

Page 1 of 46	<u>Afpa-CCTG-FRI</u>	Afpa 
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

CCTG-FRI

Cahier des Clauses Techniques Générales pour les marchés de Fourniture et de Réalisation Informatique

Mai 2023

Suivi des versions

Rédacteur / Vérificateur	Date	Version	Statut (Travail / pour validation / applicable)	Objet
DSI/DOP DSI/MCO	10/12/2021	1.0	Applicable	
DSI/Equipe SSI DSI/DOP	10/07/2023	1.1	Applicable	

Suivi des modifications

Version	Date	Objet de l'évolution	Rédacteur(s)	Fonction
1.0	01/12/2022	Création du document	Equipes DSI	DSI/DOP DSI/MCO
1.1	11/05/2023	Transfert des exigences SSI vers le CCTG-SSI Afpa, et changement des références	Equipe SSI	DSI/Equipe SSI

Vérification / Approbation

	Nom	Fonction	Date
Vérification	Mourad ZIRARI	Responsable DSI/DOP	10/07/2023
	Olivier LHERPINIERE	Responsable DSI/DET	10/07/2023
	Florence PATENNE	RSSI	10/07/2023
Approbation	Mourad ZIRARI	Responsable DSI/DOP	10/07/2023
	Olivier LHERPINIERE	Responsable DSI/DET	10/07/2023
	Florence PATENNE	RSSI	10/07/2023

Page 3 of 46	Afpa-CCTG-FRI Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	
Version 1.1		Direction des Systèmes d'Information

Documents de référence

Nom du fichier	Description
CE-DSO	Présentation de la démarche DevSecOps à mettre en place chez l'Afpa et des exigences associées
CCTG-SSI V2.0	Présentation des normes et standards liés à la sécurité

Table des matières

Suivi des versions	2
Suivi des modifications	2
Vérification / Approbation.....	2
Documents de référence	3
1. Préambule	6
1.1. Objet et destinataires du CCTG-FRI	6
1.2. Structure générale du document	7
1.3. Droits et obligations du candidat.....	10
1.4. Droits et obligations du titulaire.....	12
1.5. Livraisons	13
1.6. Fonctionnement.....	14
2. Infrastructures	15
2.1. Datacenter.....	15
2.2. Réseaux	16
2.3. Stockage, sauvegarde et archivage	20
2.4. Serveurs applicatifs et de données, et systèmes d'exploitation	21
2.5. Gestion des systèmes.....	22
2.6. Ressources utilisateurs.....	23
2.7. Services frontaux	27
2.8. Secours informatique	28
2.9. Sécurité	29
3. Middleware	29
4. Développement.....	30
3.1 Architecture applicative	30
3.2 Langages et outillage de développement.....	32
3.2.1. Langage Java	33
3.2.2. Langage PHP	33
3.2.3 Outillage de développement	34
3.3. Réalisation des développements.....	35
3.4. Règles de déploiement	38

Page 5 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

3.5 Supervision applicative	39
4. Annexes	41
4.1. Infrastructure	41
4.2. Développement	44

1. Préambule

1.1. Objet et destinataires du CCTG-FRI

Le CCTG-FRI décline la politique industrielle de l'Afpa.

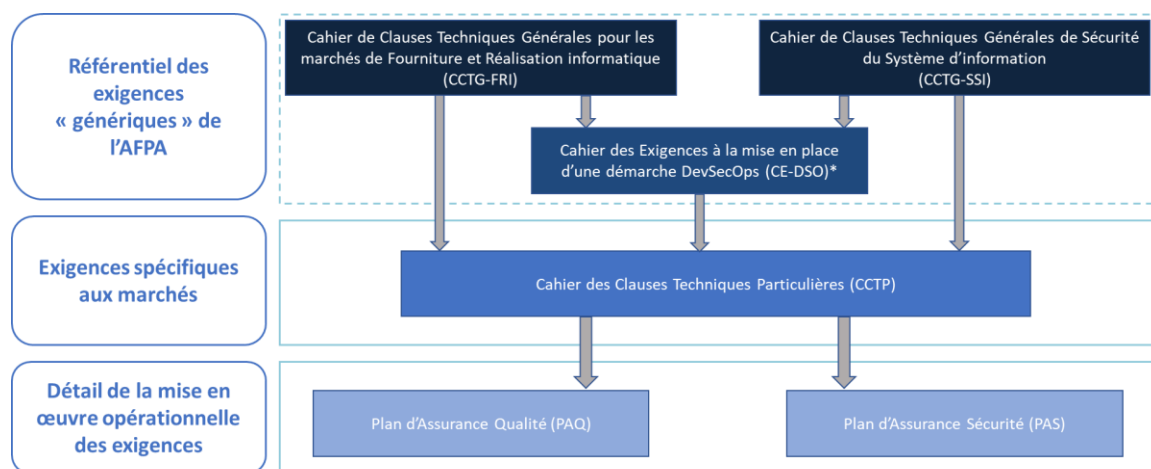
L'Afpa a une **politique industrielle** informatique.

Cette politique industrielle s'attache à **standardiser et industrialiser** les plates-formes et architectures mises en œuvre.

Le **Cahier des Clauses Techniques Générales** pour les marchés de **Fourniture** et de **Réalisation Informatique** (CCTG-FRI) décline cette politique industrielle à court et moyen terme en recensant les outils et technologies homologués par l'Afpa pour la fourniture et la réalisation de ses systèmes d'information.

Dans ce document, le terme **solution** désigne une fourniture ou une réalisation informatique intégrée et mise en œuvre dans le contexte technique de l'Afpa.

Le CCTG-FRI est un document contractuel. Il est annexé au marché de réalisation et s'articule avec les autres documents du marché de la manière suivante :



* Uniquement si la démarche DevSecOps est applicable

Destinataires

Candidats Le CCTG-FRI est d'abord destiné aux **candidats** répondant à une consultation de l'Afpa : intégrateurs de S.I., fournisseurs de logiciels, ...

Il fournit les éléments permettant aux candidats de proposer à l'Afpa la meilleure solution possible :

- La plus adaptée à son besoin,
- Respectant ses exigences.

En particulier, il leur permet de s'assurer de **l'intégration future correcte** de la solution qu'ils proposent dans l'environnement technique de l'Afpa.

Titulaire Le candidat qui remporte le marché passe au statut de **titulaire du Marché**.

1.2. Structure générale du document

Structure en chapitres

Le CCTG-FRI est structuré en chapitres.

La définition de chacun des chapitres se trouve dans le tableau suivant :

	Ce chapitre décrit
<i>INFRASTRUCTURES</i>	Le contexte technique dans lequel la fourniture devra s'intégrer : Datacenter, Réseaux, Stockage, Serveurs et systèmes d'exploitation, Gestion des systèmes, Ressources utilisateurs, Services frontaux, Secours informatique, Sécurité.
<i>MIDDLEWARES</i>	Les principes directeurs formalisés sous forme d'exigences autour des solutions d'intégration.
<i>DEVELOPPEMENT : Principes généraux, règles de réalisation</i>	Les principes d'architecture appliqués pour construire les Systèmes d'Information de l'Afpa. Les normes, les méthodes, et les outils associés qui s'appliquent en matière de développement de logiciel.
<i>ANNEXES</i>	Les exigences en termes de versionning sur le périmètre Infrastructure et Développement

Les paliers

Définition : Palier

On appelle palier un ensemble cohérent de composants intégré et industrialisé (matériel ou logiciel), ce qui garantit sa robustesse pour une utilisation en production. Pour chaque composant, la ou les versions acceptées sont définies et indiquées dans le présent document.

Paliers du CCTG-FRI

Dans le présent document, on trouve la description de deux paliers :

- Palier **actuel** : décrit l'état technique actuel avec lequel les livraisons du titulaire doivent fonctionner et être compatibles.
- Palier **à venir** : décrit l'état technique dans lequel doivent être livrés systématiquement les nouveaux composants et être compatibles.

Versions de composants

Les versions prescrites de composants sont spécifiées avec une précision dépendant du composant (par exemple PostgreSQL 8.2). La solution devra fonctionner quelle que soit la sous version retenue par l'Afpa (par exemple PostgreSQL 8.2.3 ou 8.2.4).

Sauf indication contraire, les composants prescrits dans le CCTG-FRI sont en **version Française**.

Abréviations

Quelques abréviations sont fréquemment utilisées dans le document. Le tableau ci-dessous les liste.

