuer en mode sécurisé : HTTPS

Les systèmes d'exploitation et annuaire

Les serveurs systèmes seront installés sur des machines virtuelles utilisant la technologie VMWARE.

Les standards actuels définis par la DSI sont :

Systèmes d'exploitation et annuaire	Version actuelle	Évolution engagée
Windows serveur Standard • pour les serveurs hébergeant les bases de données Oracle, • pour les serveurs d'accueil WEB ou TSE	Windows 2012 R2 64 bits	
Linux CentOS pour des serveurs applicatifs et de bases de données PostgreSQL et pour les serveurs d'applications WEB	CentOS 6.6.5	CentOS 7.x
Windows pour les serveurs de taille moyenne hébergeant les applications ou la bureautique	Windows 2012 R2	
VMware	5.5	6.0
Annuaire LDAP	Active Directory 2012 R2	
Exchange serveur	2013 SP 1	

Les serveurs systèmes seront installés sur des machines virtuelles utilisant la technologie VMWARE.

Les outils d'exploitation

Les applications devront pouvoir s'intégrer dans l'environnement d'exploitation en production suivant :

Outils d'exploitation, antivirus serveurs	Version actuelle	Évolution engagée
Logiciel d'ordonnancement de tâches	ITPAM de l'éditeur AVANTAGE PRODUCTION	
Logiciel de sauvegarde – restauration	TIME NAVIGATOR V4.3 ou supérieur de l'éditeur ATEMPO	
Logiciel de supervision IPSWITCH WHAT'S UP PRO	What's up v16.4.1 ou supérieur	
Antivirus serveurs Les logiciels antivirus de Mac Afee VirusScan pour Windows, Linuxshield, Netshield, MOVE pour les environnements virtuels.	McAfee VirusScan 8.8	VirusScan 8.8 / virtuel : Move 2.0
Mise à jour Windows pour les serveurs uniquement	WSUS 2012	

Le titulaire sera amené à préciser de quelle façon la solution intègrera les possibilités d'utilisation des logiciels ci-dessus.

Les outils de requêtes ou d'infocentre

La DSI a retenu la constitution d'un infocentre alimenté par les données utiles de certaines applications de production. Les serveurs concernés sont équipés d'un noyau ORACLE standard.

Les outils de requête et d'EIS retenus par la DSI sont :

Outils d'édition, décisionnels, d'extraction et d'infocentre	**Version actuelle**	**Version engagée**
Talend open studio	5.2.1	
BO	6.5 sp4	XI 3.1 SP5
Editions	elles devront pouvoir être créées et maintenues par les utilisateurs, de préférence sur la base d'une solution de type bureautique.	

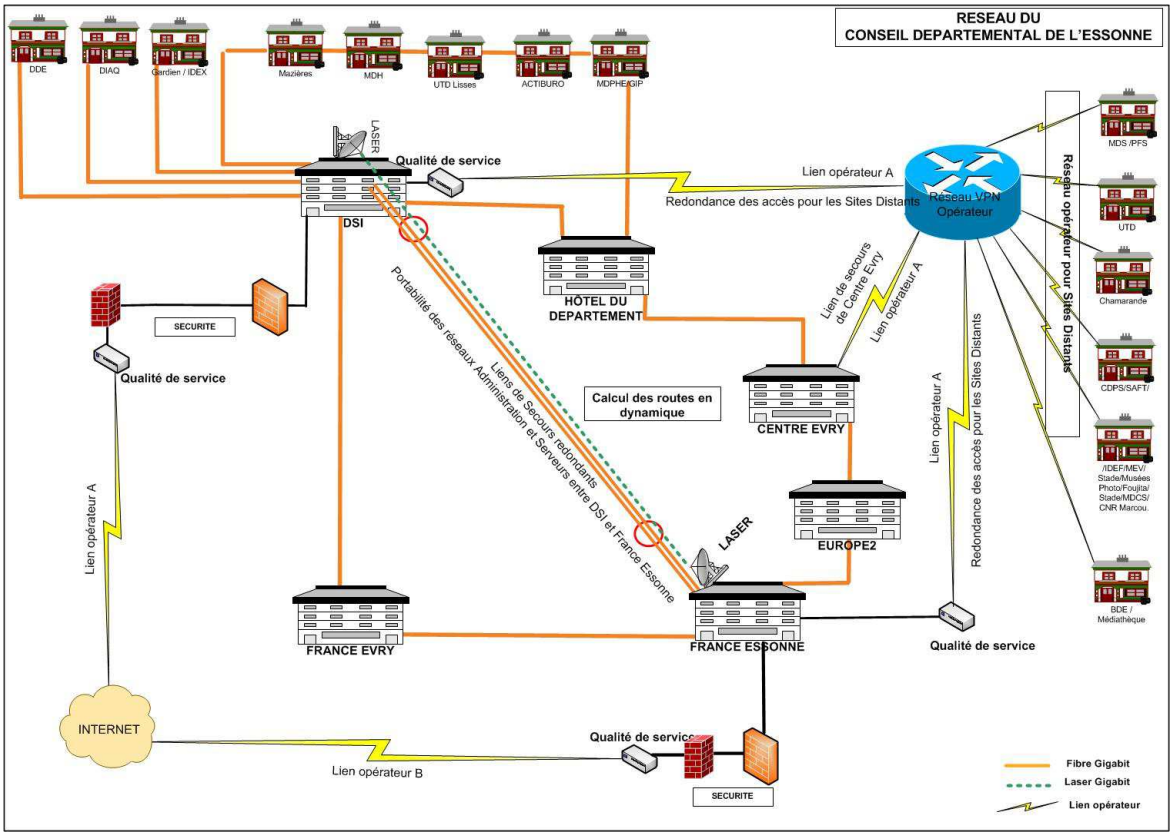
Comme outil de REPORTING ou d'extraction de données, en frontal des bases de données de production, ACCESS et EXCEL peuvent être utilisés.

