Contexte d'Intégration dans le Système d'Information de la Ville de Marseille. V3.17

mise à jour le 16/03/2017

Tableau des acteurs/responsables de contenu

Paragraphe	Responsable de la mise à jour
Paragraphe 3 : Architecture fonctionnelle	MF Fabet Nottet / C.Lico
Paragraphe 4 : Architecture de développement	C.Lico
Paragraphe 5: Architecture Technique	C.Marcy
Paragraphe 6 : Poste de Travail	R.Dorchy
Paragraphe 7 : Exploitation	R.Dorchy
Paragraphe 8 : Sécurité	R.Dorchy

Responsables éditoriaux : B.Lautard, A.Bareyan, L.Semeriva, MF [illegible]-Nottet

Table des matières

1. PRÉAMBULE

Le présent document expose l'architecture générale d'intégration dans le système d'information de la Ville de Marseille.

Les orientations présentées ici devront être prises en compte lors de la phase d'intégration de tout nouveau système dans le SI.

2. STRATÉGIE DU SYSTÈME D'INFORMATION

Dans le schéma de modernisation de la Ville de Marseille, la Direction de l'Innovation Numérique et Systèmes d'Information (DINSI) doit être force de propositions sur les systèmes d'information et sur les nouveaux usages technologiques auprès des services municipaux et des usagers.

Afin de tendre vers ces objectifs, l*a DINSI de la Ville de Marseille a entrepris une démarche d'urbanisation de son Système d'Information; une Architecture Orientée Services (ou, en anglais, SOA, Services Oriented Architecture) est en construction*.

3. ARCHITECTURE FONCTIONNELLE

3.1 Préambule

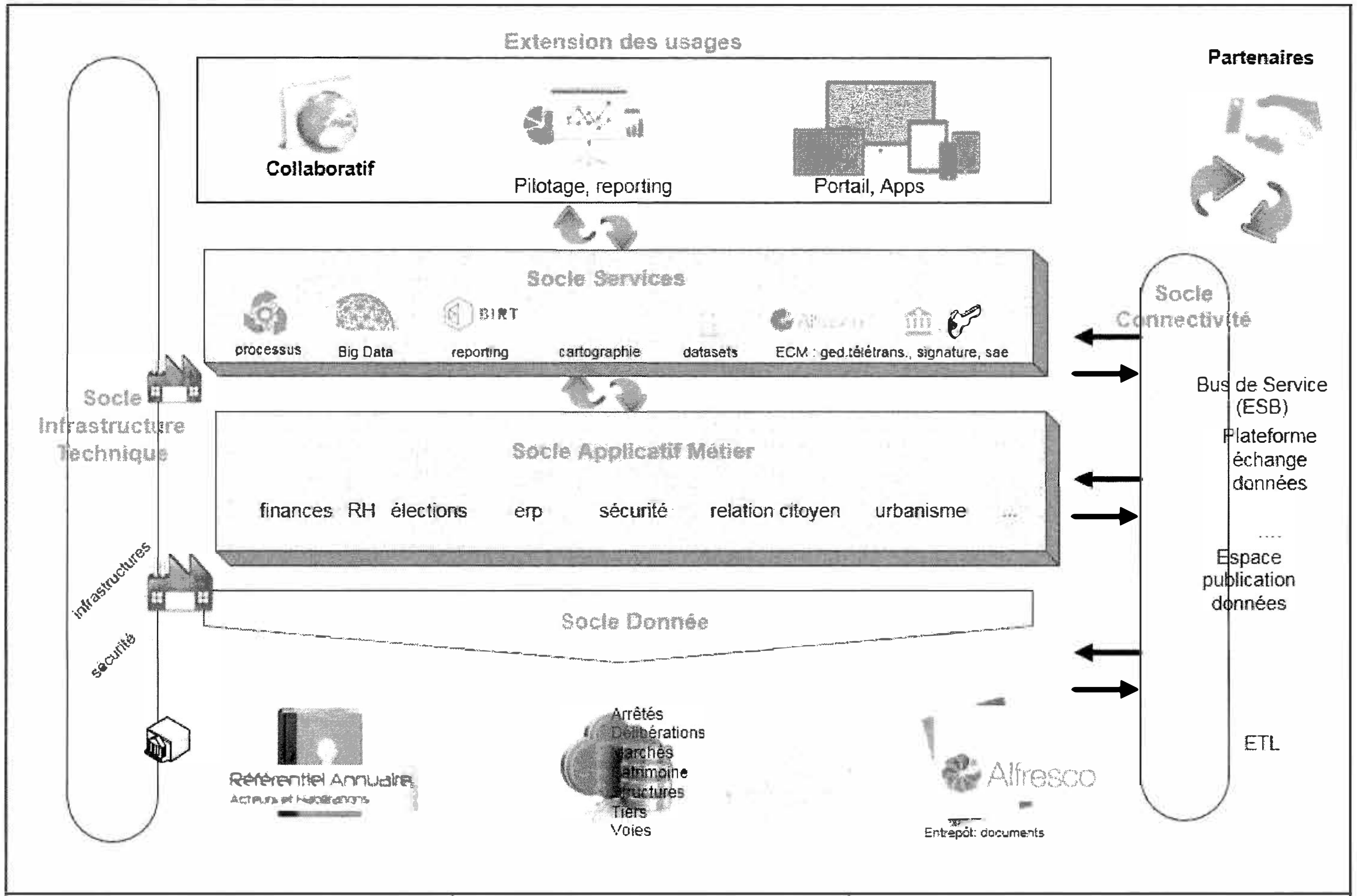
La DINSI de la Ville de Marseille a entrepris une démarche d'urbanisation fonctionnelle, bâtie sur une stratégie de « briques de services »

L'objectif est de disposer d'un système d'information évolutif et de

- limiter les impacts des évolutions
- limiter les redondances de fonctionnalités

La maîtrise de l'intégration fonctionnelle et technique dans le système d'information s'impose à toute nouvelle solution.

3.2 Intégration fonctionnelle : schéma de principe



Architecture Orientée Service Système d'Information de la Ville de Marseille	Auteurs : Christophe LICO – Philippe LAMBERTRIQUE Date : 16/03/2017

3.3 Référentiels

3.3.1 Référentiel Annuaire

Le référentiel annuaire est une base d'identification et de référencement d'objets en relation avec les concepts d'offres de services, identification, habilitation, appartenance à une cellule de l'organisation.
Il est scindé en deux projets complémentaires.

3.3.1.1 Référentiel des structures

Il permet de décrire la structure organisationnelle officielle de la Ville de Marseille, que ce soit sur le plan vertical (Délégations Générales, Directions, Services, Divisions, ...) ou sur le plan horizontal (groupes représentants une structure transversale).
Le référentiel manipule les concepts suivants :

- Organigramme : une arborescence de cellules (Délégation Générale, Direction, Service, Division etc …). Chaque cellule est caractérisée par un code, un libellé, une cellule mère et d'autres attributs complémentaires.

- Groupes (Applicatifs et Fonctionnels)

L'adresse postale d'une cellule (élément de l'organigramme ou zone géographique), est issue d'un équipement du référentiel Patrimoine.

Le référentiel des structures historise également chaque mouvement de l'organigramme, permettant ainsi de visualiser la photo de l'organisation à une date donnée ainsi que de consulter les modifications effectuées sur une cellule au cours du temps.

Le référentiel des structures provisionne l'annuaire LDAP avec des groupes représentant l'organisation. Ainsi des droits peuvent être définis par rapport à l'organisation. C'est le cas des partages de fichiers organisationnels.

3.3.1.2 Référentiel des acteurs/offres de service/habilitations

Ce référentiel permet d'identifier et de gérer le cycle de vie d'un acteur du Système d'Information de la Ville de Marseille.

Il recense également les offres de service dédiées au système d'information (applications, groupes fonctionnels, téléphonie...).

Il met en œuvre un workflow paramétrable permettant aux intervenants concernés d'instruire les demandes de créations de comptes utilisateurs ainsi que les demandes d'accès (habilitations) aux différentes offres de service.

Il offre des outils de statistiques (nombre d'utilisateurs possédant une habilitation à telle application pour une Délégation Générale, etc ...).
Il permet également d'alerter de manière automatisée lorsqu'une anomalie est constatée (utilisateur sorti de l'administration et possédant toujours des habilitations, différence entre l'affectation officielle d'un agent et son affectation réelle, ...).

Il est interfacé avec le SI de gestion des Ressources Humaines (SI RH).

Le référentiel des acteurs provisionne l'annuaire LDAP des informations sur l'utilisateur.

L'annuaire permet:

- le provisionning des utilisateurs
- l'authentification des utilisateurs: vérification compte/mot de passe
- les gestions des droits: droits d'accès aux applications (l'agent a-t-il le droit de se connecter à telle application?).

La gestion des profils applicatifs reste à la charge de chaque application.

Les authentifications et habilitations peuvent s'effectuer:

- au travers d'une connectivité LDAP pour la vérification login/mot de passe
- via un webservice «Identification» pour la vérification de l'identification et des habilitations

Le connecteur LDAP reste la solution privilégiée.

EXI-ARCHFONC-01 : La solution devra être interfacée avec l'annuaire LDAP pour la gestion des accès à l'application : vérification de l'existence de l'utilisateur et vérification de l'appartenance au(x) groupes autorisant l'accès.

3.3.1.3 Workflow lié à l'organigramme

Les modifications d'organigramme font partie de la vie d'une organisation telle que la Ville de Marseille.

Les applications déployées doivent proposer le moins d'adhérence possible à l'organisation de la Ville, dans un souci de pérennité et continuité de service.

Ainsi, la distinction doit donc être effectuée entre l'organigramme de gestion interne à l'application et l'organigramme de la Ville et les applications doivent permettre la délégation de pouvoir dans les workflows.

EXI-ARCHFONC-02 : La solution doit permettre la délégation de pouvoir dans les workflow

3.3.2 Référentiel Patrimoine

Un référentiel du patrimoine est maintenu par la ville. Il est accessible par une application web. Il est interrogeable par des services web, ou accessible sous la forme d'une base de données locale synchronisée avec le référentiel.

Le référentiel patrimoine sert à localiser physiquement la structure de la Ville de Marseille et notamment les logements de fonction des agents.

Le référentiel patrimoine porte trois concepts:

- **UPEP** qui est l'unité physique . Il y a 8 000 bâtis et terrains
  - les UPEP Bâtiments (qui se décomposent en niveaux et locaux)
  - les UPEP Terrains (qui se décomposent en surfaces et sous surfaces)

- **L'équipement.** Il s'agit de l'unité fonctionnelle (par exemple: École maternelle). Il est composé d'UPEPs ou partie d'UPEP destinés à une seule utilisation fonctionnelle et un seul affectataire.

- **Le regroupements métier.** Il s'agit de l'unité métier (par exemple: Espace vert, Chauffage). Il est composé d'UPEPs et partie d'UPEPs destinés à une seule utilisation métier par Direction Générale.

Chacun de ces concepts comporte une adresse physique principale, et peut disposer d'une liste d'adresses secondaires.
Les UPEP et les équipements existent dans le SIG et peuvent être affichés sur une carte dans un navigateur.

Il est interfacé avec
- le SIG
- le référentiel Structure
- le SI Financier
- le référentiel voirie.

3.3.3 Référentiel Voirie

Sur le territoire de la Ville de Marseille, ce référentiel de données comprend les données voies et tronçons, littérales et graphiques.

3.3.4 Référentiel Agents

Il est géré par le SIRH. On y trouve l'ensemble des informations relatives à l'agent et sa carrière au sein de la collectivité.

3.3.5 Utilisation des données de référence

Afin de garantir l'interopérabilité et l'évolutivité de son Système d'Information, la Ville de Marseille veille à ce que toute application nouvelle intégrant son SI ne gère pas de façon autonome ses propres référentiels de données.

Ces données peuvent être mises à disposition selon différents scenarii décrits dans ce document.

L'utilisation des référentiels est la règle.

Tout concept manipulé par l'application à intégrer en rapport avec une notion évoquée dans ce paragraphe devra faire l'objet d'une étude explicite d'intégration, à l'issue de laquelle le choix

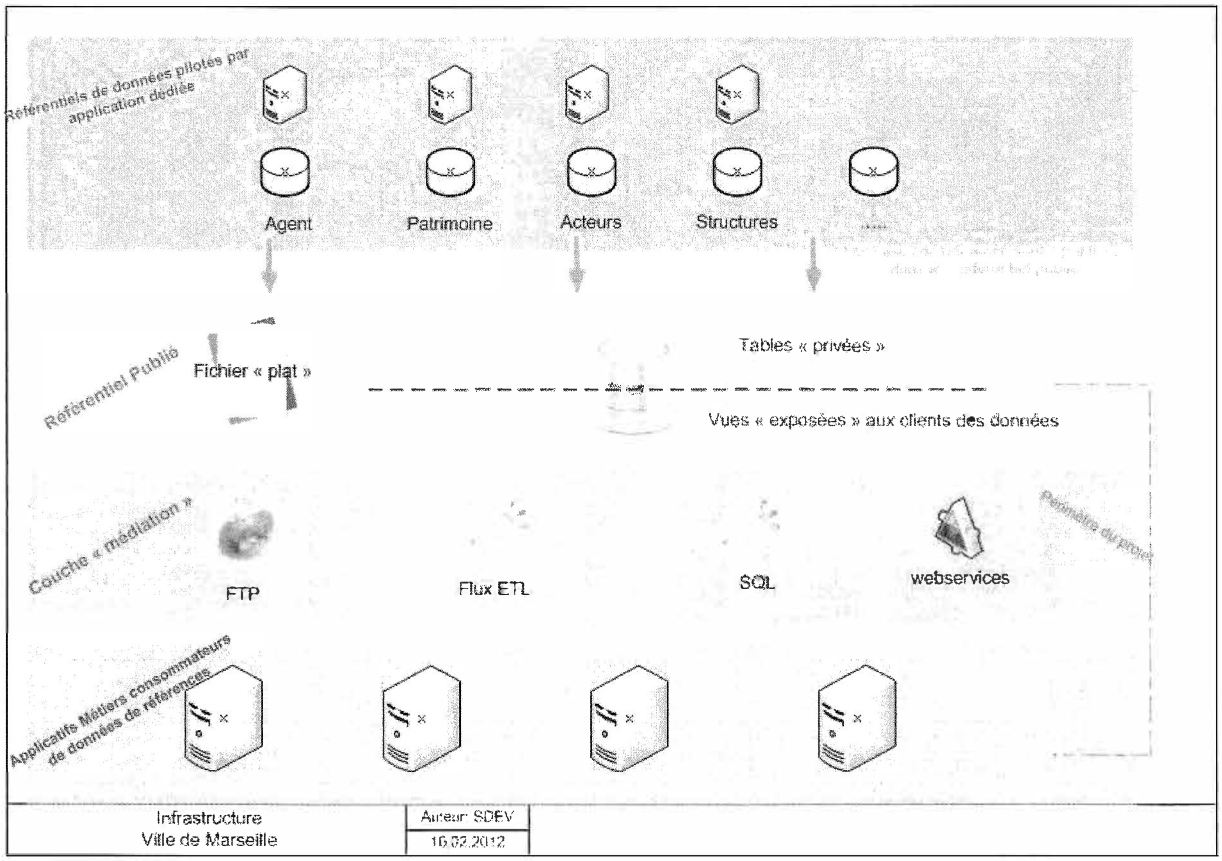
d'utilisation ou non de la donnée de référence sera arbitré.
Elle permettra également de définir la solution la plus pertinente de bonne intégration, en collaboration avec l'équipe projet de la DINSI en charge du dossier.