Abréviation	Signification
API	Application Programming Interface
DOP	Direction des OPérations. Département de la Direction des Systèmes d'Information de l'Afpa
CCTP	Cahier des Clauses Techniques et Particulières
DHCP	Dynamic Host Configuration Protocol. Protocole de configuration dynamique de l'adresse IP d'un équipement
DNS	Domain Name System
SMTP	Simple Mail Transfer Protocol

NTP	Network Time Protocol
ETL	Extract Transform and Load
VPN	Virtual Private Network
MPLS	MultiProtocol Label Switching
TCP/IP	Transmission Control Protocol/Internet Protocol
ESB	Enterprise Server Bus
Réseau FC	Réseau Fibre Channel à haut débit assurant l'interconnexion entre des serveurs et une ou plusieurs baie(s) de stockage mutualisé
IHM	Interface Homme Machine
iPaaS	Integration Platform as a Service
JRE	Java Runtime Environnement
JVM	Java Virtual Machine
RC	Règlement de Consultation
SAN	Storage Area Network. Réseau de stockage de données.
SGBD	Système de Gestion de Base de Données
DSI	Direction des Systèmes d'Information
WAF	Web Application Firewall
MCO	Maintien en Conditions Opérationnelle
KVM	Keyboard Video Mouse
SSID	Service Set Identifier
PAS	Plan d'Assurance Sécurité
PAQ	Plan d'Assurance Qualité

Page 10 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

1.3. Droits et obligations du candidat

Conformité et compatibilité de la solution proposée

Les exigences décrites dans ce document sont indiquées par un identifiant, construit en trois parties comme suit :

- « Ex », pour « exigence »
- « - XX » pour la numérotation de l'exigence
- « [...] », pour le périmètre d'applicabilité de l'exigence :
 - o « O » pour On-Premise
 - o « C » pour Cloud IaaS/PaaS
 - o « S » pour SaaS

Une exigence peut couvrir plusieurs périmètres d'applicabilité. Dans ces cas, l'ID comporte donc plusieurs lettres entre O, C et S.

Par exemple, l'exigence **EX-001 [OC]** s'applique aux périmètres On-premise, Cloud IaaS et PaaS.

Tout non-respect des exigences présentées dans ce document doit faire l'objet d'une demande de dérogation à l'Afpa en présentant les justifications et les alternatives proposées dans la grille d'analyse de l'adéquation aux exigences (21214_03i_CCTP_CCTG-FRI_GrilleAnalyse).

Conformité aux normes

Le candidat **garantit**, pour sa solution :

- La **conformité** avec les règles décrites dans le présent document,
- La **compatibilité** avec les composants du Système d'Information de l'Afpa (matériel, système d'exploitation, gestion des sauvegardes, réseau, échanges par ETL/ESB...)

Si l'objet du marché concerne le renouvellement d'un composant existant, la solution doit être compatible avec l'ensemble des composants non renouvelés.

Les points suivants seront pris en compte dans l'évaluation des propositions :

- Les **impacts** sur les infrastructures et les architectures techniques ;
- Les **évolutions** du parc matériel et logiciel de l'Afpa éventuellement nécessaires pour la mise en œuvre de l'offre.

Le CCTG-FRI décrit des règles techniques applicables aux projets de systèmes d'information. Le candidat doit respecter l'ensemble de ces règles.

Page 11 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

Note : Les composants, technologies ou variantes des exigences qui ne sont ni autorisés ni interdits doivent être instruits dans le document 21214_03i_CCTP_CCTG-FRI_GrilleAnalyse.

Le candidat a l'obligation de fournir une **réponse conforme** à la demande et aux standards de l'Afpa.

Le candidat peut néanmoins estimer que le CCTG-FRI impose des **contraintes qu'il souhaiterait lever**, parce qu'il (exemples non exhaustifs) :

- Souhaite **proposer un progiciel** très adapté au besoin métier, mais dont tout ou partie des caractéristiques techniques sort du cadre Afpa ;
- Estime qu'il a une **meilleure solution technique** en face d'exigences exprimées dans le CCTP.

Dans ce cas, le candidat doit compléter le document 21214_03i_CCTP_CCTG-FRI_GrilleAnalyse en présentant :

- La **justification** de la proposition de variante ;
- La **description** de la variante ;
- Les **contraintes techniques** induites.

Il est recommandé au candidat, sans que cela soit obligatoire, de partager son point de vue avec l'interlocuteur technique désigné dans le **Règlement de Consultation (RC)**.

Le candidat est invité à faire valoir la **conformité de sa solution aux normes ou aux réglementations** dont il peut se prévaloir, au-delà des seules exigences de l'Afpa.

Il peut pour cela présenter des certificats de conformité émis par des **organismes indépendants**, ou tout autre document en mesure de prouver cette conformité, quand les moyens de l'obtenir existent.

Les documents présentés peuvent être d'origine française ou étrangère.

Si les documents probatoires originaux ne peuvent être légalement reproduits, leur existence doit être confirmée par écrit par les organismes certificateurs et leurs références fournies.

Les documents originaux doivent pouvoir être consultés dans les locaux du candidat sur demande de l'Afpa.

1.4. Droits et obligations du titulaire

Engagement contractuel

Le titulaire du marché est **engagé** par le CCTG-FRI et les documents mentionnés du marché lors de sa signature.

Vérification de conformité

Le titulaire a l'obligation de fournir à l'Afpa les spécifications, tests, jeux d'essai et tous les moyens qu'il a utilisés pour vérifier la conformité des composants livrés (tests unitaires).

La recette de la solution globale est cependant réalisée à partir de jeux de tests Afpa.

Obligation de conseil

Le titulaire doit conseiller l'Afpa a minima sur les éventuelles incompatibilités entre les exigences (ex : sécurité, performances, pérennité, ...) et les contraintes techniques, réglementaires et organisationnelles associées au projet :

- Les risques inhérents à la problématique posée ;
- L'exploitabilité de la solution ;
- ...

Liste non exhaustive.

Demande de modification

L'avancement du projet peut conduire au souhait de lever certaines contraintes techniques. Dans ce cas, le titulaire peut soumettre une demande de modification du projet à l'Afpa qui étudie la proposition et statue sur son adoption.

Sécurité

Le titulaire a, entre autres, la responsabilité de :

- Respecter les politiques et règles de sécurité en vigueur au sein de l'Afpa décrites dans le document *CCTG-SSI V2.0*.
- Identifier, décrire et mettre en œuvre **les contrôles de sécurité** adéquats et conformes aux enjeux et besoins exprimés par l'Afpa ,
- Respecter et mettre en œuvre les **bonnes pratiques** en matière de sécurité.

Cadre légal et réglementaire

La solution doit être strictement conforme aux exigences légales, réglementaires ou normatives éventuellement spécifiques au projet (ex : RGPD, loi sur la cryptographie, loi de sécurité financière, etc.).

Page 13 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

1.5. Livraisons

Livraison

Les livraisons doivent respecter les règles suivantes :

Matériel

Le label **ENERGY STAR 5** ou équivalent, est requis pour le matériel fourni par le titulaire, lorsqu'il est applicable.

Documentation

Toute la documentation doit être livrée par le titulaire dans un format standard consultable/éditable sur un poste bureautique de l'Afpa.

Supports de formation

Si le Titulaire est amené à diffuser une formation auprès des personnels de l'Afpa, les manuels de formation devront être fournis aux stagiaires en langue française. Compte tenu de la médiocre qualité obtenue par traduction automatique, ce type de francisation n'est pas accepté.

Support de livraison et format

Tous les composants permettant d'installer la solution doivent être livrés sur un support couramment utilisé par l'Afpa.

Le format de livraison des composants doit permettre la lecture, la modification et la maintenance sur un environnement (**poste, serveur, partage**) de l'Afpa utilisant les outils prescrits dans le présent document en fonction du langage de réalisation.

Les jeux de tests ou résultats de tests doivent aussi répondre aux contraintes exprimées ci-dessus.

La solution doit implémenter un mécanisme de localisation et être livrée avec la langue française.

Page 14 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

Intégration sur le poste de travail

L'objectif de la qualification sur le poste de travail est de :

- Permettre le déploiement standard rapide et homogène d'une application sur les postes de travail de l'entreprise (par Publication et / ou Télédistribution) ;
- Assurer une installation ad hoc de l'application (gestion des pré requis, non requis, paramétrages, mode opératoire...) ;
- Assurer une installation industrialisée de l'application sur l'ensemble des postes de travail de l'entreprise en respectant les normes de celle-ci et en s'affranchissant des problèmes de collision avec d'autres applications qualifiées ;
- Disposer d'un référentiel des applications qualifiées et d'un inventaire du parc installé ;
- Mettre à disposition de la MOE des procédures de mises à jour mineures.

Qualification serveur

L'objectif de la qualification sur le serveur est de :

- S'assurer que la fourniture peut s'installer industriellement sur le serveur ;
- S'assurer du dimensionnement des ressources, notamment en espace disque, à attribuer ;
- S'assurer du respect des normes d'exploitation ;
- S'assurer de l'exploitabilité de la solution ;
- Intégrer l'automatisation d'exploitation ;
- Intégrer si besoin le Plan de Secours (voir conditions plus loin) ;
- Disposer d'un référentiel des applications qualifiées.

1.6. Fonctionnement

Absence de contrainte

Tout composant de la solution doit fonctionner sans imposer une contrainte liée à un composant physique (clef USB, processeur, disque, adresse MAC, dongle, ...) ou logique (numéro de licence, numéro du système, date d'expiration, ...).

Si une application nécessite l'utilisation de certificats, alors ceux-ci doivent être gérés par l'Afpa.

