Département des
Systèmes d'Information

CADRE DE REFERENCE TECHNIQUE SI

Date	Version
26/02/2026	v4.21

AFD
AGENCE FRANÇAISE
DE DÉVELOPPEMENT

Sommaire

I. Objectifs 5
II. Principes généraux 5
III. Structure 6
IV. Ensemble des domaines et leurs affinités 6
V. Classification (maturité technologique) 7
VI. Respect du cadre 7
VII. Cadre Technique 8
1. Solution de génie logiciel 8
1.1.1. Aide au développement d'application 8
2. Composant d'application 8
2.1. Technologie 8
2.1.1. Tiers de Présentation ([1/3 = P] Interface / Boundary / Front-End) 8
2.1.2. Tiers d'Application ([2/3 = A] Business-Rule / Back-End) 8
2.1.3. Tiers de Donnée ([3/3 = D] Donnée / Data / Back-End) 9
2.2. Analyses, Rapports et Statistiques 9
2.2.1. Communication de données (Reporting) 9
2.2.2. Affichage dynamique des données (Dashbording & Data Vizualisation) 9
2.2.3. Analyse des usages 9
2.3. Automatisation et gestion des processus 9
2.3.1. Gestion des processus 9
2.4. Communications unifiées et collaboration 9
2.4.1. Outillage collaboratif 10
2.5. Gestion des documents et du contenu 10
2.5.1. Système de gestion documentaire (GED) 10
2.5.2. Gestion de contenu Web (CMS) 10
2.5.3. Réseau Social Entreprise (RSE) 10
3. Intégration / Middleware 10
3.1.1. Bus d'entreprise 10
3.1.2. Echange de fichiers 10
3.1.3. Echange de messages 11
3.1.4. API Management 11

4. Gestion des données 11
4.1.1. Extraction, transformation & chargement (ETL) 11
4.1.2. Master Data Management (MDM) 11
5. Appareils de l'utilisateur final 11
5.1. Matériel 11
5.1.1. Espace de travail & Ergonomie 12
5.1.2. Ordinateur (fixe, portable) ou tablette 12
5.1.3. Téléphone portable (Smartphone) 12
5.2. Système d'exploitation 12
5.2.1. Ordinateur (fixe, portable) ou tablette 12
5.3. Logiciel embarqué 13
5.3.1. Ordinateur (fixe, portable) ou tablette 13
5.3.2. Téléphone portable (Smartphone) 14
6. Plate-forme de services 14
6.1. Matériel 14
6.1.1. Virtualisation 14
6.2. Système d'exploitation 14
6.2.1. Serveur 14
6.3. Containerisation 14
6.3.1. Moteur de Containers 15
6.3.2. Registry d'images 15
6.3.3. Reverse Proxy et présentation de certificats 15
6.3.4. Console d'administration 15
6.4. Serveur 15
6.4.1. Serveur Web ou d'Application 15
6.4.2. Serveur de data-visualisation 15
6.4.3. Serveur de communication 16
6.5. Stockage de données 16
6.5.1. Base de données SQL (SGBDR) 16
6.5.2. Base de Données No-SQL (SGBD) 16
6.6. Services 16
6.6.1. Solution en tant que service (SaaS) 16
6.6.2. Bureau en tant que service (VDI / DaaS) 17
6.6.3. Virtualisation d'application (RDS) 17

7. Télécom 17
7.1.1. Infrastructure 17
8. Sécurité de l'information 17
8.1. Gestion de la cybersécurité 17
8.1.1. Surveillance continue (SIEM) 17
8.1.2. Intégrité et confidentialité des données 18
8.1.3. Identification et authentification 18
8.2. Contrôles sécurité 19
8.2.1. Authentification et autorisation 19
8.2.2. Protection antivirale 19
9. Gestion des systèmes informatiques 19
9.1.1. Gestion des configurations 19
9.1.2. Surveillance des systèmes 19
9.1.3. Automatisation des processus (IT) 20
10. Développement et test 20
10.1.1. Structure logicielle (cadriciel / framework) 20
10.1.2. Outils de développement (IDE) 20
10.1.3. Gestion des configurations et versions 20
10.1.4. Validation et tests 21
11. Datacentre & local technique 21
11.1. Infrastructure 21
11.1.1. Continuité de service 21