3.3.6 Accès aux données

Le SI Ville de Marseille dispose d'une palette de solutions techniques pour accéder aux données de références.

3.3.6.1 Fourniture de jeux de données

La Ville de Marseille souhaite consolider ses référentiels au sein d'un entrepôt consolidé dit « référentiel publié » (base Oracle).



Afin d'éviter les liaisons « point à point », ce seul référentiel publié est visible des autres applications du SI Ville de Marseille.

Pour chacune des données de référence de son SI, la Ville de Marseille est en mesure de proposer :

- la fourniture d'une vue de données dédiée : il s'agit de la solution native, privilégiée. Plusieurs « vues » Oracle sont mises à disposition de l'application cliente. Elles servent pour la mise en œuvre de flux ETL nécessaires au bon fonctionnement de l'application cliente.

- la fourniture de fichiers de données « à plat » (format de type .CSV par exemple).
  Ces fichiers sont accessibles sur un espace réseau.
  Cet espace est accessible à l'aide d'un compte FTP spécifiquement créé à l'intention du consommateur des données.

Deux types de jeux de données sont mises à disposition:
- un jeu contenant les données courantes (ou actives)
- un jeu contenant l'ensemble des données: données actives + historique.

3.3.6.2 Exposition par WebServices

Cf paragraphe dédié du présent document #4.6.WebServices|outline

3.4 Archivage électronique

La Ville souhaite acquérir un système répondant aux caractéristiques du modèle OAIS, et respectant les normes édictées par le Service Interministériel des Archives de France (SIAF), notamment en matière de format d'échange des données. Il s'agit du Standard d'Échange pour les Données de l'Archivage (SEDA) publié conjointement par la Direction générale de la modernisation de l'État (DGME) et le SIAF. La description complète de ce standard est disponible à l'adresse suivante : http://www.references.modernisation.gouv.fr/presentation.
Il est conseillé aux éditeurs souhaitant implémenter cette norme de contacter seda@culture.gouv.fr pour obtenir les dernières évolutions récentes qui n'auraient pas encore été publiées.
Techniquement, cette norme impose de fournir avec chaque document à archiver une enveloppe contenant des métadonnées en XML, parmi lesquelles :
- le type de document,
- la date de production,
- la durée de conservation,
- la durée de communicabilité,
- le sort final (conservation, élimination, etc.).

Idéalement, la solution fournie doit permettre de générer automatiquement les métadonnées nécessaires à l'archivage. Les règles de conservation concernant les documents produits dans le cadre du métier sont définies dans une circulaire émise conjointement par la DAF et la direction générale des collectivités locales. Cette circulaire est disponible à l'adresse suivante : http://www.archivesdefrance.culture.gouv.fr/static/3217.

Les différents types de fichiers qu'un logiciel est susceptible de produire doivent être listés et ces formats doivent pouvoir être transformés dans des formats-cibles, propres à être archivés. Il est conseillé de s'appuyer sur les travaux du SIAF ex-Direction des Archives de France, dans le cadre du projet PILAE, concernant les formats de fichiers et disponible à l'adresse suivante : https://www.ateliers.modernisation.gouv.fr/ministeres/projets_adele/a103_archivage_elect/public/publication-sur-formats/downloadFile/file/PILAE_Formats_Fichier_Publication_V3.pdf

Il est à noter que deux circuits d'alimentation du Système d'Archivage Électronique (SAE) sont possibles :
- les documents peuvent venir directement d'une solution métier,
- les documents peuvent être stockés dans un premier temps dans un système de GED, puis, seulement dans un second temps, versés dans le SAE. Dans ce cas, les métadonnées exportées avec le document dans le logiciel de GED doivent contenir toutes les informations permettant de générer l'enveloppe SEDA. Les données exportées de la GED restent disponibles dans la GED.

3.5 Gestion Électronique de Documents

La Ville de Marseille dispose d'une plateforme mutualisée de Gestion Électronique de Documents (GED) basée sur le produit Alfresco.

La Ville de Marseille souhaite que tous ses progiciels s'appuient sur cette plateforme transverse pour stocker et restituer les documents générés ou capturés dans le cadre de l'activité métier.

Les progiciels conservent une gestion des règles de confidentialité qui permet l'accès aux documents stockés dans la GED.

Cette centralisation des documents permettra de créer un référentiel documentaire et et facilitera l'archivage électronique ultérieur.

La Ville de Marseille a mis au point un webscript générique de dépôt de contenu dans l'entrepôt qui permet l'envoi du document et la récupération du uuid du document (la référence unique dans la GED).

Les applications identifient de façon unique tout document envoyé dans l'entrepôt, à l'aide d'un clef d'identification fonctionnelle interne.

La Ville de Marseille dispose d'une licence « alfresco enterprise ».

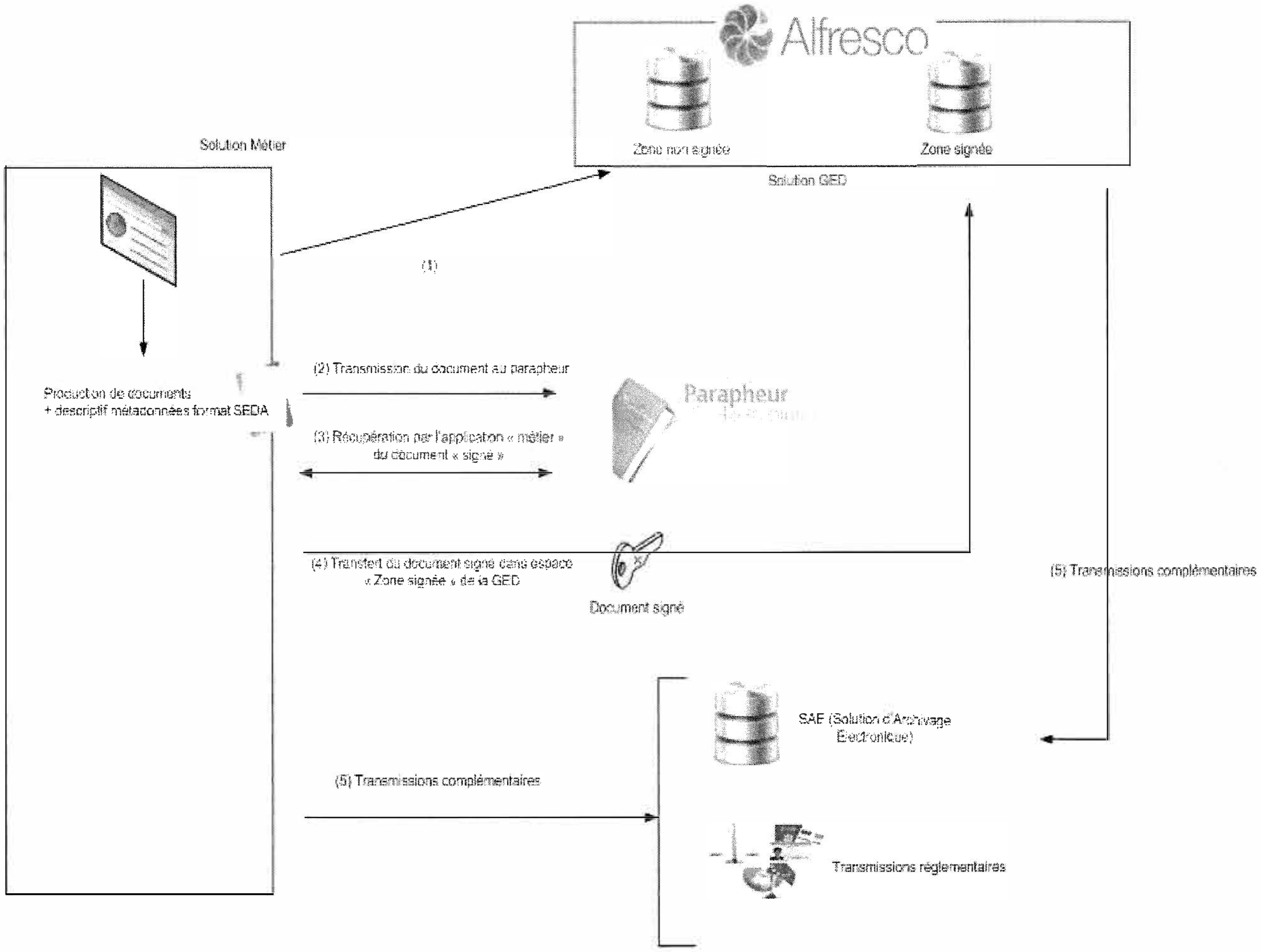
EXI-ARCHFONC-03 : La solution doit utiliser le webscript de dépôt de la Ville de Marseille pour les actions de dépôt et mise à jour des contenus. EXI-ARCHFONC-04 : La solution doit utiliser l'api RESTFul CMIS exposée par Alfresco pour toute autre communication avec la plate-forme GED, sauf pour les types de communication non couverts par cette API. EXI-ARCHFONC-05: La solution doit gérer fonctionnellement l'identité numérique du document et la stocker au niveau applicatif.

3.5.1 Cycle de vie des documents et signature électronique

La Ville de Marseille est dotée d'un parapheur électronique permettant de gérer les circuits de validation et de signature des documents puis les reverser dans l'outil de GED transversal.

Tous les documents émis seront stockés dans la GED, les documents à valeur probante seront également versés dans le Système d'Archivage Électronique.

Le schéma de principe fonctionnel de la solution retenue est le suivant:



EXI-ARCHFONC-06 : La solution consommant un service de signature électronique devra utiliser l'infrastructure en place dans le SI Ville de Marseille.

3.6 Décisionnel et Reporting

3.6.1 *L'offre Business Objetcs*

3.6.1.1 Introduction

L'offre décisionnelle de la Ville de Marseille est bâtie autour du produit Business Objects (BO).

Le cadre d'utilisation concerne: statistiques , reporting et contrôle de bases
Les utilisateurs Ville de Marseille créent leurs propres requêtes et rapports, en plus du référentiel public de documents.
Il est impératif que :

- les univers :
  - ✗ assurent l'intégrité, avec un risque minimal de création de rapport faux,
  - ✗ soient ergonomiques, simples d'utilisation,
  - ✗ garantissent une confidentialité de l'accès aux données,
- les bases de données soient performantes.

3.6.1.2 Procédures de choix pour les nouveaux projets

- Audit d'un nouvel univers ou nouvelle application BO proposé par un éditeur: effectué par notre Cellule Infocentre avec le Chef de projet,
- => Selon le résultat, soit achat de l'univers, soit développement interne par le Chef de projet ou par la TMA sous la responsabilité du Chef de Projet.

3.6.1.3 Normes de développement

Limiter au maximum le risque de création de rapports faux :

- **Créer, dans chaque univers, plusieurs contextes structurants et sécurisants** pour les utilisateurs (en général un contexte par fait), pour éviter de générer des produits cartésiens, et en conséquence des rapports faux,

- **Ne jamais mélanger deux contextes dans une même classe** : la présentation des objets de chaque contexte doit de préférence se trouver dans une même classe avec un libellé préfixé par le numéro de contexte, afin que l'utilisateur se repère plus facilement chaque fois qu'il utilise des objets de deux contextes différents dans sa requête,
- **Ne jamais utiliser de « Where » dans les objets. Il convient :**
  - ✗ Soit de positionner la condition au niveau d'une autojointure pour les restrictions persistantes (cela consiste à faire un ou plusieurs alias pour une table),
  - ✗ Soit d'utiliser des codes au niveau des objets,

- **Tendre vers le « zéro erreur » lors du lancement de l'outil « Rapport d'intégrité du désigner de BO »,**

- **Intégrer ou permettre d'intégrer de la confidentialité dans les univers,**

- **Construire les univers avec de vues** (évolutives), et non avec des tables,

- **Construire suffisamment de petits univers propres à chaque métier** pour que chaque univers diffusé soit adapté à l'organisation qui l'utilise,

- **Avoir une base de donnée infocentre performante :**
  - ✗ **Mettre en place une base infocentre** (modèle de donnée distinct de celui de l'application), avec son programme d'alimentation (en général BO Data Intégrator, ou avec

les outils d'Oracle selon le cas), pour des raisons :

- de performances : possibilité de mise en place d'index dédiés, de tables partitionnées (tables d'historiques de faits),
- de concurrences d'accès évitées avec les utilisateurs de l'application en production
- d'alimentation possible du datawarehouse : statistiques agrégées, pilotage.

- **Travailler l'ergonomie de l'univers et la facilité de compréhension :**
✗ **Faire plusieurs petits univers (200 à 300 objets)** proches des métiers pour les différents profils d'utilisateurs. Ils sont plus ergonomiques et plus faciles à prendre en main, qu'un seul univers trop gros.