Dans le cas où le système proposé nécessiterait le recours à des logiciels spécifiques, le titulaire est tenu de préciser les composants de base nécessaires à l'exécution de ses produits (outil d'alimentation de l'infocentre, moteur d'analyse multidimensionnelle, licences bureautiques ou éditiques …).

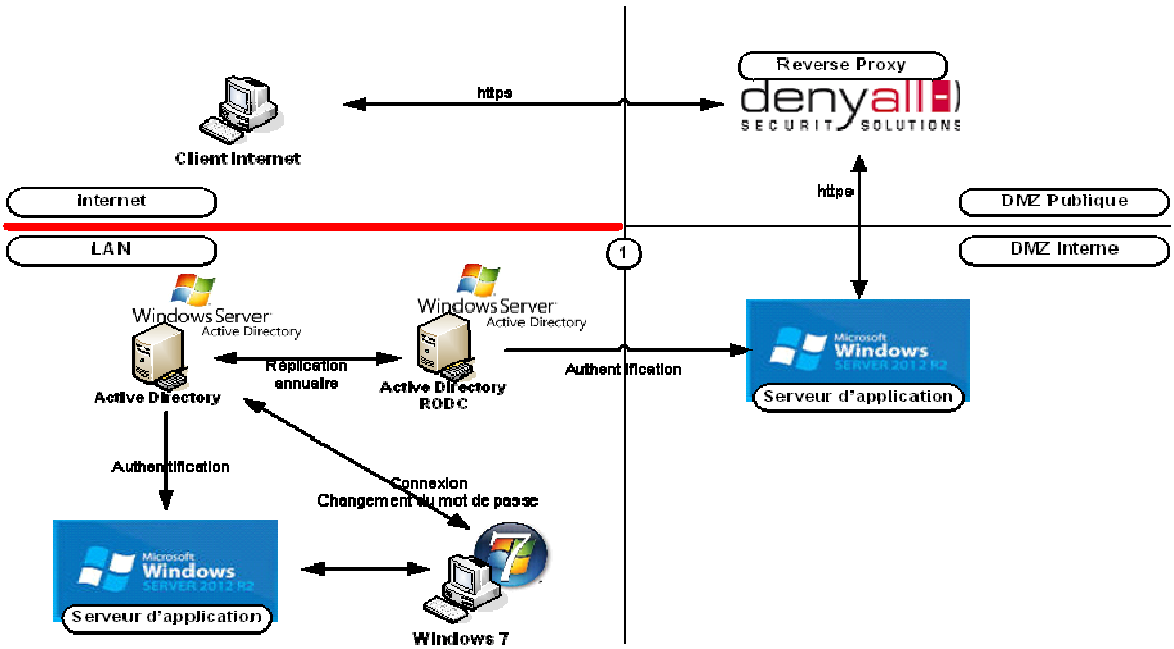
A noter

Intranet et collaboratif	**Version usuelle**	**Version engagée**
SharePoint	2013	

10.3. ANNEXE 3 Architecture réseau du Conseil départemental de l'Essonne



10.4. ANNEXE 4 Protocole d'authentification d'un utilisateur à une application métier



10.5. ANNEXE 5 Architecture métier dématérialisation du courrier et facturier