I. OBJECTIFS

Dans un contexte d'évolution rapide de l'environnement métier et technique, l'objectif principal recherché par la Direction des Systèmes d'Informations est de disposer d'un SI maîtrisé, performant (aux besoins du moment) et en capacité d'évoluer rapidement pour délivrer de nouveaux services (réduction du Time2Market). Dans ce contexte, le document « Cadre de Référence Technique SI » a plusieurs vocations :

- assurer une bonne pérennité des composants de base par la mise en œuvre de démarches de choix instrumentées, et limiter la variabilité des plates-formes et des configurations par une évolution concertée des composants ;
- maîtriser les coûts d'acquisition des progiciels et des composants logiciels ainsi que ceux des services d'intégration et d'administration en évitant que chaque application n'impose ses propres composants de base ;
- assurer la maîtrise technique des environnements en limitant la multiplication des technologies et des méthodes ;
- permettre aux applications de partager dans de bonnes conditions l'infrastructure matérielle et l'infrastructure de communication ;
- permettre aux applications d'interopérer entre elles et avec les partenaires extérieurs ;
- maîtriser les évolutions du SI en s'accostant avec les nouveaux standards issus de l'innovation technologique.

II. PRINCIPES GENERAUX

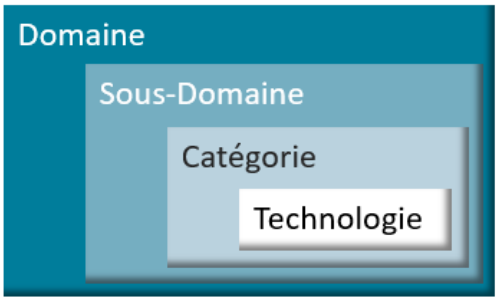
Le « Cadre de Référence Technique SI » classifie les technologies et standards à utiliser dans le cadre du déploiement des services SI. Il a pour objectif de définir les composants techniques utilisés par l'AFD, et un vocabulaire commun pour les acteurs informatiques, afin d'améliorer l'interopérabilité et favoriser la réutilisation. La standardisation des composants doit permettre des économies d'échelle dans le cadre du support, de l'exploitation et de la négociation des contrats cadres.

Pour chaque composant seront détaillées les préconisations de l'AFD en termes d'éditeur et de version.

Seules les technologies qui doivent être portées à la connaissance des soumissionnaires répondants aux appels d'offres sont évoquées dans le document.