Page 15 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

2. Infrastructures

2.1. Datacenter

Centres informatiques

Ex-001 [O] : Le titulaire doit mettre à disposition de l'Afpa un centre informatique (Datacenter) avec un site de production Tier III qui héberge en priorité les Systèmes d'Information (SI) de production, de recette et de développement.

Ex-002 [C] : Le titulaire doit mettre à disposition un hébergement Cloud pour les services IaaS et PaaS de l'Afpa. L'hébergement doit se faire sur un centre informatique localisé sur le territoire européen.

Ex-003 [S] : Les solutions SaaS doivent être hébergées dans un centre informatique localisé sur le territoire européen.

Services d'infogérance en Datacenter

L'infogérant réalise des activités d'infogérance sur les équipements suivants :

- Firewall (et sous réseaux associés), composants de sécurité,
- Proxys sortants et entrants,
- WAF,
- Serveurs physiques et virtuels sous Linux et Windows, quelle que soit leur architecture (*standalone, failover, cluster, ...*),
- Autres composants d'infrastructure liés au socle de virtualisation tels que hyperviseurs, OS,
- Instances logicielles installées entre la couche d'OS et la couche applicative (non incluse), ex : composants Middleware, base de données, ...
- Load Balancers,
- Serveur DNS interne,
- Passerelle SMTP,
- Serveur de temps NTP.

L'infogérant assure les activités suivantes sur ces équipements :

- la maintenance matérielle,
- l'application du maintien en conditions opérationnelles (MCO) des constructeurs/fournisseurs afin de bénéficier des conditions de garantie et de support,
- le suivi des événements constructeurs/fournisseurs de manière réactive (alertes) et proactive, puis l'instruction de l'événement (normal, standard, urgent),
- la sauvegarde / restauration de l'environnement technique,
- la gestion des contrats de maintenance matérielle,

Page 16 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

- la gestion des contrats de licence,
- la mise en œuvre de la politique de sécurité,
- l'exploitation,
- la supervision, l'application des consignes d'exploitation, ainsi que la pro activité sur les incidents,
- le dépannage,
- l'arrêt et le redémarrage de l'équipement, du système ou d'un logiciel (base de données, serveurs d'application, serveur Web),
- l'ordonnancement,
- le contrôle des batchs techniques.

Format des équipements

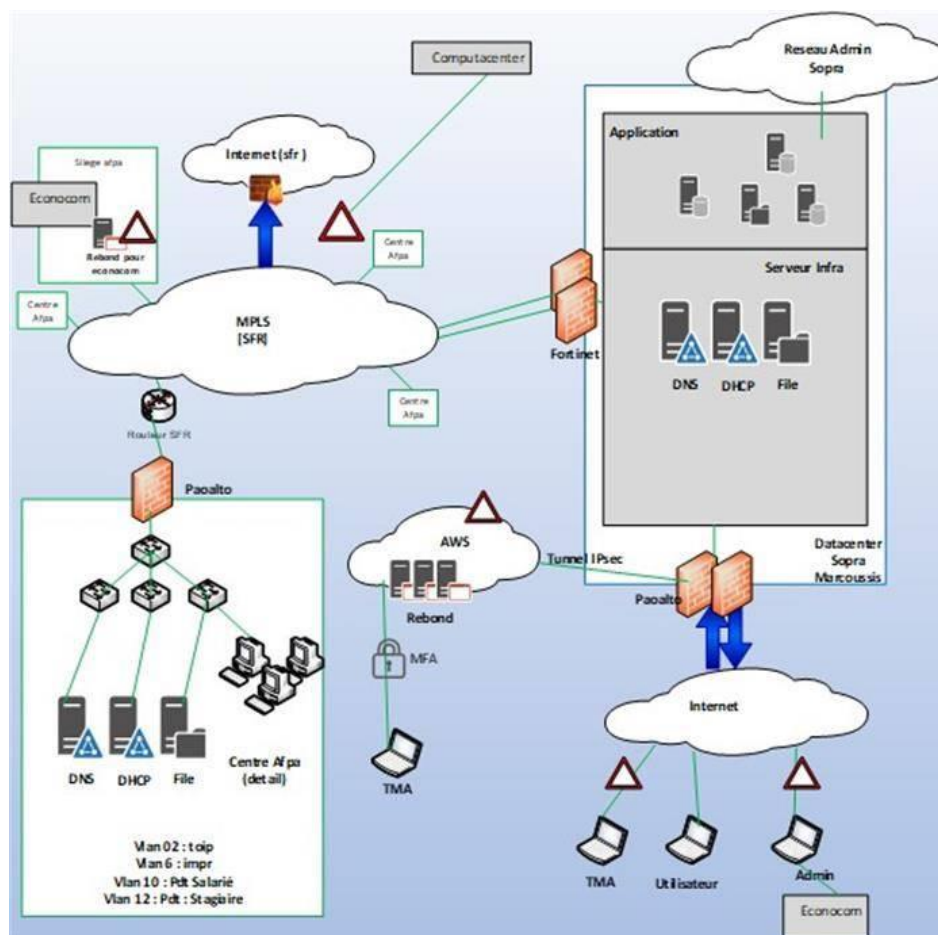
Ex-004 [O] : La salle doit être équipée de baies permettant d'accueillir des équipements au format standard 19 pouces de large avec les caractéristiques suivantes :

- La hauteur utile intérieure de la baie est de 47 unités (47U).
Noter que ces unités ne sont pas toutes affectables à des serveurs (Commutateurs IP et/ou FC, modules Écran/Clavier ou KVM).
- Ces baies doivent permettre la sécurisation électrique des serveurs par leur raccordement à deux sources d'alimentation différentes (Standard constructeur ou Système de Transfert Statique de source (STS)).

Ex-005 [O] : À l'exception des équipements « lourds » comportant leur propre armoire (Ex : baies de stockage disque, robots de sauvegarde), les équipements fournis doivent impérativement être rackables dans ces armoires.

2.2. Réseaux

Description du réseau de l'Afpa



Le réseau AFPA est un réseau MPLS (réseau maillé complet) interconnectant l'ensemble des centres AFPA dont le Datacenter

On distingue plusieurs types d'accès selon les populations :

- 1) Accès des utilisateurs internes sur Réseau Afpa :
 - a. Utilisation du réseau MPLS pour accéder aux applications en Datacenter. Tous les échanges entre le réseau de l'Afpa et les centres Afpa passent par un firewall situé sur le datacenter.
 - b. Utilisation de la sortie Internet centralisée du réseau MPLS pour accéder aux applications hébergées sur les plateformes Cloud et celles en mode SaaS.

Page 18 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

- 2) Accès des TMAs et des utilisateurs externes au réseau de l'Afpa :
- Pour un profil type utilisateur : passage par le VPN Nomade pour accéder au Datacenter (prérequis : compte dans l'Active Directory),
 - Pour un profil type administrateur : La connexion aux machines se fait par SSH ou RDP en passant par le bastion hébergé sur la plateforme Cloud (prérequis : compte dans l'Active Directory), pour administrer :
 - les applications en Datacenter (passage par le tunnel IPSEC depuis la plateforme Cloud),
 - les applications sur la plateforme Cloud.

Les applications SaaS sont accessibles directement par Internet.

- 3) Echange de données avec partenaires Afpa :
- Passage par zones d'échange pour du transfert de fichiers,
 - Passage par un proxy pour des échanges par WebServices / APIs.

Tous les échanges de données sont sécurisés au niveau de la couche transport.

Bande passante

Ex-006 [O] : La Bande Passante du réseau WAN varie selon les brins, elle doit être consommée par les flux de toute nature ; et partagée par tous les utilisateurs.

Accès distants

Il existe 3 accès entrants différents :

- Accès via le VPN Nomade
- Accès via le Bastion Windows sur AWS
- Possibilité d'accès entrant sur la plateforme centrale SFR

Il y a 2 types de sortie différents sur Internet :

- Par la sortie réseau du Datacenter
- Par la sortie MPLS

Règles de base

Ex-007 [O] : Les échanges de flux sortants du réseau Afpa vers Internet doivent être capables d'utiliser des adresses IP de sortie dynamiques :

- Adresses IP publiques attribuées par SFR,
- Adresses IP de classe /24 pour les sorties Datacenter

Surf et accès

Ex-008 [O] : Des règles de filtrage classiques s'appliquent pour la sortie du MPLS SFR (navigation des utilisateurs sur Internet).

Page 19 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

Ex-009 [O] : Pour la sortie Internet du Datacenter, tous les flux sont par défaut interdits, seuls les flux nécessaires sont autorisés et doivent être décrits (source, destination, port source, port destination)

Interconnexion du centre de Production

Ex-010 [O] : Le site de production est interconnecté au travers de liens redondés et en répartition de charge vers le réseau MPLS.

Ex-011 [O] : Un Firewall sécurise l'interconnexion entre le réseau MPLS et le Datacenter.

Ex-012 [O] : L'interconnexion entre le site de production et le Cloud se fait au travers d'un tunnel IPSEC redondé.