Par exemple :

- pour une application RH => un univers pour le suivi des carrières, un univers pour le suivi des absences, ..
- pour une application Crèches => un univers pour le suivi de la fréquentation des enfants, un univers pour la facturation des enfants, un univers pour le suivi des absences du personnel ..),

- **Respecter toujours la même règle de nommage des univers** : Un préfixe applicatif + « _ » + le nom de l'univers (par exemple RH_Paie, FI_Budget, FI_Commande, ELEC_Procurations, ELEC_Enquetes ..),

- **Faire des classes équilibrées, en adéquation avec le nombre d'objets, et ne pas descendre au delà de trois niveaux de classes,**

- **Définir des libellés de classes explicites**, sur la granularité des objets contenus dans la classe (par exemple Budget global par exercice et par DG, ou Budget par exercice et par ligne d'Imputation budgétaire ..),

- **Éviter les objets redondants ,** par exemple le cas des objets correspondants aux colonnes des 2 cotés d'une jointure,

- **Mettre un commentaire** sur chaque classe et sur chaque objet qui le nécessite (objets calculés ..),

- **Supprimer les listes de valeurs sur certains objets** comme les dates ou les clés uniques ..

3.6.1.4 Procédures de validation

Il y a deux types de validation :

- validation technique : effectuée par notre Cellule Infocentre,
- validation fonctionnelle : effectuée par le Chef de Projet Informatique assisté du Chef de Projet Utilisateur.

3.6.1.5 Formation des utilisateurs

- La formation technique est réalisée en interne par la Ville de Marseille, **Le choix préalable des agents devant être formés à Business Objects est de la responsabilité de la Cellule Infocentre.**

- La formation aux univers et aux requêtes prédéfinies est réalisée soit par le Chef de Projet, soit par le prestataire qui a développé ces univers et requêtes sous la responsabilité du Chef de projet.

3.6.1.6 Architecture de l'info-centre

Il convient de considérer trois étapes distinctes :

- La mise en œuvre de l'alimentation de la base de donnée dédiée,
- La définition et le développement des univers,
- les requêtes prédéfinies et la formation des utilisateurs aux univers.

Fonctionnellement on distingue deux besoins en matière en rapport et requêtage : les besoins en pilotage opérationnel info-centre, les besoins en pilotage stratégique (datawarehouse).

3.6.1.7 Mise en œuvre de l'alimentation de la base de donnée dédiée

L'alimentation sera faite sur une base de donnée dédiée avec des index spécifiques à l'info-centre. La mise à jour sera périodique et adaptée à la fréquence des modifications des données dans les tables. Des vues de confidentialité seront intégrés à l'info-centre. L'alimentation doit pouvoir être supervisée par les outils de la Ville de Marseille.

3.6.1.8 Définition et développement des univers

L'objectif qui guide la Ville de Marseille est la plus grande autonomie possible des utilisateurs. La plupart de ces principes sont ceux préconisés par SAP Business Objects, lors de ses audits d'univers. Les univers fournis pourront avoir des objets masqués. Lors des évolutions de ces univers les livraisons devront prendre en compte les masques déjà intégrés.

3.6.1.9 Requêtes pré-définies et formation des utilisateurs aux univers

La Ville de Marseille souhaite participer à l'élaboration aux requêtes pré-définies pour une meilleure prise en main des univers fournis par le candidat.
La formation doit être prévue selon deux types de population : les gestionnaires métiers sur des univers spécifiques au métier, les utilisateurs dans les Délégations et Services.

Plus les univers seront de qualité et en adéquation avec les pratiques de la Ville de Marseille, plus le décisionnel sera ouvert aux utilisateurs.

3.6.1.10 Datawarehouse

La stratégie de la Ville de Marseille en matière de système d'information décisionnel repose sur deux principes :

• chaque brique importante du SI (ressources humaines, gestion financière, etc.) ayant un fort besoin de reporting et d'analyse dispose de son propre info-centre dédié. La maintenance des univers de l'info-centre est confiée aux prestataires qui ont la responsabilité de leur progiciel afin qu'ils évoluent de manière cohérente, notamment lors de l'évolution de la réglementation.

• les progiciels doivent fournir des lots de collecte pour alimenter un datawarehouse global de la Ville et permettre de recouper les données entre les différents domaines (RH, finances...). La maintenance des lots de collecte est également de la responsabilité des prestataires.

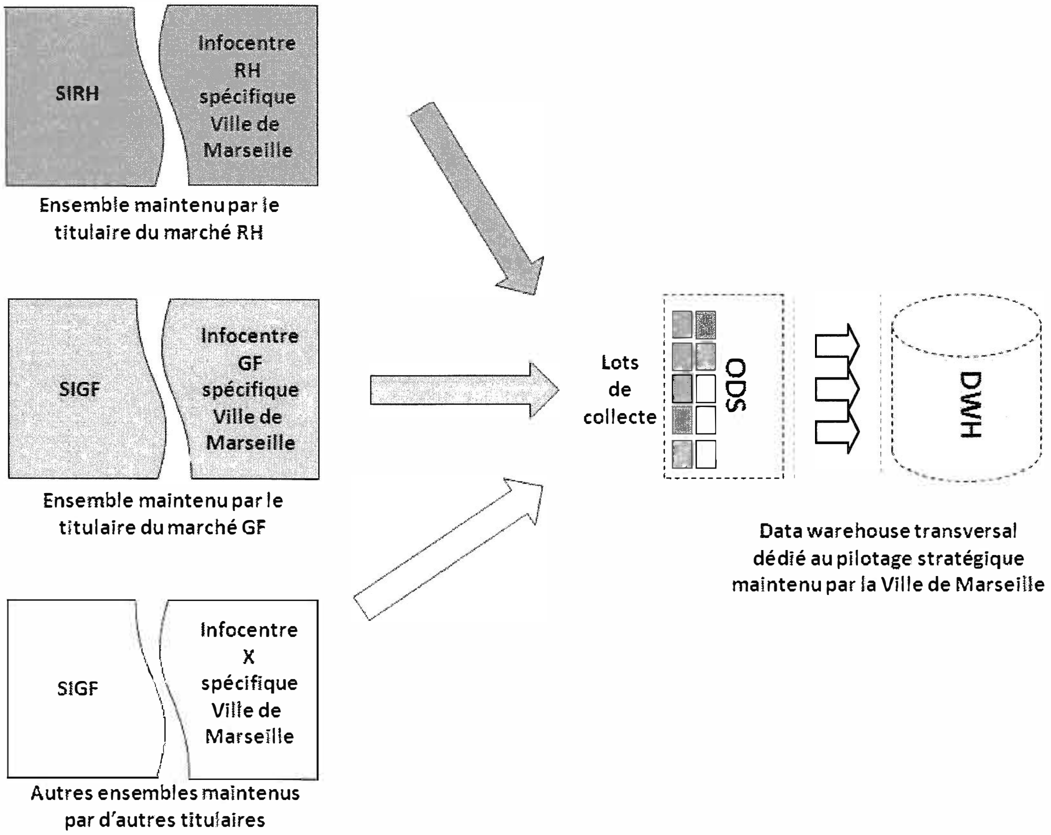


Schéma d'architecture du système d'information décisionnel de la Ville de Marseille

Le décisionnel et le pilotage s'appuieront sur la gestion d'une confidentialité par profil et par niveau de visibilité.
Une attention particulière doit être portée sur la confidentialité des données. Celle-ci ne doit pas être assurée par l'info-centre lui-même. La liste des dossiers que chaque gestionnaire peut consulter doit être maîtrisée. La sélection se fait par niveau hiérarchique de l'organigramme, soit sur les 4 niveaux de l'organisation. Puis, chaque gestionnaire à accès aux univers qui lui sont dédiés.
Fonctionnellement, on distingue trois besoins en matière de rapports et de requêtage :

• les états quotidiens doivent être traités directement dans le progiciel pour une accessibilité maximale. Il s'adresse au plus grand nombre, soit environ 500 utilisateurs.

• le pilotage opérationnel concerne environ 150 gestionnaires répartis pour un tiers à la DRH et pour les deux autres tiers dans les autres directions. Ce pilotage sera réalisé à partir d'un info-centre dédié.

- le pilotage stratégique touche par nature tous les domaines métiers de la Ville. Il est réalisé à partir d'un datawarehouse central, unique regroupant les informations RH, Financières...

La Ville de Marseille établit les principes directeurs de conception suivants.
L'objectif qui la guide est la plus grande autonomie possible des utilisateurs. La plupart de ces principes sont ceux préconisés par SAP Business Objects lors de ses audits d'univers.

Les univers fournis ne doivent pas proposer un trop grand nombre d'objets. Plusieurs univers, de taille plus réduite, sont plus facilement utilisables qu'un seul univers, très vaste.

Par ailleurs, les univers doivent être contextualisés, pour éviter les produits cartésiens d'ensembles.
Une attention particulière doit être portée sur la confidentialité des données. Celle-ci doit être assurée en amont, et pas par des filtrages dans l'infocentre lui-même, dépendant de manipulations de l'utilisateur. La liste des dossiers que chaque agent peut consulter doit être contrôlable. La sélection se fait par niveau hiérarchique, sachant que les 4 niveaux sont possibles. Ensuite, l'accès est donné univers par univers.

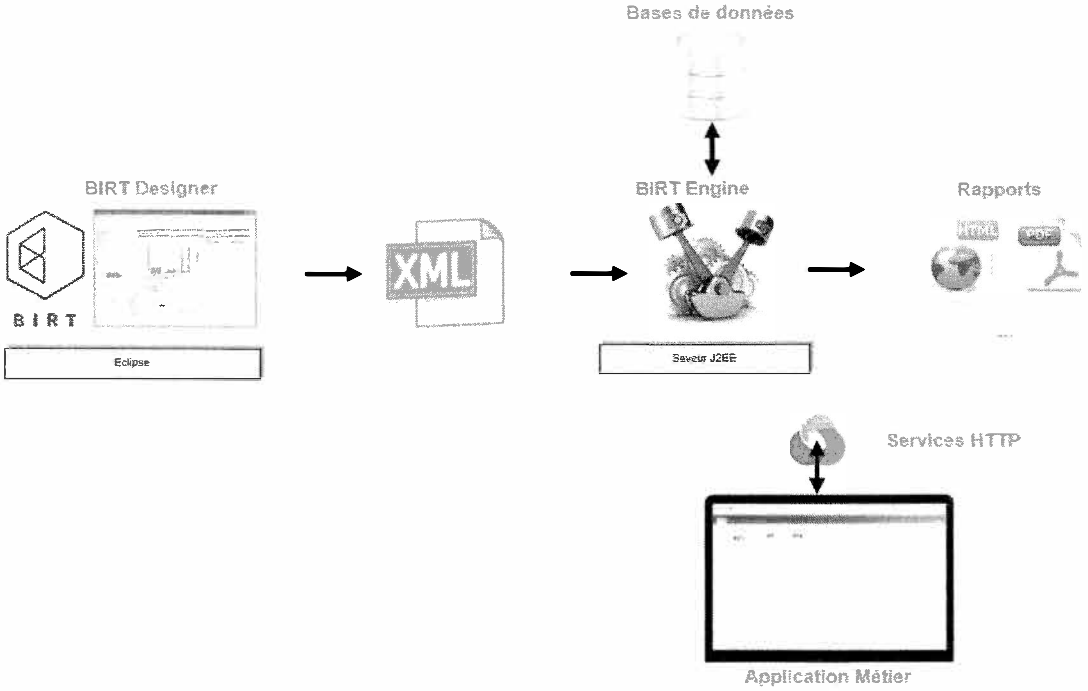
3.6.2 Plateforme de services BIRT

Le SI Ville de Marseille dispose d'une infrastructure serveur dédiée à l'exécution du moteur de reporting BIRT.

BIRT (The Business Intelligence and Reporting Tool) est un projet de la communauté Eclipse comprenant un générateur de graphiques, un générateur de rapports et un environnement de conception.

Il est demandé pour la production de tableaux de bord adhoc, listing de données peu complexes ne nécessitant pas l'abstraction du modèle physique de données (cas justifiant l'usage de la suite Business Objetcs) d'utiliser ce moteur de reporting.

3.6.2.1 Schéma d'architecture générale



3.7 Diffusion, Portail, Espaces collaboratifs

3.7.1 Portail intranet

La Ville de Marseille possède un portail Intranet généraliste (E-media).
C'est un outil de communication sur les problématiques transverses de la Ville.

Cet intranet est complété par un ensemble de sites intranets dédiés à une communication plus opérationnelle au niveau des services de la Ville (Délégations/Directions).

Le portail intranet est un point d'entrée direct vers :
- ➢ les applicatifs métiers du SI Ville de Marseille,
- ➢ certaines fonctionnalités intégrées à un applicatif métier mais également directement

accessible par une URL.

Ces liens d'accès sont publiés sur le portail dans une zone dédiée « Boîte à outils ».

3.7.2 Espace collaboratif

La Ville de Marseille utilise le produit Alfresco Share comme solution de gestion d'espace collaboratif.

Cette solution fait l'objet d'une infrastructure logicielle et technique dédiée.

3.8 Services Géographiques

3.8.1 Définitions

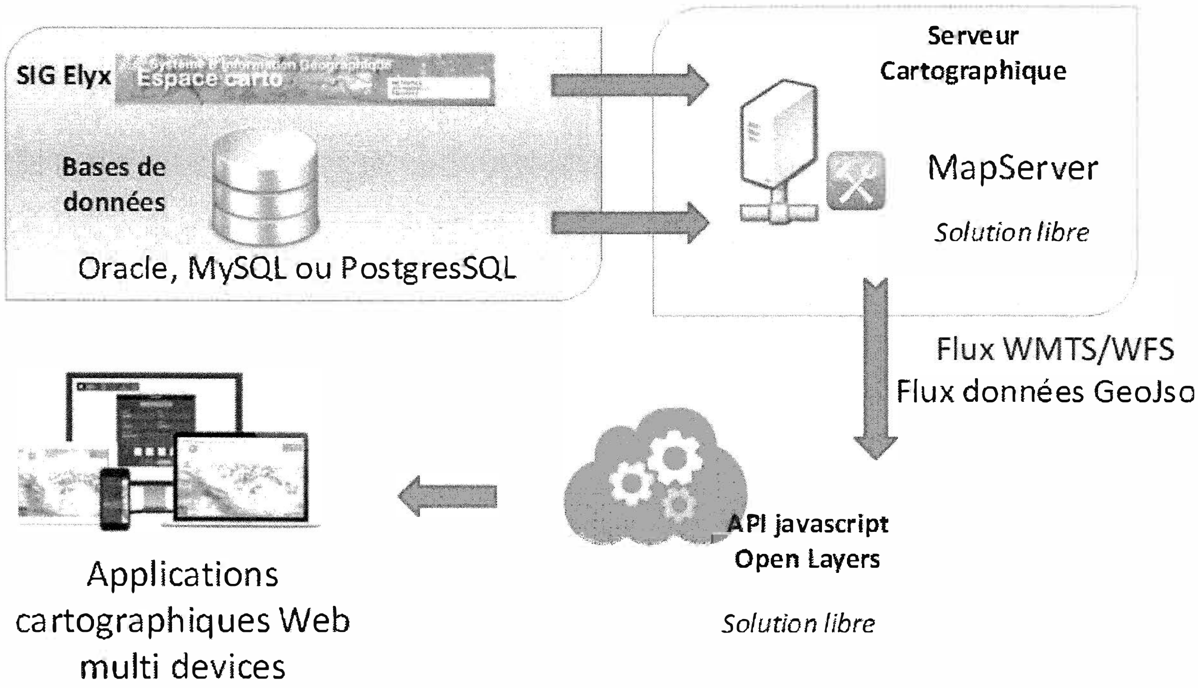
Geojson : Format d'échange textuel utilisé pour encoder les données géospatiales

WMS : Un service WMS sert à retourner une image visualisable (JPEG, PNG ou GIF).