Ex-013 [O] : L'accès internet du site de production se fait via un lien WAN redondé et en répartition de charge.

Interconnexion des centres Afpa

Ex-014 [O] : Un équipement Firewall doit être installé au niveau de chaque sortie des centres Afpa vers le MPLS.

Réseau entreprise

Les réseaux de l'Afpa s'appuient sur un réseau MPLS, et offrent les services suivants :

- Service **Téléphonique sur IP**
- Service de transport de **Données**
- Service **d'interconnexion**

Tous les équipements informatiques installés à l'Afpa sont connectés sur un réseau local.

Ethernet

Ex-015 [O] : Les réseaux locaux installés à l'Afpa doivent être conformes à la norme Ethernet (IEEE 802.3).

Wifi

Ex-016 [O] : De nombreux réseaux locaux doivent être équipés d'un service de connexion Wifi qui diffuse des SSID pour les salariés et stagiaires (nécessitant un compte utilisateur du domaine Afpa de l'Active Directory), pour les invités, mais aussi pour les sociétés implantées dans les "Afpa Village".

Protocole TCP/IP

Ex-017 [O] : Le protocole réseau utilisé est **TCP/IP**. La solution doit être conçue pour fonctionner aussi bien sur un réseau IP v4 que sur un réseau IP v6.

Ex-018 [O] : L'accès aux applications doit s'appuyer sur la résolution de nom DNS.

Page 20 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

Service DHCP **Ex-019 [O]** : Les solutions doivent fonctionner indépendamment du mode d'adressage IP des équipements d'accès au SI.

Messagerie **Ex-020 [O]** : Tout email sortant du réseau de l'Afpa et présentant une adresse d'émission d'un domaine non géré par l'Afpa doit être rejeté.

Ex-021 [O] : Tout email entrant, présentant une adresse d'émission d'un domaine géré par l'Afpa (ex : adresse@afpa.fr), est rejeté sauf s'il existe un enregistrement SPF qui autorise l'envoi du mail.

Si la solution nécessite l'utilisation du service de messagerie, le titulaire peut s'adresser à l'Afpa pour obtenir le nom de domaine à utiliser.

Réseau IP en Datacenter

Ex-022 [O] : Le cœur de réseau interne sur le centre de production doit être redondé, depuis chaque serveur jusqu'à l'accès à l'extérieur du centre de production.

Supervision et Métrologie

Ex-023 [O] : Le titulaire doit être doté d'une solution de supervision de l'ensemble des éléments d'infrastructure, et donner les droits en lecture à l'Afpa a minima.

2.3. Stockage, sauvegarde et archivage

Infrastructure de stockage

Ex-024 [O] : L'infrastructure de stockage (propriété du titulaire du marché d'infogérance) doit héberger les données directement accédées par les serveurs applicatifs.

Ex-025 [O] : Les données des SI doivent être stockées sur des baies mutualisées au travers d'un réseau de type SAN.

Baies de stockage

Ex-026 [O] : Les baies doivent assurer le stockage des données et des programmes.

D'autres données telles que les logiciels d'exploitation ou les noyaux de SGBD peuvent si besoin être stockées sur le SAN.

Ex-027 [O] : Les éléments suivants doivent être stockés sur les disques internes des serveurs physiques :

- Le système d'exploitation,
- Les logiciels d'exploitation : Logiciels de sauvegarde, d'automatisation, de surveillance, ...

- Les logiciels de bases de données ;
- Les serveurs d'application (middleware).

Réseau SAN FC **Ex-028 [O]** : Les interconnexions entre serveurs applicatifs et les baies de stockage doivent être assurées par un réseau FC (Fibre Channel) redondé :

- Chaque serveur doit accéder au réseau FC du datacenter par deux connexions à deux commutateurs FC différents.
- Chaque baie de stockage doit être accédée par deux commutateurs FC.

Solution sauvegarde **Ex-029 [OCS]** : La solution de sauvegarde externalisée doit être distante et sécurisée par chiffrement.

Ex-030 [OCS] : Une politique de sauvegarde, décrivant le volume à sauvegarder, la rétention, le type de sauvegarde (incrémentale, différentielle et full) doit être définie avant toute mise en œuvre.

Ex-031 [OC] : L'infrastructure de sauvegarde doit être sur un réseau dédié (réseau administration)

Solution d'archivage **Ex-032 [OC]** : L'Afpa étudie une offre d'archivage à valeur probante, qui devra être considérée en priorité par le titulaire.

2.4. Serveurs applicatifs et de données, et systèmes d'exploitation

Support des applications métier

Ce paragraphe traite des serveurs supportant des applications métiers exploitées par la DOP dans ses centres informatiques (datacenter). Il existe deux types de serveurs : physiques et virtuels.

Virtualisation

Ex-033 [O] : Les serveurs virtuels s'appuient sur la solution VMware, implémentée sur des châssis DELL dont l'Afpa est propriétaire ; ainsi que des racks. Les demandes de VM sont réalisées conformément à des modèles de serveur prédéfinis (voir annexe §4.1).

Serveurs physiques

Ex-034 [O] : La configuration **minimale** des serveurs installés en production est la suivante :

- 2 CPU de type x64 ;
- 16 Go de mémoire RAM ;
- 2 disques internes en miroir supportant le système d'exploitation ;
- 4 interfaces Ethernet 1Gb/s soit 2 cartes de 2 ports ;

Page 22 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

- 1 carte de prise de main à distance pour administration du serveur
- 2 interfaces Fiber Channel ;
- Une alimentation électrique redondante.

Système d'exploitation

Ex-035 [OC] : Les systèmes d'exploitation sont :

- Linux Redhat RHEL ;
- Windows Server.

Infrastructure virtualisée/consolidée

Equipement en cartes réseaux

Ex-036 [O] : Chaque lame hébergeant des serveurs virtuels doit être équipée de :

- 2 cartes réseaux pour un total de 6 interfaces Ethernet 1Gb/s minimum ;
- 2 interfaces redondantes en équilibrage de charge pour l'accès des utilisateurs au SI ;
- 2 interfaces redondantes en équilibrage de charge pour l'administration du serveur ;
- 2 interfaces redondantes en équilibrage de charge pour la tolérance de panne VMware ;
- 1 carte 2 ports FC (HBA) 8Gb/s minimum en interface avec l'infrastructure de stockage (systèmes d'exploitation et applicatifs).

2.5. Gestion des systèmes

Introduction

Ce paragraphe traite des outils d'exploitation :

- Surveillance des systèmes et des applications
- Hypervision
- Sauvegardes/restaurations
- Automatisation
- Métrologie

Outil d'exploitation

Ex-037 [OC] : Les outils à utiliser par l'infogérant pour l'exploitation des systèmes et applications métier sont Appdynamics (propriété de l'Afpa), Automator de Axway (propriété de l'Afpa) et Cacti.

Surveillance de la solution

Ex-038 [OCS] : La solution doit être supervisée afin que l'exploitant puisse déterminer si le service est rendu aux utilisateurs. Au-delà des procédures de surveillance technique (CPU, mémoire, espace disque,

processus, état des bases de données, ...), l'infrastructure de surveillance doit permettre d'analyser les éléments suivants :

- Fichiers de journalisation (log) produits par les applications (non applicable pour une application en mode SaaS) ;
- Vérification technique et fonctionnelle des transactions utilisateurs / accès à une base de données ;
- Serveur Web – Serveur d'application – Serveur de données.

Surveillance depuis l'internet

Ex-039 [OCS] : L'Afpa dispose d'un outil externe InternetVista, permettant de surveiller les systèmes d'information ouverts sur l'Internet.

Cette solution basée sur l'exécution de scénarios prédéfinis doit permettre de disposer de tableaux de bord sur les éléments suivants :

- Temps de réponse ;
- Taux de disponibilité.

Sauvegardes

Ex-040 [OCS] : Le titulaire doit suivre les principes généraux suivants consistant à réaliser pour les environnements applicatifs :

- Une sauvegarde quotidienne incrémentale (fichiers modifiés depuis la dernière session de sauvegarde) ;
- Une sauvegarde hebdomadaire totale ;
- Une durée de rétention de sauvegarde minimum, variable en fonction du type d'application.

A ces sauvegardes applicatives s'ajoutent les sauvegardes systèmes.

Technologies utilisées

Ex-041 [OC] : Le titulaire doit réaliser les sauvegardes des systèmes d'information et des environnements de type image, soit par des méthodes dites « à froid », soit « à chaud » :

- On appelle sauvegarde à froid une sauvegarde réalisée une fois les services arrêtés ;
- On appelle sauvegarde à chaud une sauvegarde réalisée sans arrêt des services.

Accès aux informations ressource

Ex-042 [OCS] : L'hébergeur doit pouvoir être en mesure de partager des métriques de l'application liées à son utilisation (garbage collector, taux d'utilisation des pools de connexion, nombre de sessions actives) afin d'identifier de manière proactive de potentielles dérives, et aider au diagnostic.

2.6. Ressources utilisateurs

Intégration des applications

Sur le poste de travail

Ex-043 [OCS] : La solution doit être indépendante des outils bureautiques du poste client. Par conséquent, l'utilisation des macros de Microsoft Office est interdite.

Les fichiers de données exportées doivent être créés sans appel direct aux outils bureautiques du poste de travail.

Interaction utilisateur

IHM

Ex-044 [OCS] : Sauf spécification contraire, les IHM sont conçues pour une résolution écran a minima 1280x1024 mais doivent rester compatibles avec d'autres résolutions.

Qualité de vidéo

Ex-045 [OCS] : La résolution des vidéos doit être compatible avec les outils de lecture vidéo et le navigateur du poste de travail.

Ex-046 [OCS] : Le titulaire doit être conforme à la totalité des exigences RGAA dans le cadre de diffusion vidéo.

Client léger

Ex-047 [OCS] : Les applications client léger doivent respecter a minima le standard Internet HTML 5 pour tout nouveau projet ainsi que pour la diffusion de vidéos.

Ex-048 [OCS] : Les applications doivent respecter la norme RGAA.

Navigateurs cibles

Ex-049 [OCS] : Les règles de visualisation en fonction du type d'utilisateur sont les suivantes :

Type de site web Afpa	Règle de visualisation
Internet	L'information mise à disposition sur les sites Internet Afpa doit être accessible avec tous les navigateurs du marché.
Intranet	Toute page mise à disposition sur l'Intranet doit pouvoir être visualisée à l'identique sur les navigateurs Internet des équipements d'accès au SI de l'Afpa.

Page 25 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

Données

Formats bureautiques préconisés

Ex-050 [OCS] : Les formats à utiliser en priorité pour la génération de fichiers par le SI à destination des points de terminaison sont :

- **PDF/A** pour les besoins de lecture seule avec mise en forme ;
- **CSV** pour les besoins d'édition de données tabulées sans mise en forme ;
- **DOCX, XLSX, XLSB et PPTX** : pour les besoins d'édition de données avec mise en forme.

Les points de terminaison (postes Pédago, tablettes...) doivent être en mesure de lire les fichiers ainsi générés par le SI.

Les documents générés doivent garantir l'accessibilité numérique.

Le format à utiliser en priorité pour l'alimentation d'un SI à partir de données collectées sur un équipement d'accès est :

- **CSV ou XML** pour les besoins d'importation de données ;
- Les fichiers doivent être compatibles avec la suite bureautique Microsoft Office365.

Accès aux OS Linux par les administrateurs

Ex-051 [OCS] : Le protocole à utiliser est SSH v2 avec des clefs d'une taille comprise entre 256 bits et 2048 bits.

Poste de travail

Ex-052 [O] : Le parc de l'Afpa comprend environ 50 000 postes. Toutes les applications métiers doivent pouvoir être utilisables sur le poste de travail.

Poste fixe

Ex-053 [O] : Le titulaire doit être capable de proposer une offre de PC poste fixe comprenant 2 modèles de configuration :

- Poste bureautique standard (SSD, RAM 16 Go)
- Poste station de travail (SSD, RAM 16 Go, Nvidia quadro)

Poste portable

Ex-054 [O] : Le titulaire doit être capable de proposer une offre de PC portable comprenant 3 modèles de configuration :

- PC standard bureautique (15 pouces, technologie SSD)
- PC ultra léger (configuration spécifique avec faible poids et faible taille, moins de 2 kg, 14 pouces)
- Poste station de travail (Core I5 ou équivalent minimum, Nvidia quadro)

Les postes de travail peuvent être équipés en processeurs d'origine Intel ou AMD.

Sécurité d'usage du poste Pédago

Ex-055 [O] : Les principales mesures de sécurité relatives à l'usage des postes de travail du domaine Pédago sont par défaut que leurs utilisateurs :

- Doivent être authentifiés par Active Directory ;
- Les prestataires doivent appartenir exclusivement au groupe « Utilisateurs du domaine » et ne peuvent donc pas modifier la configuration du poste alors que les stagiaires doivent appartenir à un autre groupe spécifique.

Sécurité d'usage du poste Gestion

Ex-056 [O] : Les principales mesures de sécurité relatives à l'usage des postes de travail du domaine Gestion sont par défaut que leurs utilisateurs :

- Doivent être authentifiés par Active Directory ;
- Les stagiaires doivent appartenir exclusivement au groupe « Utilisateurs du domaine » et ne peuvent donc pas modifier la configuration du poste alors que les prestataires doivent appartenir à un autre groupe spécifique.

Logiciels

Ex-057 [O] : Les postes doivent fonctionner sous Microsoft Windows.

Ils doivent être livrés avec un socle logiciel commun mais peuvent disposer de logiciels optionnels.

Les tableaux ci-dessous listent les logiciels pouvant équiper ce type de poste.

Logiciels du socle commun pour le Master Gestion	
Composant	Produit
Suite bureautique	Microsoft 365 Apps
Client de messagerie	Outlook
Client d'agenda partagé	Outlook
Lecteur de fichiers PDF	Edge / Acrobat Reader DC
Navigateur	Edge Chromium / Firefox ESR

Logiciels du socle commun pour le Master Pédago	
Composant	Produit
Suite bureautique	Microsoft Office 2016
Client de messagerie	Outlook

Client d'agenda partagé	Outlook
Lecteur de fichiers PDF	Edge / Acrobat Reader DC
Navigateur	Edge Chromium

Déploiement **Ex-058 [O]** : Le titulaire doit proposer une solution équivalente à SCCM lors du déploiement du poste de travail comme outil de gestion du parc bureautique. L'outil doit présenter a minima les fonctionnalités suivantes : déploiement d'applications et d'OS, télédistribution logicielle, prise en main à distance, remontée d'inventaires, patch management...

Terminaux mobiles Le parc de l'Afpa comprend environ 4000 téléphones basiques et 2500 smartphones.
Il n'est à ce jour pas demandé aux smartphones d'être en mesure d'accéder aux services frontaux de l'entreprise ainsi qu'aux systèmes d'information.

Logiciels **Ex-059 [O]** : Les smartphones doivent fonctionner sous les systèmes suivants :

- IOS, pour des terminaux utilisés par les VIP (Direction) ;
- Android, pour les terminaux utilisés par les autres acteurs.

Des tablettes en Windows et Android peuvent exister également dans le parc Afpa.

Déploiement **Ex-060 [O]** : Si la solution est accompagnée d'applications natives mobiles, alors elle doit passer par un mode de déploiement avec Intune pour permettre la gestion du parc mobile.

2.7. Services frontaux

Services d'authentification Les services d'authentification mentionnés ci-dessous s'appliquent aux utilisateurs.

Accès aux applications **Ex-061 [OCS]** : Toute nouvelle application métier doit permettre une authentification en SSO.

Autres situations **Ex-062 [OCS]** : L'authentification des utilisateurs de l'infrastructure bureautique de l'entreprise s'appuie sur Active Directory on-premise et sur

Page 28 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

Azure Active Directory. L'infrastructure Active Directory est répartie entre le Datacenter et les plateformes Cloud, et multi redondée.

Partage de ressources bureautiques

Ex-063 [OCS] : Les ressources partagées (fichiers) doivent être sur Teams via Sharepoint Online et OneDrive.

Messagerie

Ex-064 [OCS] : Le logiciel de messagerie doit être celui de la suite Microsoft Office 365.

Applications Intranet et Internet

Ex-065 [OCS] : L'Afpa utilise la solution Mozzaik365 sur Sharepoint Online pour les futurs portails intranet.

Impression

Imprimantes partagées

Ex-066 [O] : Les moyens d'impression de l'entreprise doivent être partagés. Il s'agit d'imprimantes lasers ou de copieurs multifonctions connectés aux réseaux locaux.

Ex-067 [O] : Ces moyens d'impression doivent supporter a minima PCL6 et si possible du PS.

Ex-068 [O] : Les principales caractéristiques des points d'impression des imprimantes doivent respecter les mesures suivantes :

- 50 ppm ;
- 600 DPI (Dots Per Inch) ;
- Recto-verso ;
- Bac multifonctions A4 et A3 ;
- Drivers disponibles sous Linux et Windows Server.

Ex-069 [O] : La politique d'impression impose :

- Impression monochrome par défaut ;
- Impression recto-verso ;
- Impression retenue.

2.8. Secours informatique

Plan de secours Abordé dans le CCTG-SSI V2.0.

Haute disponibilité Abordé dans le CCTG-SSI V2.0.

Page 29 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

2.9. Sécurité

Exigences de sécurité Abordées dans le CCTG-SSI V2.0.

3. Middleware

Socle des applications métier

Ex-070 [OCS] : Les composants SGBD du socle technique à utiliser, sont par ordre de priorité :

- PostgreSQL
- MariaDB
- MySQL
- SQL Server

Principes d'intégration inter-applicatifs

Ex-071 [OCS] : Un flux ne doit transiter par une brique ESB / ETL que s'il y a une valeur ajoutée (ex : transformation, monitoring, ...).

Ex-072 [OCS] : Les accès en lecture / écriture directs d'une application dans la base de données d'une autre application sont interdits (applicable également à l'ETL).