WMTS : (Web Tile Map Service) permet d'obtenir des cartes ***tuilées*** précalculées mises en cache => meilleure fluidité d'affichage.

WFS : Un service WFS permet d'interroger des serveurs cartographiques afin de consulter/modifier les attributs d'objets géographiques.

3.8.2 Schéma d'architecture générale



Le SI Ville de Marseille dispose d'un socle SIG piloté par la suite d'applications ELYX.
La couche « services » destinée à la mise en œuvre d'applications tierces est assurée par l'infrastructure MapServer.

Les principaux services à disposition sont
- Fond de plan Ville tuilé (WMTS)
- Photo aérienne tuilée (WMTS)
- Webservices de géolocalisation (Rest GeoJSON)

3.8.3 Formats d'échanges

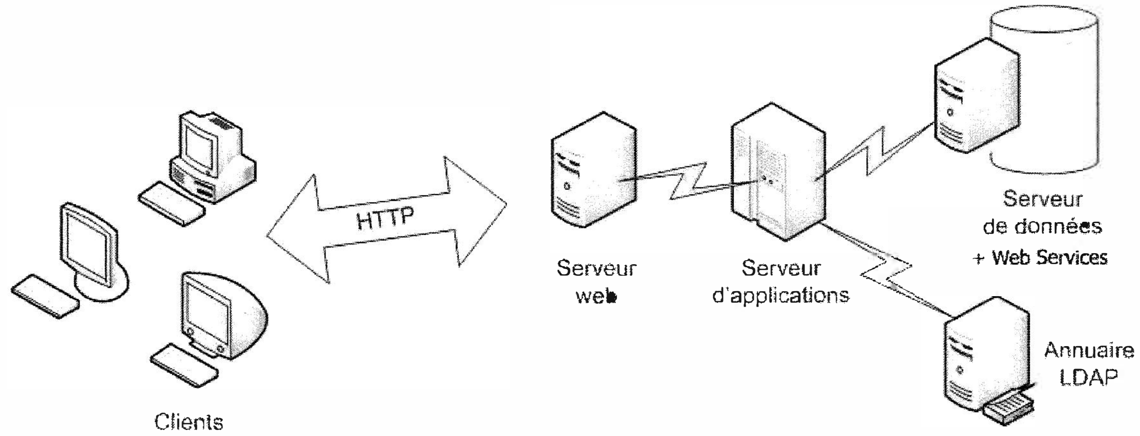
Les échanges de données géographiques se font au format GeoJSON.

EXI-ARCHFONC-08 : Les flux de données structurées ayant une composante géométrique sont produits au format GeoJSON

4. ARCHITECTURE DE DÉVELOPPEMENT

Le but de ce paragraphe est de présenter et de décrire l'architecture logicielle de la Ville de Marseille afin de définir un cadre normé pour les développements spécifiques.

L'architecture multi-tiers suivante sera valable pour tous les développements :



L'ensemble des postes clients se connectent aux applications web par l'intermédiaire du serveur de présentation ou serveur web. Celui-ci transmet les traitements à exécuter au serveur d'applications. Ce dernier peut traiter des données stockées dans le(s) serveur(s) de données et/ou dans l'annuaire LDAP, ainsi qu'au travers de « web services ».

Dans le cadre des développements spécifiques en technologie « web », l'environnement J2EE est privilégié.

Les applications J2EE sont déployées au sein du serveur d'application JBOSS.

Le conteneur de servlet Tomcat peut rester une alternative après motivation du choix.

L'intégration de logiciels libres en technologie PHP est une option retenue par la Ville de Marseille pour le développement de son système d'information ; elle a notamment entrepris une démarche de montée en compétence sur l'intégration d'applications développées sur la base du framework openMairie.

Par ailleurs, l'atelier logiciel 4D est également utilisé pour certains développements internes.

4.1 <u>Cadre de développement</u>

4.1.1 Langages

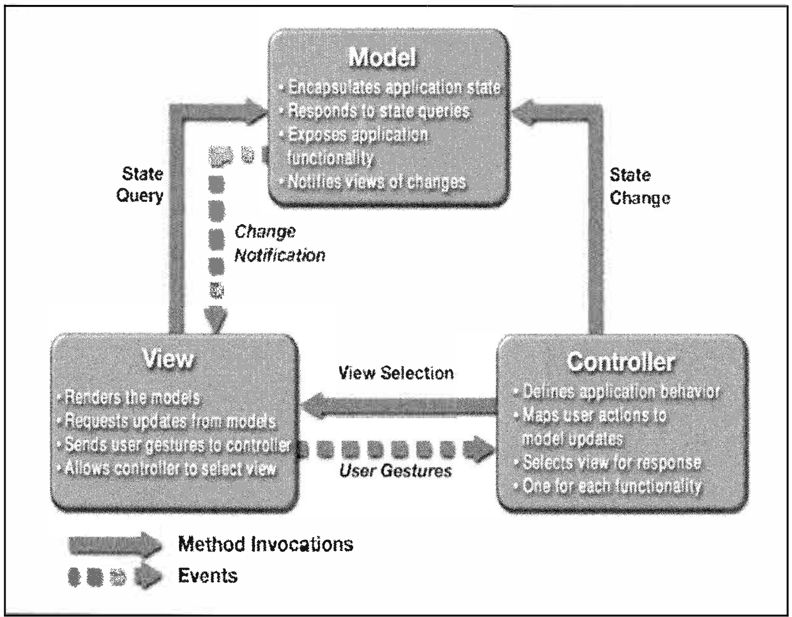
Les principaux langages utilisés sont les suivants :

- Java : traitements côté serveur
- HTML : présentation côté client,
- JavaScript : contrôles et présentation côté client,
- XML : paramétrages et configurations côté serveur, échanges de données,
- SQL : requêtage en base de données.

Le codage des pages HTML doit être valide W3C. Pour cela, les pages seront testées avec l'outil de validation du W3C : http://validator.w3.org.

4.1.2 Modèle MVC

Le Modèle-Vue-Contrôle (MVC) permet la séparation en 3 couches principales :



Le modèle MVC doit être implémenté dans toute développement.

4.1.3 Modèle multi-couches

<u>Le tiers Client</u> : Responsable de la mise en œuvre des interactions avec l'utilisateur, il s'exécute sur le poste de travail de l'utilisateur au travers d'un navigateur (langage HTML) ;

<u>Le tiers Web</u> : Responsable du traitement des requêtes utilisateurs, et des réponses au tiers client (par le protocole HTTP), assure également un contexte de session « client ». Il est mis en œuvre par le biais d'un serveur HTTP frontal et d'un serveur d'application.

<u>Le tiers Métier</u> : Responsable de la fourniture des services métiers, implémenté avec des composants;

Le tiers Données : Responsable de la persistance des données de l'application.

Le tiers Services : Responsable de la mise à disposition des web services.

Une architecture multi-tiers sera mise en oeuvre dans tout développement spécifique.

4.2 Spécificités développement J2EE

4.2.1 Design Patterns

Le design patterns de référence : Gang Of Four et patterns J2EE.

4.2.2 Accès aux données

4.2.2.1 DataSources

Pour les applications J2EE, l'accès aux bases de données via ***JDBC (Java DataBase Connectivity)*** devra se faire par le biais de la technologie des DataSources. Les drivers JDBC seront installés en tant que librairies communes sur Tomcat et Jboss.

Sur **TOMCAT**, les datasources seront définies dans le fichier context.xml, situé dans le répertoire META-INF de toute application web.

Sur **JBOSS**, les datasources seront déclarées dans le serveur via la console d'administration (Web ou shell)

4.2.2.2 DAO : Data Access Object

Utilisation du design pattern ***DAO (Data Access Object)*** pour récupérer des données dans un SGBD ou dans tout autre système de stockage.

Le design pattern DAO permet de :

- centraliser l'accès aux données,
- rendre indépendante l'application par rapport à toutes les sources de données potentielles,
- masquer le détail de l'implémentation des sources de données.

4.2.3 Déploiement par fichier war

Toute application web J2EE sera livrée pour déploiement sous la forme d'une archive de type WAR. Toutes les informations propres à un environnement doivent être externalisées afin que le WAR soit unique.

Sous TOMCAT, pour rendre le fichier de datasources commun aux différents environnements, on utilisera des variables d'environnement :

- vdm.app.<CODE_APPLI>.pwd : Mot de passe pour la base de données
- vdm.app.<CODE_APPLI>.service : SID pour la base de données Oracle
- vdm.env : Environnement de l'instance (dev, int, va ou prod)
- vdm.domain : Domaine l'instance (dev.mars, int.mars, va.mars ou vdm.mars)
- vdm.bdd.domain : Domaine des bases de données de l'instance (dev.bdd.mars, int.bdd.mars, va.bdd.mars ou prod.bdd.mars)

Ci dessous, la liste des variables permettant de définir le port de la base de données.

	Environnements				
	Variable	**DEV**	**INT**	**VA**	**PROD**
MySQL	vdm.bdd.mysql.port1	3311	3321	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.mysql.port2	3312	3322	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.mysql.port3	3313	3323	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.mysql.port4	3314	3324	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.mysql.port5	3315	3325	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.mysql.port6	3316	3326	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.mysql.port7	3317	3327	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.mysql.port8	3318	3328	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
Oracle	vdm.bdd.oracle.port1	1521	1521	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port2	1521	1521	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port3	1523	1522	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port4	1521	1521	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port5	1524	1524	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port6	13055	13055	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port7	13055	13056	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port8	13055	13056	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port9	13055	13056	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port10	13058	13059	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port11	13056	13056	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port12	13058	13059	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port13	13058	13059	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.oracle.port14	1521	1521	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
PostgreSQL	vdm.bdd.postgresql.port1	5462	5452	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.postgresql.port2	5463	5453	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.postgresql.port3	5464	5454	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
	vdm.bdd.postgresql.port4	5465	5455	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*

Environnements				
Variable	DEV	INT	VA	PROD
vdm.bdd.postgresql.port5	5492	5492	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*
vdm.bdd.postgresql.port6	5494	5494	*Fournies en phase de mise en service*	*Fournies en phase de mise en service*

Sous JBOSS, le fichier des datasources sera externalisé (« <CODE_APPLI>-ds.xml ») et livré en même temps que le war.

4.2.3.1 précision de la version

Le tag <display-name> du fichier : xxxx.war\WEB-INF\web.xml) doit porter la mention de la version de l'application (qui doit être identique à la version du nom de répertoire « Version x.y.z »).

4.2.3.2 gestion des datasources

Une standardisation des jndi pour les datasources est requise : utiliser la norme java:/jdbc/{code appli}

Si il y a plusieurs datasources, elles doivent être toujours prefixées par le {code appli}
exemple :java:/jdbc/{code appli}/datasource1

4.2.3.3 externalisation et nommage des propriétés

Afin de faciliter le déploiement des applications sur les différents environnements (Développement, Intégration, Vérification d'Aptitude, Production ...), les propriétés utiles au fonctionnement de l'application ***doivent être sorties du livrable executable***.

La solution retenue est :

serveur	Solution d'externalisation
JBOSS	Fichier(s) chargé(s) en tant que module et placé(s) dans le répertoire de module : vdm/configuration/main situé à la racine du répertoire module.
TOMCAT	Placer les fichiers .properties dans le répertoire catalina.base/conf-app

Si il y a plusieurs fichiers de propriétés, il convient de nommer ces fichiers en préfixant par le code application
exemple :
{code appli}.properties
{code appli}.fichier2.properties
{code appli}.fichier3.properties

Pour le **nommage des propriétés**, il convient de préfixer chaque propriété du code de l'application exemple :
{code appli}.propriété1
{code appli}.propriété2
etc ....

4.2.3.4 gestion des logs

Au niveau des logs, utiliser les variables :

serveur	variable
JBOSS	${jboss.server.log.dir}
TOMCAT	${catalina.base}/logs/

4.2.4 Règles de codage

4.2.4.1 Java

Les règles de codage en Java respectent les standards préconisés par Sun MicroSystems.
http://java.sun.com/docs/codeconv
http://java.sun.com/docs/codeconv/CodeConventions.pdf.

4.2.5 Logiciel et choix technologique

La ville de Marseille privilégie :

- **Eclipse** comme IDE
- **Jboss** comme serveur J2EE
- **JSF** comme framework Java
- ***Jquery et Jquery UI*** : librairies javascript pour l'ajout de fonctionnalités de type AJAX http://www.jquery.com et http://www.jqueryui.com

4.3 Traçabilité des livrables

4.3.1 Versionning

Toute application déployée dans le SI Ville de Marseille doit comporter un numéro de version permettant de l'identifier, ce, afin de faciliter les opérations de support et maintenance.
Ce numéro de version est accessible au travers de l'application.

Un fichier version.txt comportant la seule mention du numéro de version est déposé à la racine du livrable (à la racine du.war ou de l'archive php pour les cas les plus répandus dans le SI VDM)

EXI-ARCHDEV-01 : Tout composant (application, module) déployée dans le SI Ville de Marseille doit disposer d'un numéro de version permettant de clairement l'identifier. Ce numéro de version est en particulier renseigné dans un fichier version.txt systématiquement mis à disposition avec un livrable applicatif.