Ex-073 [OCS] : Tous les échanges doivent être définis et soumis à approbation par une instance dédiée avant leur mise en œuvre.

Ex-074 [OCS] : Toute application qui doit échanger des données Afpa doit être authentifiée.

Ex-075 [OCS] : Tout échange inter applicatif doit être chiffré (données en transit).

Ex-076 [OCS] : Tous les échanges avec les partenaires doivent être tracés. Les flux inter applicatif Afpa doivent être tracés lorsque cela est techniquement possible (au niveau de l'application ou via la plateforme d'intégration).

Ex-077 [OCS] : Toute interface doit pouvoir être supervisée afin de s'assurer de son bon fonctionnement (au niveau de l'application ou via une brique middleware) et déclencher des alertes si nécessaire.

Ex-078 [OCS] : Tout échange par API vers un partenaire doit passer par une brique middleware de type ESB ou iPaaS.

Ex-079 [OCS] : Tout échange par API d'un partenaire vers des applications Afpa doit passer par une solution d'API Management ou équivalent.

4. Développement

3.1 Architecture applicative

Types d'architecture

Architecture « n-tiers »

Ex-080 [OC] : Le titulaire doit adopter le modèle n-tiers pour la réalisation de ses applications, présenté dans le tableau ci-dessous.

Les couches

Les couches typiques d'une application sont :

Couche	Description
Affichage	Affichage pour l'utilisateur.
Présentation	Production de l'IHM, gestion des sessions utilisateurs, interaction utilisateurs, appel de processus.
Coordination	Gestion processus métier, appels de services, gestion des erreurs applicatives et techniques, gestion des éventuelles portées transactionnelles, gestion de la traçabilité, des accès et des habilitations.
Service	Support technique de l'accès à la couche domaine et ses objets, contrôle des transactions.
Domaine	Validation des règles métier, fourniture des accès aux informations.

Persistence	Persistence et cycle de vie des occurrences des entités métier.
--------------------	---

Types de solutions

Ex-081 [OC] : Les applications informatiques doivent être basées sur deux types de solutions :

- **Solution progicielle** : Produit « sur étagère », existant déjà hors contexte et spécificités Afpa. Un progiciel doit être déployé et fonctionner sous Linux ou sous Windows ;
- **Solution logicielle** : Développement « sur mesure » réalisé sur spécifications de l'Afpa. Le logiciel doit être déployé sous **Linux**.

Licences

Ex-082 [OC] : Les applications informatiques doivent utiliser des solutions open-source gratuites, incluant les frameworks de développement.

Ex-083 [OC] : Dans les cas où le titulaire utilise une solution open source ayant pour impact une « contamination » logicielle (=propagation des termes de la licence aux développements), celui-ci devra en informer l'Afpa et détailler les raisons de ce choix de licence et les impacts associés.

Ex-084 [OC] : Le titulaire doit communiquer à l'Afpa les types de licence associés aux composants open source qu'il souhaite utiliser, et obtenir la validation de l'Afpa pour tout recours à une licence contaminante.

Règles d'architecture applicative

Paramétrage utilisateur

Ex-085 [OCS] : Les paramétrages propres à chaque utilisateur doivent être stockés sur un serveur dans un répertoire ou une base de données dans le cadre d'une architecture 3-tiers.

Ex-086 [OC] : Les données locales doivent pouvoir être stockées à un emplacement paramétrable.

Multi-utilisateur

Ex-087 [OCS] : La solution doit être multi-utilisateurs.

Ex-088 [OCS] : Si des paramétrages, propres à chaque utilisateur, sont utilisés, la solution doit stocker les paramètres dans un espace distinct pour chaque utilisateur.

Page 32 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

Tolérance aux fautes

Ex-089 [OCS] : Pour maximiser la disponibilité du service en cas de défaillance, la solution doit être conçue de façon à ce que l'indisponibilité de l'un de ses composants ait un impact réduit sur le reste des modules de la solution. Pour cela, la solution doit favoriser le découplage, la redondance de ses constituants critiques et pourra également s'appuyer sur des caches de données (caches contribuant également à répondre aux exigences de performance).

Ex-090 [OCS] : Les applications doivent être tolérantes vis-à-vis des problèmes liés à la qualité du réseau :

- Reprise avec perte de communication ;
- Variation de bande passante disponible ;
- Forte latence ;
- ...

Echanges inter-applicatif par API

Ex-091 [OCS] : Les flux API REST sont privilégiés pour les échanges inter-applicatifs Afpa.

Ex-092 [OCS] : Tout échange d'API REST doit exposer des opérations sur un objet métier spécifique.

Développement IHM

Ex-093 [OC] : Toutes les IHM doivent se faire avec une architecture client léger.

Ex-094 [OCS] : Les applications doivent être conformes en totalité avec la norme RGAA dans le cadre de développements IHM.

Ex-095 [OCS] : Le code JavaScript doit respecter la norme ECMA-262 avec l'édition en vigueur ou précédente pour les nouvelles applications et RGAA.

Ex-096 [OC] : Les applications web doivent être développées en suivant l'approche Responsive Web Design.

3.2 Langages et outillage de développement

Choix technologiques

Ex-097 [OC] : Les produits retenus pour le développement des solutions sont par ordre de préférence :

- Java ;
- PHP.

Le langage préférentiel à utiliser est Java. Toute utilisation du langage PHP devra faire l'objet d'une justification.

Page 33 of 46	<p style="text-align: center;"><u>Afpa-CCTG-FRI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique</p>	
Version 1.1		Direction des Systèmes d'Information

3.2.1. Langage Java

Usages Java

Ex-098 [OC] : La solution ne doit pas implémenter d'EJB.

Ex-099 [OC] : les langages Angular, React ou Vue.js doivent être utilisés pour les développements d'IHM.

Ex-100 [OC] : Dans le cadre de développement d'application avec le langage Java, le titulaire doit utiliser les frameworks de gestion de Log comme par exemple Log4j.

Ex-101 [OC] : L'intégration de services à un portail se fait au travers de portlets au standard JSR168 (Java Specification Request).

Ex-102 [OC] : Le Mapping objet-relationnel doit se faire via le framework Hibernate/JPA.

Accès aux Base de données

Ex-103 [OC] : La couche d'accès aux bases de données doit dépendre du langage utilisé pour le développement du tiers applicatif.

Développement Java

Outils

Ex-104 [OC] : Le titulaire doit pouvoir auto-générer la documentation de son code à l'aide d'un outil de type JavaDoc ou similaire.

Ex-105 [OC] : Le titulaire doit réaliser des tests unitaires automatisés pour tous les projets de développement Java, en s'appuyant sur un outil de type JUnit ou équivalent.

3.2.2. Langage PHP

Socle technique

Usages PHP

Comme mentionné dans l'exigence **Ex-097 [OC]**, le langage PHP est à justifier.

Framework

Ex-106 [OC] : Dans le cadre de développement d'application avec le langage PHP, le titulaire doit utiliser le framework Symfony et son ORM doctrine.

Développement PHP

Outils Ex-107 [OC] : Le titulaire doit réaliser des tests unitaires automatisés pour tous les projets de développement PHP, en s'appuyant sur un outil de type PHPUnit ou équivalent.

Ex-108 [OC] : Le titulaire doit pouvoir auto-générer la documentation de son code à l'aide d'un outil de type DOCBlox ou similaire.

3.2.3 Outillage de développement

Outillage Ex-109 [OCS] : Dans une logique d'industrialisation et de standardisation de l'outillage DevSecOps*, les projets de développement applicatifs doivent soit utiliser la liste des outils ci-dessous, mise à disposition par l'Afpa à travers sa forge, soit fournir des livrables compatibles avec ces outils. Par exemple, dans le cas de développements réalisés par un tiers (intégrateur / TMA), celui-ci pourra utiliser son propre outillage mais devra livrer à l'Afpa des scripts compatibles avec les outils de sa forge

Fonction	Produits et Outils
Environnement de développement	IntelliJ IDEA ou Eclipse IDE pour Java, Eclipse PDT pour PHP
Gestion des sources	Gitlab
Dépôt d'artefact / gestion des dépendances	Maven, avec repository manager Archiva
Qualimétrie	Sonarqube
Tests d'intégration pour les tests d'API	Postman
Tests de performance	Gatling
Tests de sécurité	OWASP ZAP
Déploiement de l'infrastructure	Terraform
Déploiement des applications	Ansible

Gestion des containers	Docker
Plateforme d'Intégration Continue (PIC)	Jenkins
Supervision et gestion des performances applicatives	APPDynamics
Gestion de projet	Jira

* : la présentation de la démarche DevSecOps de l'Afpa et les exigences associées se retrouve dans le document : 21214_03c_CCTP_CE-DSO.

Ex-110 [OCS] : Les livrables techniques (fichier WAR, fichier JAR, scripts PHP...) fournis par le titulaire doivent pouvoir être installés et recompilés avec les outils de la forge Afpa.