4.3.1.1 Pour le cas des applications JAVA (déploiement war ou ear)

Le tag <display-name> du fichier : xxxx.war\WEB-INF\web.xml) doit porter la mention de la version de l'application (qui doit être identique à la version du nom de répertoire « Version x.y.z »).

4.4 Sources applicatives

Lorsque la ville est propriétaire des sources d'une application, celle ci doivent être mise à disposition et versionné sur le SCM (Source Code Management) de la ville de Marseille à chaque livraison.
Ce SCM héberge des repository de type SVN ou GIT.

Dans le cas des applications Java, la ville souhaite que les livrables soit aussi déposé sur le repository Maven de la Ville.

EXI-ARCHDEV-01 : Les développements effectués de façon spécifiques pour la Ville de Marseille

4.5 Accessibilité et ergonomie

Tout développement doit tenir compte dans sa mise en œuvre, des travaux menés par la DGME sur l'accessibilité, en particulier de la « charte graphique et ergonomique des télé-procédures publiques » et du RGAA (Référentiel Général d'Accessibilité dans l'Administration) disponible à l'adresse suivante: http://www.references.modernisation.gouv.fr/rgaa-accessibilite.

4.5.1 Adaptabilité des applications web (responsive design)

La consultation des applications web s'effectue sur une large gamme de support : poste fixe, ordinateur portable, tablette, téléphone.

Un site web adaptatif (anglais RWD pour **responsive** web **design**, conception de sites web adaptatifs selon l'OQLF) est un site web dont la conception vise, grâce à différents principes et techniques, à offrir une expérience de consultation confortable même pour des supports différents.

EXI-ARCHDEV-02 : Toute application WEB, c'est à dire utilisée au travers d'un navigateur, doit être « Responsive web design » à priori. Un arbitrage spécifique pourra être fait par la Ville de Marseille sous réserve de justifications qu'elle jugera pertinentes lors de la phase d'étude d'intégration de la solution.

4.6 WebServices

4.6.1 Norme de développement

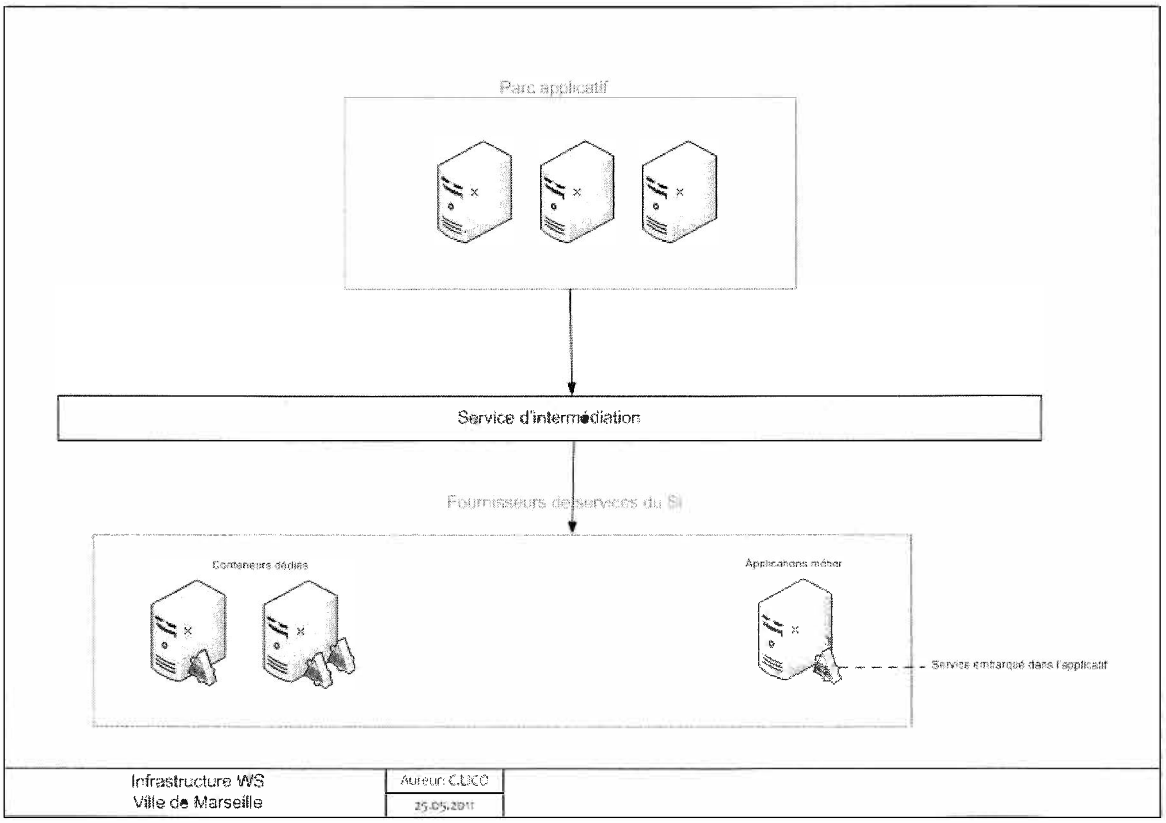
Au vu de la taille de notre SI et de son hétérogénéité en terme de technologie, il est indispensable que l'accès aux services soit le plus large possible.

L'exposition selon le protocole REST est requise de façon systématique. Une exposition via le protocole SOAP est un complément appréciable.

De plus l'accès à chaque service doit être filtré via un groupe fonctionnel issu du LDAP (CF Référentiel Annuaire)

4.6.2 Modalités d'exposition

Les webservices sont exposés au travers d'un service d'intermédiation qui
- référence l'ensemble des webservices du SI Ville de Marseille
- les expose aux consommateurs de services et oriente ces consommateurs sur la ressource qui fournit le service.



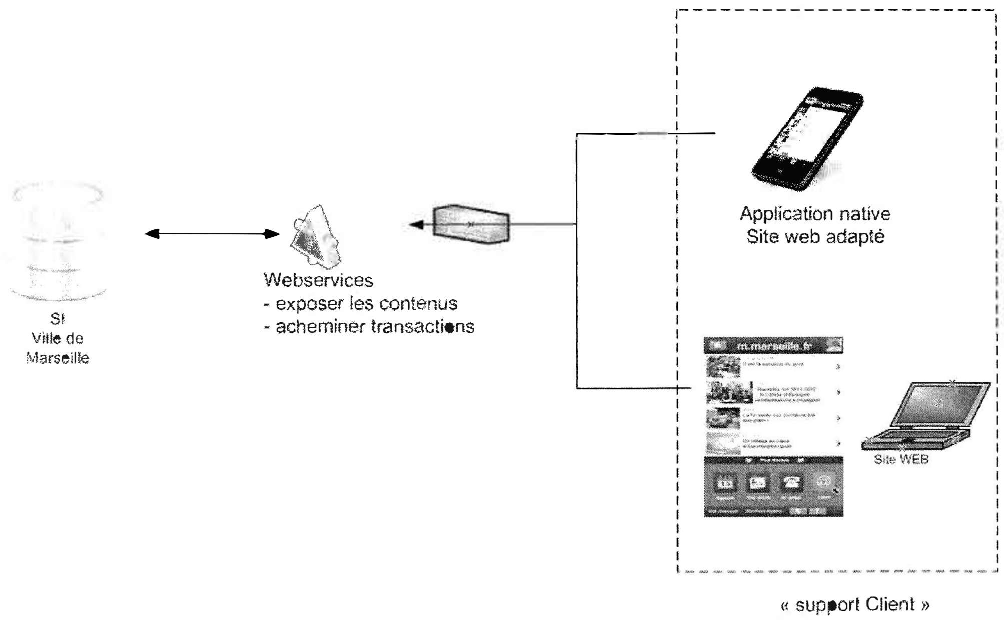
Ce service permet un couplage faible entre « consommateur » de service et « fournisseur » de service.
L'accès s'effectue via un canal sécurisé **https.**
La liaison https s'effectue entre le consommateur du service et la couche « service d'intermédiation ».

La consommation des webservices est effectuée par des clients identifiés auprès du webservice. (technique d'authentification BASIC permettant d'échanger ses « crédentials » afin d'assurer l'authentification du consommateur).

4.7 Applications mobiles

4.7.1 Principe d'architecture général

Une application mobile native ('app') est un "logiciel" que l'on installe sur son support (téléphone, tablette).
Une web-application ('webapp') est un site internet créé spécialement pour les supports « mobile », avec une interface adaptée à l'utilisation tactile.
Dans les deux cas, on utilise les protocoles standards du WEB (HTTP(S)) pour acheminer les contenus.
Le schéma de principe à respecter est le suivant :



4.7.2 Sécurisation

4.7.2.1 De l'accès

Dans le cas où l'application manipule des données jugées sensibles par la Ville de Marseille, une authentification préalable de l'utilisateur sur les annuaires de la Ville est requise.

En mode déconnectée, si l'application stocke de la donnée jugée sensible par la Ville de Marseille, un mécanisme d'authentification préalable est également requis.

Pour des raisons de confidentialité, les cinématiques d'authentification en vigueur au sein du SI Ville de Marseille seront communiquées en phase d'étude d'intégration de la solution.

4.7.2.2 Du stockage

Dans le cas où l'application stocke des données jugées sensible par la Ville de Marseille, un chiffrement local est requis.

Pour des raisons de confidentialité, les précisions sur les modalités de chiffrement en vigueur au sein du SI Ville de Marseille seront communiquées en phase d'étude d'intégration de la solution.

4.7.2.3 des échanges

Les flux échangés avec les couches de services du SI Ville de Marseille doivent être
- chiffrés
- authentifiés

Cf paragraphe ***WebServices*** du présent document.

EXI-ARCHDEV-03 : Les échanges de données entre les applications mobiles et le SI Ville de Marseille se font de façon chiffrée et authentifiée.

EXI-ARCHDEV-04 : Le stockage de données jugées sensible par la Ville de Marseille en phase d'étude d'intégration de la solution, devra être chiffré.

4.7.3 Les applications hybrides

Ces applications sont basées sur un ensemble de langages communs entre toutes les plateformes: HTML, CSS, JavaScript.
Elles présentent les caractéristiques des applications natives : accès aux ressources du téléphone, mode déconnecté...grâce à l'utilisation d'une surcouche (ou wrapper) qui permet, pour faire simple, de compiler et générer à partir d'un même code une version d'application par OS cible.

Pour des raisons de maintenabilité, la Ville de Marseille privilégie le développement d'applications hybrides (WebView)

EXI-ARCHDEV-05 : Toute application mobile développée spécifiquement pour la Ville de Marseille doit être mise en œuvre sous forme d'application dite hybride. Un arbitrage spécifique pourra être fait par la Ville de Marseille sous réserve de justifications qu'elle jugera pertinentes lors de la phase d'étude d'intégration de la solution.

La solution technique utilisée par la Ville de Marseille est la suivante :

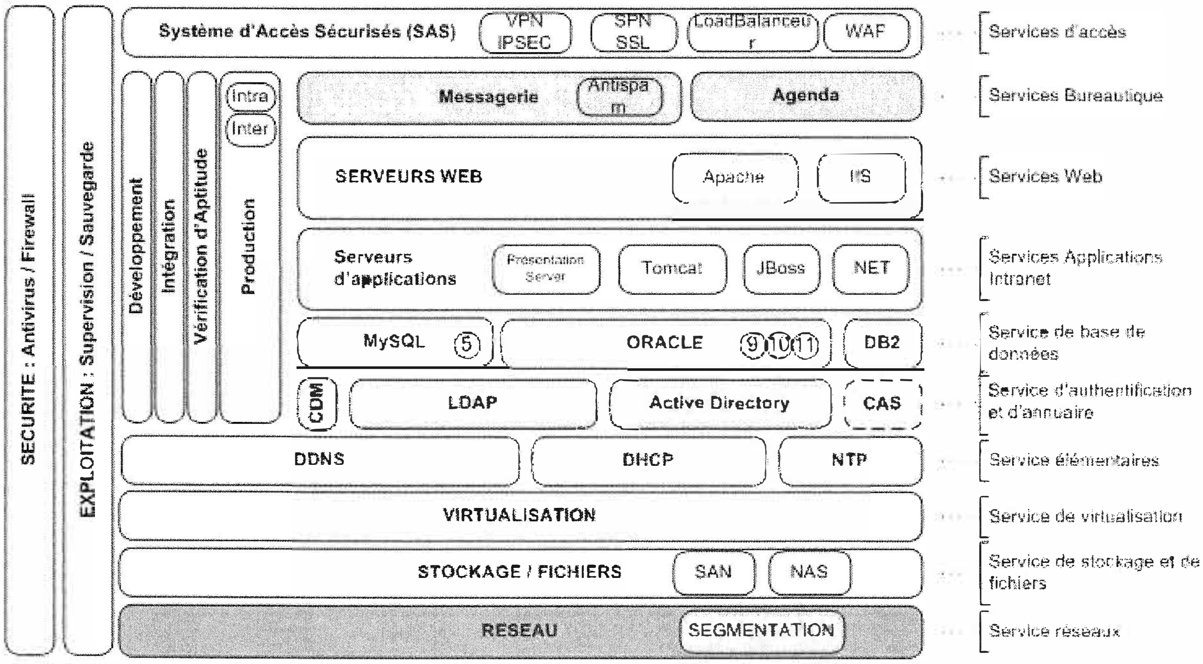
Solution : Hybrid Mobile App (WebView)
Packaging: Cordova (PhoneGap)
Framework de développement : Ionic
Base de données: SQLite + plugin encrcyption
OS de dév: Indépendant de la plateforme de Dév

5. ARCHITECTURE TECHNIQUE

5.1 Introduction

La DINSI de la Ville de Marseille a bâti un référentiel technique suivant une stratégie de «briques de service». Ce dernier fournit des «services d'infrastructure» permettant de satisfaire aux besoins d'intégration d'application métiers.

Il est architecturé comme suit:



5.2 Services réseaux

5.2.1 Réseau physique

Le réseau de la Ville de Marseille est architecturé en étoile. Cette étoile est bâtie autour de deux sites principaux sur lesquels se trouvent aussi les deux « Data Centers ».

Ces deux sites principaux fonctionnent en tolérance de panne et desservent ensuite 6 sites de distribution.
Les deux sites principaux et les six sites de distribution constituent le cœur de réseau. Ils sont reliés en double adduction par des fibres optiques. Le cœur de réseau est donc sécurisé en terme de disponibilité et permet un débit de 10 Gb/s entre ces huit sites.
Les sites utilisateurs au nombre de 250 sont interconnectés derrière les différents sites du cœur. Ces interconnexions sont conjointement assurées par des liaisons du réseau indépendant de la Ville de Marseille et des liaisons xDSL fournies par un tiers opérateur. Ces sites utilisateurs peuvent donc bénéficier d'un débit allant de 500 Kb/s à 1 Gb/s.

5.2.2 Segmentation

Afin d'assurer une sécurité plus importante, un ensemble d'applications et de services fournis par des serveurs est isolé par une segmentation réseau (VLAN) ; séparant ainsi la couche de présentation, d'application et de données et les environnements d'intégration, de validation et de production.
Des règles explicitement définies règlent les autorisations de flux entre les différents segments

Il conviendra au candidat de fournir l'ensemble des besoins de communications entre les différents modules de l'application et les services existants afin que les autorisations soient définies.

5.3 Services élémentaires

5.3.1 DHCP

Le service DHCP est assuré par des serveurs Windows Server 2008 R2 au travers du rôle « Services DHCP ». Ces serveurs distribuent l'ensemble de la configuration réseau à tous les sous-réseaux relayés par des switchs CISCO.

5.3.2 DNS

Le service DNS est décomposé en deux parties : la partie Internet (publique) des noms de domaines marseille.fr, mairie-marseille.fr, etc. est assurée par des serveurs BIND sous Linux RedHat ; la partie Intranet (privée) des noms de domaines mars, vdm.mars et bmvr.mars (correspont à notre architecture Active Directory) est assuré par des serveurs Windows Server 2008 R2 au travers du rôle « Serveurs DNS ».
L'enregistrement dynamique des ressources est autorisé en mode sécurisé pour tous les postes de travail Windows et pour les DHCP qui assurent majoritairement l'inscription des adresses distribuées.
Compte tenu de la fonctionnalisé de DNS Dynamique, les services WINS ont été arrêtés.

5.3.3 NTP

La ville de Marseille dispose d'une architecture NTP se synchronisant sur le temps Internet et garantissant la synchronisation des horloges de l'ensemble des systèmes.

Il conviendra au candidat de prévoir de configurer l'ensemble de ses systèmes sur l'architecture NTP afin de garantir l'exécution synchroniser des traitements et l'exactitude des horodatages des logs.

5.4 Services d'authentification et d'annuaire

5.4.1 Active Directory

La Ville de Marseille dispose d'une architecture de domaine Windows basé sur Active Directory. Elle est composée d'une hiérarchie à 3 domaines dans une forêt unique :

- Un domaine racine : mars
- Deux domaines enfants :
  - vdm, annuaire des utilisateurs de la VDM,
  - bmvr, annuaire des utilisateurs de la Bibliothèque Municipale à Vocation Régionale

Les annuaires Active Directory (AD) contiennent les utilisateurs et les groupes utilisés par l'infrastructure Windows et les services consommateurs :

- Vérification des ouvertures de session Windows,
- Gestion des droits NTFS sur les serveurs de fichiers,
- Authentification des applications basées sur Activie Directory,
- Infrastructure Citrix XenApp 6.5

Les niveaux fonctionnels de la forêt et de tous les domaines (mars, vdm.mars et bmvr.mars) sont en ***Windows Server 2008.***

Produit utilisé	**Domaine Windows** Microsoft Windows Server 2008

Recommandations	L'authentification et l'accès l'application doivent s'appuyer sur les annuaires utilisateurs existants. La gestion des droits d'accès à l'application devra être implémentée dans le REFERENTIEL ACTEURS.

Evolutions en cours	En raison d'évolution organisationnelle, l'architecture Active Directory va faire l'objet, en 2016, d'une restructuration. Toutes les ressources (utilisateurs, groupes, Ordinateurs et GPO) du domaine BMVR vont être migrées vers le domaine VDM. Au terme de cette opération, le domaine BMVR sera supprimé.

5.4.2 LDAP Oracle Directory Server

La Ville de Marseille dispose d'un annuaire utilisateurs, rassemblant toutes les personnes accédant à son système d'information (agents, prestataires, partenaires, etc.).

Cet annuaire d'entreprise, basé sur le standard LDAPv3, rassemble l'ensemble des comptes utilisateurs des différents domaines Active Directory (7500 utilisateurs), les groupes (1500).

Cet annuaire est utilisé pour :

- La messagerie (attributs spécifiques),
- Le contrôle d'accès aux applications intranet,
- L'authentification sur le proxy Internet

Le provisionning (création, suppression, modification) des utilisateurs, des droits d'accès, etc. est assuré par un produit spécifique développé par la VDM.
Il fournit des capacités de workflow pour la validation des demandes. Il fournit également une interface utilisateur permettant à l'agent de gérer son compte et notamment effectuer une modification de son mot de passe.

Le provisionning des groupes est assuré aussi par un développement spécifique.

Produits utilisés	**Annuaire LDAP** Oracle Directory Server Entreprise Edition 7.0 (DSEE) **Synchronisation DSEE / AD** Oracle Identity Synchronization for Windows 6.0 SP1 (ISW) **Provisionning des groupes** RFS (développement spécifique) basé sur COGNITUM Calendra Directory Manager **Provisionning des utilisateurs et droits d'accès** RFA (développement spécifique Java)

Recommandations	L'authentification et l'accès l'application doivent s'appuyer sur les annuaires utilisateurs existants. La gestion des droits d'accès à l'application devra être implémentée dans le REFERENTIEL ACTEURS.

Evolutions en cours	Lors du 2T 2016, la solution Directory Server EE va faire l'objet d'une mise à niveau vers la version 11.1.1.7. Les produits DSEE et ISW étant arrêtés par ORACLE, ils seront par la suite remplacés respectivement par ORACLE Unified Directory 11 (OUD) et Oracle Directory Integration Platform 11 (ODIP). Cette évolution ne pourra avoir lieu qu'à l'issue de la déclaration officielle d'ORACLE du support du produit Communication Suite sur l'annuaire OUD.

5.4.3 Authentification unique (Single Sign On Web)

La Ville de Marseille est en train de mettre en service un composant permettant la mise en place de l'authentification unique pour les applications Web.
Il s'agit de l'application « Central Authentification Server » (CAS Jasig, http://www.jasig.org/cas) en mode HTTPS qui s'appuie sur l'annuaire LDAP de la Ville.

5.5 Services de stockage et de fichiers

La Ville de Marseille dispose dans ses datacenters de plusieurs baies de disques permettant le stockage des données volumineuses.

L'infrastructure de stockage, permet de fournir du stockage à des serveurs, à l'infrastructure virtuelle et aux utilisateurs à travers d'un SAN (FiberChanel, SATA) en mode bloc ainsi que d'un NAS en mode fichiers.

Le service de fichiers NAS est assuré par deux clusters ISILON de 4 nœuds. Il y a un cluster sur chacun des deux datacenters de production. Ceux-ci permettent de délivrer les données à travers les protocoles SMB, NFS et FTP.

Le service de fichiers fournit les fichiers personnels des utilisateurs, les fichiers partagés ainsi que les fichiers gérés et manipulés par des applications, qui sont alors structurés par dossiers applicatifs dédiés.

Les services de stockage et de fichiers disposent de la capacité à répliquer une partie de leur stockage entre les deux datacenters, snapshot, etc. Ces services de réplication et de snapshot sont variables en fonction du niveau de l'offre de service.

5.6 Services de virtualisation

La Ville de Marseille a mis en œuvre un service de virtualisation pour ses infrastructures serveurs, celui-ci s'appuie sur la technologie de Vmware vSphere.
Ce service est réparti sur les deux datacenters avec deux vCenter assurant la gestion de la solution de virtualisation. Un ensemble d'hôtes vSphere en cluster assurent l'hébergement des serveurs virtuels (VM) pour les environnements de développement, d'intégration, de validation et de production.

Le service de virtualisation permet d'accueillir des serveurs Windows, Linux, Mac ou des appliances virtuelles compatibles. Il est à noter que nous sommes en capacité à gérer des VM au format OVF (Open Virtual Machine).

Les serveurs virtuels consomment des ressources de l'hôte vSphere tel que la vRAM, la vCPU et du vDISK. Ces ressources sont configurées à la création de VM en fonction des besoins nécessaires et dans les limites des ressources disponibles.

Le service de virtualisation permet d'une part d'assurer la disponibilité des VM par un redémarrage de celles-ci sur un autre membre vSphere du cluster en cas de défaillance, et d'autre part de faire des spnashots des VM.

5.7 Messagerie

La Ville de Marseille est dotée d'un service de messagerie électronique déployé sur ces infrastructures propres. Il s'agit d'une messagerie s'appuyant sur les standards de l'internet POP3 / IMAP4 / SMTP.

Par défaut, un utilisateur dispose d'un quota de 1 Go sur le serveur pour le stockage des messages dans sa boite aux lettres.

Les échanges de messages font l'objet de règles précises :

- La taille d'un message est limité à 20 Mo,
- Les pièces jointes ne peuvent faire plus de 20 Mo,
- Les pièces jointes ne peuvent pas contenir plus de 500 pièces jointes après décompression,
- Une pièce jointe décompressée ne doit pas dépasser 40 Mo pour les échanges internes et 80 Mo pour les échanges vers l'externe.

Les envois de message par une application via le protocole SMTP doivent respecter la norme RFC821.

Les envois de messages (effectués par un utilisateur ou par une application) sont réalisés via des frontaux SMTP Antivirus et antispam. L'échange entre le réseau VDM et l'extérieur est assuré également par des passerelles antivirus, antispam placées en DMZ publique.

La messagerie est accessible par un client Webmail de type AJAX nommé CONVERGENCE, client de messagerie unifiée d'Oracle.

Pour les accès extérieurs (essentiellement depuis la flotte de « smartphones »), le protocole IMAP(S) et SMTP(S) authentifié sont exposés sur l'internet via une passerelle Proxy, elle aussi en « DMZ Publique ».

Produits utilisés	**Serveur de messagerie** ORACLE Unified Communication Suite 7u1 / Module Messaging Server 7u4 (anciennement SUN Java System Communication Suite 7) **Passerelles SMTP antivirus/antispam** Appliance McAfee Secure Content Management

Recommandations	Le protocole d'accès aux boites aux lettres doit être IMAPS et SMTPS Authentifié. L'usage du protocole POP ne sera réservé qu'au cas particulier le nécessitant et justifié. Dans le cas où une application nécessiterait l'utilisation du service de messagerie, il sera nécessaire d'évaluer le nombres de messages échangés par jour ainsi que leur taille et de déterminé le trafic généré.

Evolutions en cours	L'éradication des boites aux lettres de type POP est en cours et devrait être achevée 2T 2016 pour que l'ensemble des BAL soient de type IMAP. Courant 2016, l'ensemble de la solution va faire l'objet d'une mise à niveau vers la version 8.01. L'infrastructure va être renforcée mais les services resteront identiques.

5.8 Agenda partagé

La Ville de Marseille dispose d'un agenda partagé permettant aux agents de gérer leur emploi du temps et de monter des réunions en invitant les participants. L'agenda partagé permet de voir et de trouver automatiquement les disponibilités communes.

L'accès à l'agenda partagé depuis l'extérieur est possible au travers du Client web Meeting Maker publié sur la passerelle SSL ou pour les appareils mobiles au travers d'une passerelle Active Sync.

Produits utilisés	**Serveur d'agenda** People Cube Meeting Maker 8.1 Passerelle Active Sync **NOTIFYLink Enterprise Server 4.8.2**

Recommandations	Si une application souhaite s'appuyer sur le service d'agenda partagé pour générer des invitations, il sera nécessaire de faire une étude préalable pour garantir la faisabilité.

Evolutions en cours	Suite au rachat par la société ASURESOFTWARE, le produit Meeting Maker ne fait plus parti de la gamme de produit de l'éditeur et son développement est abandonné. La Ville de Marseille a décidé de migrer son service d'agenda partagé vers le produit ORACLE Communication Suite / Module Calendar Server 8. Ce produit s'appuie sur le protocole standard CalDAV. Calendar Server s'appuie également sur le client Web unifié Oracle Convergence.

6. POSTE DE TRAVAIL

6.1 Les Systèmes d'Exploitations utilisés à la Ville de Marseille

Les postes de travail représentent plus de 5000 machines.

6.1.1 Les différents OS

Environnements PC représentant 72 % du parc
- XP SP 3
- Windows Seven

Environnement MAC représentant 28 % du parc
- X.5
- X.6
- X.8

6.1.2 La composition du parc

88 % de postes à usage bureautique
10 % de portables
2 % de postes graphiques

6.2 Les Services Bureautique

6.2.1 Messagerie

Aujourd'hui, 75 % des postes utilisent le protocole IMAP. Une migration est en cours pour les postes utilisant encore le protocole POP.

6.2.2 Agenda Partagé

Deux modes d'accès :
- client lourd installé sur le poste de travail
- interface web

6.2.3 Autres services du poste de travail

Le poste de travail est configuré avec :
- la suite bureautique « LibreOffice » version 3.6.5.2
- la suite bureautique « Microsoft Office » (si indispensable)
- le navigateur web « Firefox » version 17.0.3 ESR
- le client de messagerie « Thunderbird » version 17.0.3 ESR
- un outil de décompression (PC 7zip 9.2 / Apple BOM Archiver pour Mac)
- un outil de sauvegarde (Cobian 11 / Foldersynchroniser 3.6.3 pour Mac)
- un lecteur multimédia (VLC 2.0.5 pour PC, VLC 2.0.6 pour Mac)
- un outil de prise de main à distance (Timbuktu 7 (XP, X.5, X.6) et Teamwiever 7 (Seven, X.8)
- un outil de gravure (Infrarecorder 053 pour PC et LiquidCD pour Mac X.5, X.6)
- un outil de gestion de parc et de télé-déploiement (OCS 2.0.5.0 pour PC, OCS 2.0.3 pour Mac)
- un lecteur pdf (Acrobat 11.02 pour PC et Aperçu 6.0.1 pour Mac)
- une machine virtuelle Java 1.6.0.27 pour PC et Java 1.6.0.43 pour Mac
- un antivirus Symantec 12
- des modules complémentaires comme Adobe Flash 11.6 et NetframeWork 4.0.30319 pour PC

7. EXPLOITATION

Les sous-chapitres suivants décrivent les principales caractéristiques des solutions utilisées par la Ville de Marseille pour assurer l'exploitation de son Système d'Information.