3.3. Réalisation des développements

Normes de développement

Design patterns

L'utilisation de « design patterns » par le titulaire est recommandée. Les « design patterns » correspondent à un ensemble de bonnes pratiques de conception qui permettent d'appliquer des modèles éprouvés pour bâtir des applications.

La description du pattern MVC2 est présentée ci-dessous pour exemple. C'est une recommandation, mais le titulaire est libre d'utiliser d'autres patterns.

Un choix structurant pour l'architecture d'une application concerne la communication de la couche de présentation avec les couches services ou domaine.

Pattern MVC2 :

Le pattern universel MVC2 organise cette communication entre les deux couches.

Ce pattern s'articule autour des 3 responsabilités :

- La partie **Modèle** : Contient les données et les règles de gestion associées et ignore totalement la manière dont les données sont affichées ;

Page 36 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

- La partie **Vue** : Affiche les données contenues dans le modèle ;
- La partie **Contrôleur** : Détecte les actions utilisateurs et met à jour le modèle.

Les frameworks de présentation préconisés par l'Afpa respectent ces bonnes pratiques.

Indépendance et portabilité

Ex-111 [OC] : La solution doit être indépendante de la version du système d'exploitation installé sur le serveur.

Une couche d'abstraction, comme par exemple la JVM pour les applications Java, doit systématiquement être utilisée par la solution pour communiquer avec le système d'exploitation.

Ex-112 [OC] : La solution ne doit pas :

- S'appuyer directement sur des services dépendant du système d'exploitation ;
- Appeler directement des primitives du système d'exploitation ou d'autres applications.
- Adresser directement des périphériques ou nécessiter des pilotes spécifiques.

Application des Services Packs

Ex-113 [OC] : Une solution s'appuyant sur Windows ou sur SQL Server doit impérativement **supporter l'application des Services Packs** édités par Microsoft.

Séparation données/traitements

Ex-114 [OC] : Les données doivent être séparées de leur traitement.

Ex-115 [OC] : Toute mise à jour de la solution qui nécessite de migrer les données doit être accompagnée d'une procédure de migration des données et de roll-back.

Mécanismes de cache

Ex-116 [OC] : Un logiciel spécifique ne doit pas gérer directement de mécanisme de cache des données mais doit s'appuyer sur les mécanismes intrinsèques aux briques constituant le socle des applications.

Code

Ex-117 [OC] : Le code de la solution doit utiliser uniquement les instructions standards et normalisées du langage sur lequel elle s'appuie ou des langages qu'elle utilise.

Les instructions non normalisées, par exemple des extensions spécifiques proposées uniquement par un éditeur à des fins d'optimisation, ne doivent pas être utilisées.

Ex-118 [OC] : Le code doit être indépendant de la localisation physique de l'application, de l'URL, et des divers contextes physiques.

Page 37 of 46	<p style="text-align: center;"><u>Afpa-CCTG-FRI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique</p>	
Version 1.1		Direction des Systèmes d'Information

Qualité du code

Ex-119 [OC] : Les indicateurs de qualité de code suivants doivent être minima produits. Les taux (minimum/maximum) sont à définir dans le PAQ de chaque projet.

- Taux de couverture de tests unitaires ;
- Taux de duplication de code acceptable ;
- Nombre de violations critiques ;
- Maintenabilité du code ;
- Nombre de vulnérabilités dans le code.

Accès aux bases de données

Ex-120 [OC] : Le développement de connecteurs de base de données doit s'appuyer sur les pilotes fournis par les éditeurs ou la communauté open-source.

Validation de données

Ex-121 [OC] : La solution doit systématiquement valider les données d'entrée avant tout traitement pour se prémunir des attaques (injection, xss, ...). Il s'agit de vérifier :

- Les valeurs hors intervalle ;
- Les caractères invalides dans les champs de données ;
- Les données manquantes ou incomplètes ;
- Le non-respect des limites inférieures et supérieures en termes de volume ;
- Les paramètres non autorisés ou incohérents.

Les contrôles de syntaxe ou de validité doivent être doublés (côté client et côté serveur).

Exigences sur le processus de développement et maintenance logicielle

Traçabilité des composants et interfaces

Ex-122 [OCS] : Le titulaire doit assurer la traçabilité des interfaces mises à disposition des systèmes internes et externes. Celle-ci doit passer par des moyens techniques comme une séparation franche des modules et de leur mode de déploiement, une utilisation cohérente des espaces de nommage à tous les niveaux où ils existent (namespaces java, dépendances entre librairies, namespace des documents XML, adresses des services, ...). Des frameworks peuvent éventuellement venir renforcer ces bonnes pratiques.

Page 38 of 46	<p style="text-align: center;"><u>Afpa-CCTG-FRI</u></p> <p style="text-align: center;">Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique</p>	
Version 1.1		<p style="text-align: center;">Direction des Systèmes d'Information</p>

Ex-123 [OCS] : Le titulaire doit également assurer la traçabilité par la mise en place des procédures adaptées et par une gestion de documentation rigoureuse permettant de décrire les dépendances entre modules, de suivre l'évolution de ces dépendances au fil du temps et des évolutions des composants.

Mise en place et traçabilité des différentes plates-formes

Ex-124 [S] : La gestion du cycle de vie des solutions doit comprendre un ensemble de procédures et de documents spécifiques permettant d'assurer la traçabilité des composants sur les différentes plates-formes utilisées pour la réalisation et les évolutions (plate-forme de développement, d'intégration, de tests techniques, de validation fonctionnelle, de formation, de production(s), ...). Ces procédures doivent permettre de garantir en permanence la maîtrise des environnements en définissant les processus et les critères permettant à un composant de basculer d'un environnement à un autre. Ces processus doivent identifier les acteurs, définir les critères et méthodes de validation permettant pour chaque composant de passer d'un environnement à un autre. Ces éléments doivent permettre d'identifier de façon certaine quels composants sont installés sur quelles plateformes et dans quelles versions.

Audit de qualité logicielle

Ex-125 [S] : Le Titulaire doit produire un rapport d'audit de qualité logicielle (architecture logicielle, code, documentation) conformément aux bonnes pratiques de production logicielle.

Ex-126 [S] : Le Titulaire s'engage à donner à l'Afpa si elle en fait la demande les moyens nécessaires à la validation de ces rapports (accès aux outils d'audit utilisés, régénération de rapport d'audit de code à partir d'échantillons de code...).

3.4. Règles de déploiement

Localisation des composants

Ex-127 [OC] : La solution doit être installée dans un répertoire d'installation dédié. Le nom de ce répertoire doit être paramétrable.

Ex-128 [OC] : Pour une application client lourd, si la solution personnalise des éléments pour les utilisateurs, ce paramétrage doit être stocké dans un répertoire ou la ruche de la base de registre personnel de l'utilisateur.

Page 39 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

Localisation sur serveur

Ex-129 [OC] : Tous les composants d'une application sur une machine donnée doivent être regroupés dans l'arborescence de l'application.

Localisation sur poste de travail

Ex-130 [OC] : Pour une application client lourd, le répertoire d'installation doit être un sous répertoire du répertoire où sont installés tous les logiciels sur un poste Pédago (par défaut le répertoire C:\Program Files pour Microsoft Windows).

Stockage des fichiers sur un serveur

Ex-131 [OC] : Si la solution stocke des fichiers (documents bureautiques, multimédia, graphiques...) sur un serveur, elle doit être :

- Dans la base de données de l'application en utilisant des mécanismes de type BLOB ou assimilé ;
- Dans l'arborescence de l'application du serveur de données ;
- Dans un serveur ou une application de gestion de fichiers (ex : SharePoint)

Volumétrie

Ex-132 [OCS] : Si le titulaire conçoit une solution qui génère un modèle de volume et de structure disproportionné (ex : plus de 30 niveaux d'arborescence, 500 000 fichiers pour l'application...), le titulaire devra indiquer et justifier le résultat et proposer des axes d'optimisation si envisageable.

3.5 Supervision applicative

Mécanismes de supervision

Ex-133 [OCS] : Toute application doit offrir des mécanismes permettant de la superviser techniquement et calculer un taux de disponibilité, en exposant par exemple une url de statut qui permet de s'assurer que le serveur applicatif est actif, et que la communication avec la base de données est opérationnelle.

Métriques

Ex-134 [OCS] : Toute application doit pouvoir rendre disponible des informations permettant de vérifier son bon fonctionnement, que ce soit par url, par API, ou au travers de fichiers de log. Celles-ci seront ensuite traduites en métriques / indicateurs fonctionnels / métiers dans le cadre des activités d'exploitation.

Gestion des logs et des erreurs

Ex-135 [OCS] : L'application doit pouvoir générer des logs avec un niveau de sévérité adapté (a minima ERROR, WARN, INFO, DEBUG) et configurable à chaud, pour permettre l'analyse et gérer les erreurs.

Ex-136 [OCS] : L'ensemble des erreurs techniques et fonctionnelles doivent être gérées, identifiées, documentées et horodatées (coupure réseau intempestive, flux fonctionnel erroné...).