7.1 Ordonnancement / Lancement des traitements différés

La Ville de Marseille ne dispose pas à ce jour d'ordonnanceur permettant de gérer de manière centralisée l'ensemble des traitements différés de ses applications.

Aujourd'hui, les traitements différés sont programmés en utilisant des schedulers internes aux serveurs qui hébergent les applications (« cron » pour les environnements Linux et « at » pour les environnements Windows).

Par contre, s'il s'agit de traitements Oracle, la Ville de Marseille utilise l'outil Grid pour leur planification.

L'automatisation de l'exécution des traitements (batchs, interfaces...) doit être possible au travers d'un ordonnanceur intégré à la solution proposée. Les manipulations humaines se réduisent au traitement des incidents (supervision, analyse des causes, correction, suivi). L'intervention des services opérationnels se restreint donc à une surveillance périodique des alertes générées par ces traitements.
Les traitements pourront être déclenchés de la façon suivante :

- automatiquement après une action donnée,
- automatiquement suite à un feu vert de la part des utilisateurs,
- planifiés à des jours et heures précis.

En cas d'incident, d'anomalie, ou de choix de l'exploitant, un déclenchement manuel est possible. Ce déclenchement peut être réalisé par des administrateurs fonctionnels et ce, sans avoir recours à des administrateurs techniques.
Au delà de la génération d'un fichier de données, la solution proposée doit fournir un journal d'exécution permettant la surveillance des traitements.
En fin de traitement, des messages d'alertes devront être générés dans ce journal d'exécution, à destination des administrateurs ou des référents de l'application source mais également de l'application cible. Ces messages permettront de déclencher des actions manuelles nécessaires à la bonne fin et validation de l'interface. Ces actions pourront être des contrôles, du paramétrage, des saisies complémentaires ou un simple accusé de réception. Les supports de communication de l'alerte peuvent être divers : mail, SMS, flux RSS, etc...

7.2 Sauvegardes

Le Système d'Information de la Ville de Marseille s'appuie sur l'outil de sauvegarde centralisée Netbackup v6.5 de chez Symantec / Véritas.
Tout nouveau serveur Linux ou Windows est intégré à la sauvegarde centralisée grâce à l'agent Netbackup.
La stratégie de sauvegarde des données se résume ainsi : la solution Netbackup centralise les sauvegardes pour tous les serveurs qui sont sur le réseau Gigabit, la période de rétention est de 15 jours pour tous les fichiers, les sauvegardes se font entre 19h00 et 6h00 sur deux sites différents (sauvegardes croisées), pour les bases de données Oracle, les sauvegardes peuvent se faire à chaud pour les applications nécessitant une disponibilité étendue (agent Netbackup RMAN), toutes les nuits, les serveurs sont sauvegardés en différentiel (1 To) et tous les week-end les serveurs sont sauvegardés en « Full » (18 To).

7.3 Supervision / Monitoring

La supervision du bon fonctionnement des applications s'effectue principalement à deux niveaux :

- la supervision matérielle,
- la supervision applicative.

7.3.1 Supervision matérielle

Tous les éléments actifs du réseau sont supervisés via l'outil HP NNM qui consolide l'état de l'ensemble des équipements actifs sur une et une seule console de supervision.

Le monitoring temps réel des flux réseaux sur nos principaux nœuds est effectué avec la solution CACTI.

La supervision matérielle des serveurs s'effectue avec la solution Nagios qui nous permet d'avoir une cartographie temps réel de l'état de nos matériels serveurs IBM et HP. Le protocole SNMP natif est retenu pour l'ensemble des autres constructeurs sachant que le détail des MIB remontées doit être fourni. Les matériels intégrés devront communiquer des alertes SNMP conformes à la norme RFC1157.

7.3.2 Supervision applicative

Deux approches complémentaires nous permettent de superviser le bon fonctionnement en temps réel d'une application :

- la première consiste à tester la disponibilité de chacun des maillons qui constituent la chaîne de l'application (réseau, serveur de présentation, serveur de traitement, serveur de base de données). Ces différents tests sont effectués à travers l'outil NAGIOS.
- la seconde consiste à disposer d'une transaction de test que l'on joue à intervalles réguliers pour simuler la position « end-user ». La transaction de test qui peut se traduire par une url en entrée et un code retour en sortie sera fournie par le titulaire de marché. Ces tests sont aussi joués sur l'outil NAGIOS.

Les modalités détaillées de mise en œuvre sont fixées avec les services techniques de la Ville de Marseille pendant la phase d'installation.

Le titulaire du marché doit s'exprimer sur la compatibilité de son produit avec les solutions de supervision actuelles ou à défaut doit proposer une solution de supervision dédiée.

7.4 Editique

La Ville de Marseille dispose aujourd'hui d'imprimantes Xerox. Ces imprimantes permettent d'imprimer sur les formats A5, A4 et A3, en noir & blanc comme en couleur. L'assemblage peut être fait automatiquement par simple agrafage ou par encollage (jusqu'à 250 feuilles).

Les impressions peuvent également être mises sous pli automatiquement dans des enveloppes à fenêtre. Un système de code barre sur les impressions permet de regrouper plusieurs feuilles dans la même enveloppe.

L'équipe Editique de la Ville gère également les pré-imprimés. Un mécanisme d'attente se déclenche pour qu'un opérateur introduise le bon type de papier avant le lancement de l'impression. Il est également possible d'insérer des documents dans des magasins spécialisés et de demander leur insertion automatique dans un autre document.

7.4.1 Formats de fichiers acceptés

Il est possible de transmettre les formats suivants aux imprimantes :

- POSTSCRIPT,
- PDF,
- DOC,
- ODT,
- RTF.

Les documents sont transmis automatiquement sur les files d'attente du serveur sur une combinaison d'adresse IP et de port.

7.4.2 Serveurs d'impressions et files d'attentes

Des files d'attente peuvent être créés pour diriger les impressions sur les imprimantes locales ou sur le serveur d'impression de la DINSI, en fonction de différents critères :

- le volume du document,
- le type de document,

- le nombre d'exemplaires, etc.
- Par exemple les documents imprimés en 200 exemplaires seront routés vers l'infrastructure d'impression en masse, plutôt que vers une imprimante locale.
  La solution du titulaire doit permettre d'analyser le volume à éditer et proposer soit l'édition locale soit l'édition sur le serveur de la DINSI.

Des files d'attentes d'impression peuvent porter des règles de transformation, de composition ou de routage.
Voici des exemples :
• Plusieurs PDF peuvent être fusionnés avec les documents envoyés sur la file et imprimés. De cette manière on peut par exemple ajouter le logo de la Ville sur tous les documents. Cette solution a deux avantages :
• inutile de modifier les rapports standards de la solution,
• légèreté du rapport qui ne comporte pas le logo, qui peut être très lourd pour obtenir une bonne qualité d'impression.
À noter que ce logo est enregistré dans la mémoire physique de l'imprimante dédiée. Il n'est ni sur le serveur, ni dans la file d'attente.

Le candidat proposera une solution adaptée au besoin.

A Noter : L'impression recto-verso d'un document PDF pose un léger problème technique: Les méta-données dans un documents PDF ne permettent pas d'indiquer le type d'impression nécessaire : recto simple ou recto-verso. Des solutions de contournement sont possibles.

7.4.3 Composition

La Ville de Marseille prospecte actuellement pour la mise en place d'une solution de composition.

8. SÉCURITÉ

8.1 Infrastructure

8.1.1 Antivirus / Analyse de contenu

Pour le filtrage des flux de messagerie, la Ville de Marseille utilise des « Appliances ». Les postes et les serveurs sont équipés d'une solution antivirale.

8.1.2 FireWall

Un cluster de FireWall est positionné sur le lien Internet. Un autre cluster de Firewall est positionné en interne, il fédère un certain nombre de segments sécurisés entre lesquels il assure des fonctions de filtrage et de détection / prévention d'intrusion.

8.1.3 Filtrage d'URL

Deux « Appliances », intégrant un moteur de filtrage Web, positionnés dans un segment sécurisé lié au cluster de Firewall, assurent le filtrage d'URL en tant que proxy « transparent » afin d'éviter que les utilisateurs naviguent sur des sites catégorisés comme illicites au regard de la loi (pédophilie, drogue, armement ...).

Chaque utilisateur est contraint à se signer pour sortir sur Internet (couple login/password de l'annuaire LDAP).

De plus, afin de préserver la bande passante, les flux importants sont filtrés (audio, vidéo ...) et soumis à autorisation.

8.1.4 Filtrage protocolaire & QoS

Une Appliance fait du filtrage protocolaire et de la gestion de la QoS sur les flux Internet.

8.1.5 Passerelle SSL

Une Appliance assure le service d'accès SSL. Cette passerelle agit en tant qu'intermédiaire entre des postes clients « externes » et des applications Ville de Marseille.

De ce fait, les prestataires d'applications ayant besoin de cet accès, devront appliquer les normes fournies par le constructeur de celle-ci.

8.1.6 Accès en télémaintenance

Quand la possibilité de télémaintenance est inscrite dans le cadre de la consultation, les accès en télémaintenance se font via une connexion VPN SSL dont les caractéristiques seront fournies par la Ville de Marseille.

Le télé-mainteneur devra s'engager à respecter une charte qui lui sera fournie et qui sera soumise à signature.

8.1.7 Anonymisation des données

La Ville de Marseille dispose d'un utilitaire qui permet de rendre anonyme les jeux d'essais des données de production.

8.1.8 Sécurisation des communications

Toutes les communications qui doivent véhiculer des informations personnelles, sensibles ou des authentifications/identifications, doivent être chiffrées.

8.1.9 Sonde de prévention d'intrusion

Tous les flux de données inter-segments sont analysés par le firewall interne. S'ils contiennent du trafic malveillant ou du trafic ne respectant pas les normes, les paquets sont purement et simplement rejetés et la connexion fermée. Ceci afin de parer à toute attaque, quelque soit la couche visée.

8.1.10 Extranet authentifié et Extranet public

La ville de Marseille dispose de 2 moyens de publier des ressources :

- un Extranet dit « Authentifié » qui, après authentification sur une passerelle SSL, permet l'accès à la ressource Web. Les accès aux ressources dépendent des droits des utilisateurs authentifiés, ce qui permet une maîtrise complète de la chaîne de données,
- un Extranet dit « Public » qui permet l'accès, par l'intermédiaire de relais filtrants, à des ressources de manière non authentifiée . Ceci permet d'optimiser la ressource qui doit être fournie, avec une analyse et un filtrage intermédiaire non dépendant du produit publiant la

ressource.

8.1.11 Bonnes pratiques

Afin de garantir une sécurité à tous les niveaux, il est demandé que les règles suivantes soient scrupuleusement suivies lors du développement d'applications. Ces règles, si elles sont prises en compte en amont de projet, ne sont que peu contraignantes.
La Ville de Marseille se réserve le droit de contrôler le bon respect des règles suivantes par les audits ponctuels.

Les bonnes pratiques édictées par l'OWASP (Open Web Application Security Projet https://www.owasp.org/) sont la référence à respecter, selon laquelle la Ville de Marseille se réserve le droit d'auditer les solutions déployées sur son système d'information.

8.1.11.1 Simplicité, traçabilité et gestion de version du code

Un code simple est toujours plus facile à maintenir et à sécuriser qu'un code complexe. La complexité est l'ennemie de la sécurité et de la capacité à évoluer.
Par exemple, il est inutile de ré-inventer des algorithmes de chiffrement alors que des standards, tels que AES, existent, de même pour l'échange de clefs avec Diffie-Hellman.

8.1.11.2 Validation des données en entrées

Toutes les données venant de l'extérieur d'une application et plus généralement d'une fonction doivent être normalisées, analysées et épurées. C'est à dire qu'aucune confiance ne doit être faite par la couche présentation et applicative sur le contenu et la bonne validité des données lui étant envoyées.
Par exemple :

- un champ recevant un mail ne devra que contenir des caractères valides et respecter la RFC 53221 (taille, casse ...),
- un nombre ne peut être constitué que des caractères 0 à 9 et du signe ',' et peut être précédé du signe + ou -. Il sera en plus borné (longueur et valeur).

Toute donnée non conforme à l'attendu, devra être rejeté avec un message d'erreur conforme et explicite ou simplement non pris en compte. Il ne doit pas faire l'objet d'une évaluation et/ou consommation par l'application.

8.1.11.3 Validation des données en sortie

De même que précédemment, les données envoyées à l'utilisateur doivent être analysées et encodées pour quelles ne puissent pas être interprétées par le navigateur comme du code HTML, javascript ou autre lorsque cela n'est pas nécessaire.

8.1.11.4 Normalisation des messages d'erreurs

Les messages d'erreurs ne doivent pas donner d'information autre que le fait qu'il y a eu une erreur. En particulier les messages d'erreur de débogage ne doivent jamais être visibles et accessibles par les utilisateurs. Ils doivent respecter la règle : « toute information qui n'est pas utile pour le quidam, ne doit pas être donnée ». Les messages de débogage sont envoyés vers un fichier et non vers l'utilisateur.

8.1.11.5 Authentification et autorisations

Si des mécanismes d'authentification forte n'ont pas été mis en œuvre dans une application, un attaquant peut accéder à ses contenus sensibles sans avoir à s'authentifier.
Il faut instaurer des règles simples telles que :

- appliquer la politique de mot de passe définie par la Ville de Marseille,
- mettre en œuvre un délai après un échec d'authentification, afin d'éviter les attaques par force brute,
- ne pas utiliser des CAPTCHA trop simples,
- protéger les accréditations lors du transit :
- chiffrer les données entre le client et le serveur,

- ne pas envoyer le mot de passe au serveur mais une empreinte du mot de passe (MD5, SHA1 ...),
- définir des rôles et des niveau d'accréditations dans les applications.
- Désactiver la possibilité de stocker le mot de passe dans la base locale du navigateur.

Ces règles ne sont pas exhaustives, mais donnent une orientation dans laquelle il faut se diriger.

8.1.11.6 Gestion des sessions et des cookies

Les sessions et le contenu des cookies, ont des identifiants non prédictibles et doivent intégrer au minimum l'adresse IP du client, un aléa, un secret et un paramètre dépendant de la date et de l'heure. Ceci afin de permettre une impossibilité de rejeux de l'identification tout en gardant une validité dans le temps. La base de temps ne sera pas celle du client, mais uniquement celle du serveur.

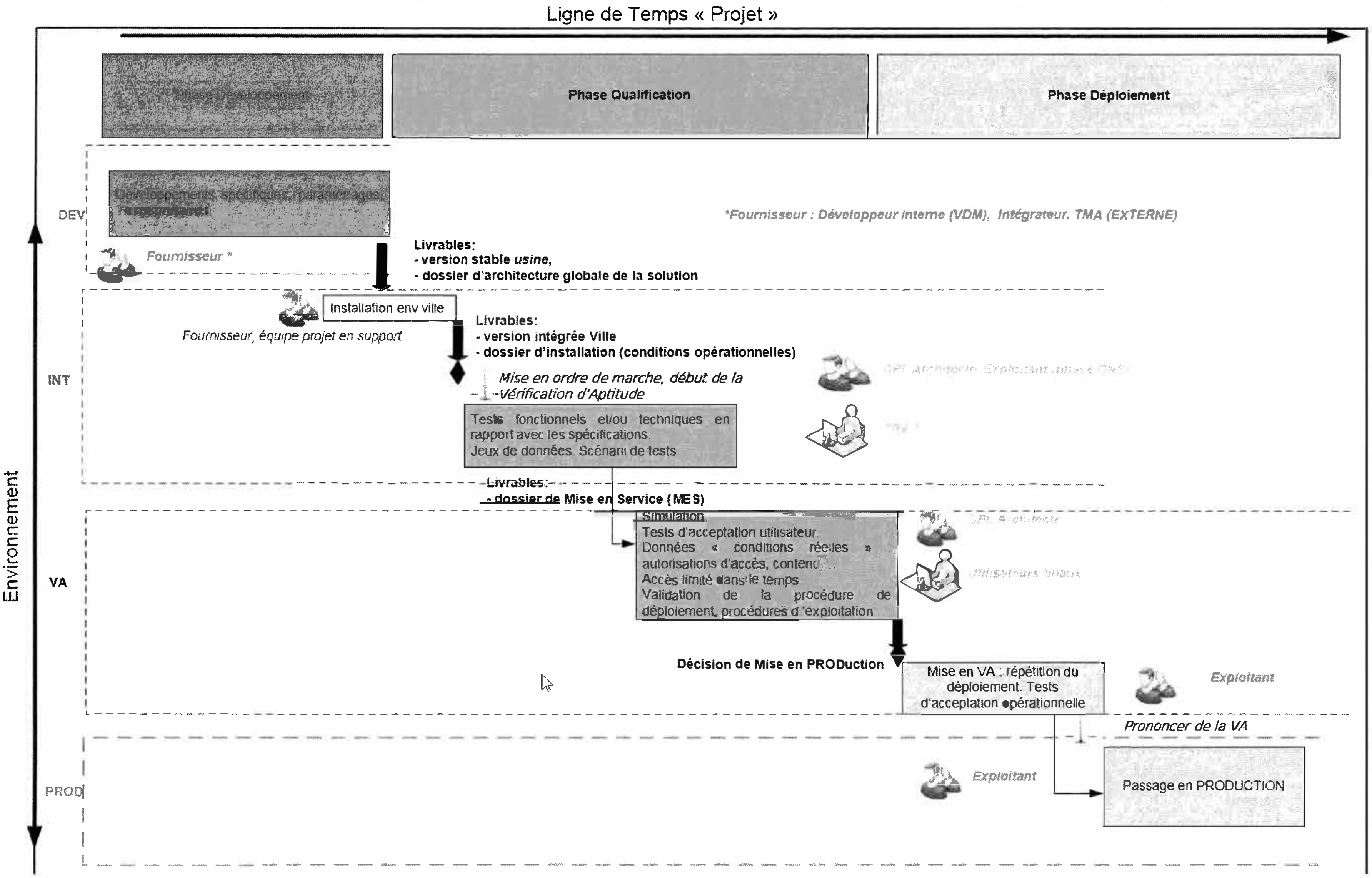
9. CADRE MÉTHODOLOGIQUE DE DÉPLOIEMENT

L'objet de ce paragraphe est de présenter le cadre méthodologique en vigueur au sein de la DINSI, dans lequel l'intégrateur devra s'inscrire.

9.1 Activités / environnements au sein des infrastructures DINSI

L'intégration d'une solution dans le systèmes d'informations de la Ville de Marseille, nécessite l'alignement d'infrastructures sur des activités du cycle de vie du projet.

Le schéma ci-après représente la cas nominal (selon la règle des 80/20). Tout besoin complémentaire devra être motivé pour arbitrage, dans le cadre du projet.



Ligne de Temps « Projet »
Phase Développement
Phase Qualification
Phase Déploiement
DEV
Développements spécifiques, paramétrages
*Fournisseur : Développeur interne (VDM), Intégrateur, TMA (EXTERNE)
Fournisseur *
Livrables:
- version stable usine,
- dossier d'architecture globale de la solution
Installation env ville
Fournisseur, équipe projet en support
Livrables:
- version intégrée Ville
- dossier d'installation (conditions opérationnelles)
INT
Mise en ordre de marche, début de la Vérification d'Aptitude
Tests fonctionnels et/ou techniques en rapport avec les spécifications.
Jeux de données. Scénarii de tests
Environnement
Livrables:
- dossier de Mise en Service (MES)
Simulation
Tests d'acceptation utilisateur.
Données « conditions réelles » autorisations d'accès, contenu...
Accès limité dans le temps.
Validation de la procédure de déploiement, procédures d 'exploitation
VA
Décision de Mise en PRODuction
Mise en VA : répétition du déploiement. Tests d'acceptation opérationnelle
Exploitant
Prononcer de la VA
PROD
Exploitant
Passage en PRODUCTION

9.1.1 La phase de développement

Par développeur on entend ici
- un développeur interne DINSI
- un intégrateur : progiciel , développements spécifiques à qui la Ville fournit une infrastructure de développement pour être dans une configuration au plus proche de la cible (poste de travail, base de données, serveur d'application etc ...).
- un mainteneur : TMA

Ces activités sont effectuées, si nécessaire, sur un ***environnement de DEVeloppement***, sur la base de jeux de données unitaires.

A l'issue des tests unitaires concluants, réalisés par les développeurs, une version figée est livrée pour intégration dans le SI Ville de Marseille.

9.1.2 La phase de qualification

C'est une phase de qualification qui fait intervenir :
- ➔ l'équipe projet : chef de projet informatique, chef de projet utilisateur, architecte technique
- ➔ l'exploitant
- ➔ tierce recette applicative (éventuellement)

L'architecte et l'exploitant interviennent dans le cas de la mise au point de nouveaux système.
L'exploitant, intervient seul dans le cas des mises en services sur l'environnement de VA.

Les environnements associés sont :

L'***environnement d'INTégration*** fait l'objet des tests suivants :
tests d'intégration : tests fonctionnels et/ou techniques en rapport avec les spécifications. Ces tests sont effectués sur des jeux de données, des scénarios sont enregistrés et rejoués au besoin.

tests système :
tests d'interfaces matériels et logiciels, tests de services : performance, stress, reprise, robustesse

Le déploiement est effectué par le développeur avec le support du chef de projet (SDEV) et de l'architecte technique (AT).

Les livrables de cette étape sont :
- une solution opérationnelle
- la documentation de déploiement en condition opérationnelle consolidée avec le chef de projet et l'architecte technique.

Le développeur prononce alors la mise en ordre de marche. C'est le début de la période de Vérification d'Aptitude.

L'***environnement de VA***

C'est un environnement destiné à une activité de simulation ; cet environnement fait l'objet d'une configuration proche de la production : données manipulées, droits des utilisateurs.

Cet environnement permet d'effectuer
les tests d'acceptation utilisateur :
- reprise de données, tests de complétude, tests de traitement de masse,
- les corrections de bug suite à incident de production ...

les tests système : tests de déploiement (documentation) tests d'interfaces matériels et logiciels, test d'administration, tests de services : performance, stress, reprise, robustesse

Cet environnement, usuellement non accessible par l'équipe projet, est mis à disposition suite à validation du circuit hiérarchique, pour une durée limitée dans le temps.

L'équipe projet aura indiqué au préalable les ressources auxquelles elle doit avoir accès (base de données, serveur d'application etc ...).

On distingue ici deux cas usuels :

- cas n°1 : application en maintenance
dans ce cas, le besoin d'ouverture de l'environnement de VA, sur de la donnée de production concerne essentiellement la correction de bug. Cette ouverture est alors très ponctuelle et le travail d'analyse est effectuée entre équipe projet du SDEV et l'exploitant.

- cas n°2 : nouvelle application ou nouvelle version d'application en maintenance
Ici la période d'ouverture de l'environnement de VA pourra être plus longue.

Dans les deux cas, il peut s'avérer nécessaire de procéder à plusieurs déploiements sur l'environnement de VA (mise en service) dans des délais très courts (ex : tests utilisateurs finaux / bug décelé et corrigé aussitôt / redéploiement) ; l'équipe projet planifie donc la phase de tests nécessitant cet environnement , en informe l'exploitant et celui-ci se rend disponible pour assurer les différents déploiements.

Au besoin, d'autres environnements peuvent être mis à disposition à ce stade du projet dans des cas spécifiques où l'équipe projet a besoin de qualifier des modules indépendants nécessitants une stabilité des données manipulées.

A l'issue des tests concluants, l'équipe projet décide que la version du produit a vocation à passer en production. Elle sollicite alors le service EXPloitation pour un déploiement.

9.1.3 La phase déploiement

Elle permet à l'exploitant de prendre le projet en main.
Elle s'effectue en deux temps :
- la mise en VA : elle permet de valider la documentation de déploiement, les procédures d'exploitation, la complétude technique, les tests de charge

- la mise en PROD : c'est l 'étape ultime.

9.2 Livrables

Le fournisseur devra livrer l'ensemble des documents permettant la compréhension, l'installation et l'exploitation de la solution.

Cette documentation prendra la forme suivante :

- Schéma d'architecture : schéma représentant les ressources virtuelles, les différents composants logiciels, les flux d'échanges, les ports accédés, ...
  et de manière générale ***toutes les informations utiles permettant de décrire le fonctionnement et les composants techniques mis en œuvre dans la solution***.

- Dossier d'installation : comme décrit précédemment, il s'agit de l'ensemble des procédures d'installation et de paramétrage permettant de reconstruire dans l'intégralité la solution en condition opérationnelle.

- Dossier d'exploitation : il s'agit de l'ensemble des opérations qui doivent, d'une part être réalisées de manière périodique (journalière, hebdomadairement, mensuellement, etc.) pour garantir la continuité du bon fonctionnement et d'autres part l'ensemble des procédures élémentaires nécessaires à l'exploitation de la solution (arrêt, redémarrage, réinitialisation, etc).
  Le dossier comprendra également les procédures de sauvegarde et de restauration permettant de garantir l'intégrité de l'application en cas de restauration.

- Dossier de supervision : il décrit l'ensemble des composants techniques et fonctionnels qui doivent être surveillés par l'exploitant hébergeur pour vérifier l'état de bon fonctionnement de la solution

- Dossier matériel (optionnel, uniquement dans le cas où du matériel additionnel est nécessaire):
  - fournir les caractéristiques du matériel sur lequel tourne la solution (caractéristiques techniques, idéalement fournir une copie de la facture)
  - fournir la documentation pour réinstaller la solution en cas de changement de matériel (ex : IPAD cassé et changé)

10. RÉCAPITULATIF DES EXIGENCES

Code	***Libellé***	***Obligatoire / Optionnel***
Architecture fonctionnelle		
EXI-ARCHFONC-01	La solution devra être interfacée avec l'annuaire LDAP pour la gestion des accès à l'application : vérification de l'existence de l'utilisateur et vérification de l'appartenance au(x) groupes autorisant l'accès.	Obligatoire
EXI-ARCHFONC-02	La solution doit permettre la délégation de pouvoir dans les workflow	Obligatoire
EXI-ARCHFONC-03	La solution doit utiliser le webscript de dépôt de la Ville de Marseille pour les actions de dépôt et mise à jour des contenus.	Obligatoire
EXI-ARCHFONC-04	La solution doit utiliser l'api RESTFul CMIS exposée par Alfresco pour toute autre communication avec la plate-forme GED, sauf pour les types de communication non couverts par cette API.	Obligatoire
EXI-ARCHFONC-05	La solution doit gérer fonctionnellement l'identité numérique du document et la stocker au niveau applicatif.	Obligatoire
EXI-ARCHFONC-06	La solution consommant un service de signature électronique devra utiliser l'infrastructure en place dans le SI Ville de Marseille.	Obligatoire
EXI-ARCHFONC-07	La solution doit exposer un service permettant de remonter de l'information au niveau de la corbeille de tâches générale de l'agent.	Optionnel
EXI-ARCHFONC-08	Les flux de données structurées ayant une composante géométrique sont produits au format GeoJSON	Obligatoire
Architecture de développement		
EXI-ARCHDEV-01	Tout composant (application, module) déployée dans le SI Ville de Marseille doit disposer d'un numéro de version permettant de clairement l'identifier. Ce numéro de version est en particulier renseigné dans un fichier version.txt systématiquement mis à disposition avec un livrable applicatif.	Obligatoire
EXI-ARCHDEV-02	Toute application WEB, c'est à dire utilisée au travers d'un navigateur, doit être « Responsive web design » à priori. Un arbitrage spécifique pourra être fait par la Ville de Marseille sous réserve de justifications qu'elle jugera pertinentes lors de la phase d'étude d'intégration de la solution.	Obligatoire sauf arbitrage contraire en phase d'étude d'intégration
EXI-ARCHDEV-03	Les échanges de données entre les applications mobiles et le SI Ville de Marseille se font de façon chiffrée et authentifiée.	Obligatoire
EXI-ARCHDEV-04	Le stockage de données jugées sensible par la Ville de Marseille en phase d'étude d'intégration de la solution, devra être chiffré.	Obligatoire
EXI-ARCHDEV-05	Toute application mobile développée spécifiquement pour la Ville de Marseille doit être mise en œuvre sous forme d'application dite hybride. Un arbitrage spécifique pourra être fait par la Ville de Marseille sous réserve de justifications qu'elle jugera pertinentes lors de la phase d'étude d'intégration de la solution.	Obligatoire sauf arbitrage contraire en phase d'étude d'intégration