Page 40 of 46	<u>Afpa-CCTG-FRI</u>	
Version 1.1	Cahier des Clauses Techniques Générales pour les marchés de Fournitures et de Réalisation Informatique	Direction des Systèmes d'Information

Ex-137 [OCS] : L'application doit permettre de mettre en place un mécanisme de rotation des logs et configurable à chaud sur une fenêtre temporelle pour éviter la saturation des espaces disques.

Performance **Ex-138 [OCS]** : L'application doit pouvoir être en mesure de partager des informations liées à sa performance (temps de réponse...).

Rapport et décisionnel

Pour information, l'Afpa dispose de la solution Power BI pour couvrir les éventuelles activités de reporting.

4. Annexes

Objet

Ce chapitre liste les noms et les versions de produits mis en œuvre :

- **Palier actuel** : Assemblage cohérent tels que défini au chapitre 1.2
- **Palier à venir** : Assemblage cohérent tel que défini au chapitre 1.2. Un nouveau palier est le plus souvent lié à une nouvelle version de système d'exploitation.
- **Produits actuels** : briques techniques, indépendantes des notions de paliers, prescrites à la date de publication du CCTG-FRI ;
- **Produits à venir** : briques que l'Afpa envisage de mettre en œuvre, lorsqu'elles sont connues ou pressenties.

Tout nouveau projet doit démarrer sur les paliers à venir et être compatible avec les solutions fonctionnant sur les paliers antérieurs.

4.1. Infrastructure

<i>Réseaux</i>	Produits actuels	Produits à venir
Métrologie	Cacti	Pas de projet d'évolution connu

<i>Serveurs et systèmes d'exploitation</i>	Paliers actuel	Paliers à venir
Socle de virtualisation	VMWARE ESX 6.5 update 3	VMWARE ESX 7
Socle Linux pour les serveurs applicatifs	Linux RHEL ES 6.5 (64 bits) (*) Linux CentOS 6.5 (64 bits) Linux CentOS 7 (64 bits)	Linux RHEL ES 8 (64 bits)
Système d'exploitation	Linux RHEL ES 6.5 (64 bits) (*) Linux CentOS 6.5 (64 bits) Linux CentOS 7 (64 bits)	Linux RHEL ES 8 (64 bits)
Java	JRE 1.6 à 1.9	JRE 8

Socle Linux pour les serveurs de données	Linux RHEL ES 6.5 (64 bits) (*) Linux CentOS 6.5 (64 bits) Linux CentOS 7 (64 bits)	Linux RHEL ES 8 (64 bits)
--	---	---------------------------

(*) L'Afpa pouvant être amenée à faire évoluer le socle OS (à la suite de dysfonctionnements, recommandations éditeur, ...), les fournitures doivent supporter l'application de paliers mineurs sans retouche du code.

<i>Middlewarees (Socle Linux)</i>	Produits actuels	Produits à venir
Serveur WEB	Apache 2.2	Apache 2.4
Conteneur de Servlet, moteur JSP	Tomcat 7.0	Tomcat 10
Moteur PHP	PHP 5.3	PHP 8
SGBD PostgreSQL	PostgreSQL 9	PostgreSQL 14
SGBD Oracle	Oracle SGBD 11.2 Entreprise Edition	NA

<i>Middlewarees (Socle Linux, application internet)</i>	Produits actuels	Produits à venir
Serveur WEB	Apache Version fournie par Redhat avec RHEL 6.x	Pas d'évolution de stratégie prévue
Conteneur de Servlet, moteur JSP	Tomcat Version fournie par Redhat avec RHEL 6.x	Pas d'évolution de stratégie prévue
PHP	PHP Version fournie par Redhat avec RHEL 6.x	Pas d'évolution de stratégie prévue
SGBD PostgreSQL	PostgreSQL 9	PostgreSQL 14, Version fournie par Redhat avec RHEL

<i>Gestion des systèmes (Datacenter)</i>	Produits actuels	Produits à venir
Surveillance	Cacti	Pas de projet d'évolution connu

Hypervision	Appdynamics 4.2	Pas de projet d'évolution connu
Sauvegarde	Solution fournie par l'infogérant	Pas de projet d'évolution connu
Automatisation	Automator 3.7	Pas de projet d'évolution connu

<i>Gestion des systèmes (Infra Microsoft)</i>	Produits actuels	Produits à venir
Surveillance	Solution en cours d'acquisition	Solution en cours d'acquisition
Hypervision	Appdynamics 4.2	Pas de projet d'évolution connu
Sauvegarde	Solution fournie par l'infogérant	Pas de projet d'évolution connu
Automatisation	Automator 3.7	Pas de projet d'évolution connu

<i>Ressources utilisateurs (Logiciels de base Postes Pédago)</i>	Palier actuel	Palier à venir
Système d'exploitation	Windows 10	Pas de projet d'évolution connu
Framework	.NET 4.0	Pas de projet d'évolution connu
Suite bureautique	Office 2016	Office 365
Traitement de Texte	Word 2016	Word 365
Tableur	Excel 2016	Excel 365
Outil de présentation	PowerPoint 2016	PowerPoint 365
Client de Messagerie	Outlook 2016	Outlook 365
Client d'agenda partagé	Outlook 2016	Outlook 365
Lecteur de PDF	Adobe Acrobat Reader 11.0.10	Produit sujet à évolution permanente en fonction des correctifs de sécurité
Navigateur	Internet Explorer 11	Microsoft Edge Chromium

Plugin Navigateur	JRE 1.6.0_16	Produit sujet à évolution permanente en fonction des correctifs de sécurité
Plugin Navigateur	Produit interdit : Flash Player	Produit interdit : Flash Player
Moteur d'accès aux données	ODBC Engine	ODBC Engine v17 Pas de projet d'évolution connu

Les postes Pédago dont la capacité technique à faire fonctionner Windows 10 est jugée insuffisante verront leur renouvellement anticipé à l'occasion de la migration sur ce palier.

<i>Ressources utilisateurs (Logiciels optionnels, Postes Pédago)</i>	Produits actuels	Produits à venir
Éditeur de PDF	Adobe Acrobat Pro 9.2	Adobe Acrobat Pro 11
Émulation mode caractère	Putty 0.74	Pas de projet d'évolution connu

<i>Ressources utilisateurs (Terminaux mobiles)</i>	Palier actuel	Palier à venir
Système d'exploitation	<ul style="list-style-type: none"> IOS (version >= 11) Android (version >= 10) 	<ul style="list-style-type: none"> IOS (version >= 15) Android (version >= 12)

<i>Services frontaux</i>	Produits actuels	Produits à venir
Messagerie	Exchange 2010 / 2013 / Online	Exchange Online
Applications intranet	Portail Jalios	Mozzaik365 sur Sharepoint Online
Gestionnaire de contenu	JCMS de Jalios	Mozzaik365 sur Sharepoint Online

4.2. Développement

<i>Services d'échange</i>	Produits actuels	Produits à venir
ETL & ESB	Talend Open Studio : dernière version réputée stable	

<i>Outil décisionnel</i>	Produits actuels	Produits à venir
Power BI	Power BI v2.91	Pas de projet d'évolution connu

<i>Gestion des composants</i>	Produits actuels	Produits à venir
Gestion des sources	Gitlab v 10.8.3 / Github	Gitlab v14.5.2
Tests de montée en charge	Gatling	Pas de projet d'évolution connu
Tests fonctionnels sur Serveur	Solution en cours d'acquisition	Pas de projet d'évolution connu
Tests fonctionnels sur poste client	Solution en cours d'acquisition	Pas de projet d'évolution connu
PIC	Jenkins 1.461	Jenkins 2.3
PIC	Sonar 3.0.1	Sonar 8

<i>Java</i>	Produits actuels	Produits à venir
Versions préconisées	JDK Java de 1.6 à 1.9	JDK Java 17
Environnement de développement	Eclipse IDE 4, intelli J	Pas de projet d'évolution connu
Outil de compilation	Maven 3	Pas de projet d'évolution connu
Tests unitaires	JUnit 4	JUnit 5
Documentation	JavaDoc	Pas de projet d'évolution connu
Framework	<ul style="list-style-type: none"> Angular React Vue.js 	Dernier palier stable connu

Conteneur léger	Spring 3.1.2	Spring 5
Présentation poste client	SWT	Produit interdit : SWT
Présentation HTML	Spring MVC	Spring 5
Logs	Log4j	Dernier palier stable connu
Mapping Relationnel Objet	Hibernate 5	Pas de projet d'évolution connu
Mapping Relationnel Objet	EclipseLink	Produit interdit : EclipseLink

<i>PHP</i>	Produits actuels	Produits à venir
Versions préconisées	PHP 7	PHP 8
Environnement de développement	Eclipse IDE 4, intelli J	Pas de projet d'évolution connu
Tests unitaires	PHPUnit	Pas de projet d'évolution connu
Documentation	DOCBlox	Pas de projet d'évolution connu
Framework	Symfony	Symfony 5.3
Mapping Relationnel Objet	Symfony 1.4 / 2.x avec doctrine ORM	Symfony 5.3
Présentation	Symfony	Symfony 5.3