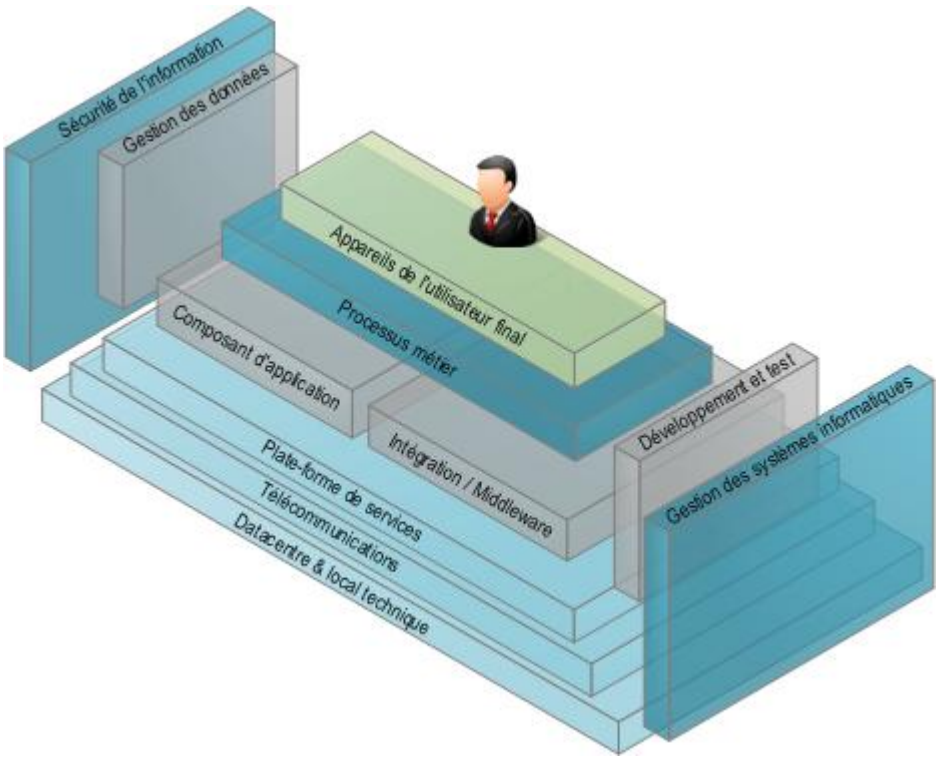
III. STRUCTURE

Afin de faciliter la lisibilité, des subdivisions thématiques sont définies pour classifier les technologies. Un premier niveau qualifié « Domaine », un sous niveau « Sous-Domaine » et un troisième « Catégorie » englobent les différentes technologies.



Chacune des technologies sera associée à un niveau de maturité dans le cadre de son cycle de vie.

IV. ENSEMBLE DES DOMAINES ET LEURS AFFINITES



V. CLASSIFICATION (MATURITE TECHNOLOGIQUE)

Les niveaux de maturité des technologies sont définis comme tels :

- Technologie « **Préconisée** » : Technologie logicielle ou matérielle fortement conseillée pour l'alignement à la stratégie définie par la DSI. Elle est déployée dans le SI pour des activités de production.
- Technologie « **Acceptée** » : Technologie logicielle ou matérielle maîtrisée par l'AFD. Elle est déployée dans le SI pour des activités de production.

VI. RESPECT DU CADRE

Les technologies « **Préconisée** » doivent être utilisées **en priorité** dans le cadre des projets et des évolutions du système d'information.

Il est **OBLIGATOIRE** pour toutes équipes projet de spécifier et justifier le non-respect d'une technologie « **Préconisée** ». Ces écarts devront être présentées pour validation au comité d'architecture de la DSI.

Le cadre technique préconise généralement les technologies dans leur version majeure (1 ou 2 digits) ; cependant **les composants à installer doivent se baser sur leur version mineure supportée et la plus sécurisée**.

VII. CADRE TECHNIQUE

1. Solution de génie logiciel

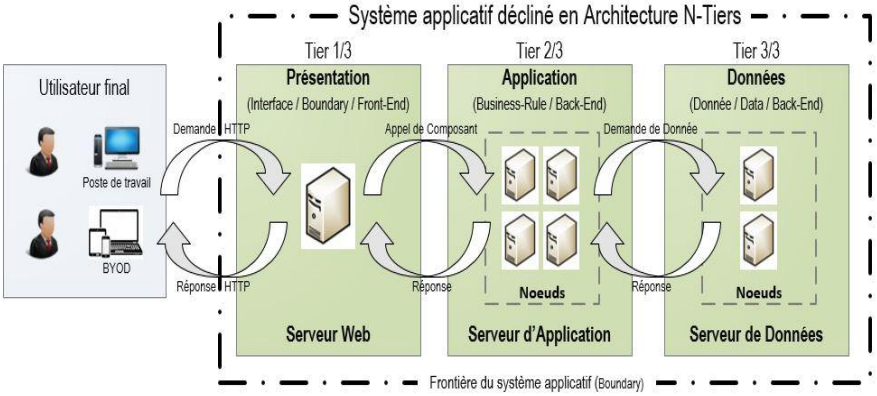
1.1.1. Aide au développement d'application

Cette catégorie représente les solutions utilisées pour la réalisation d'applications métiers.

Description	Acceptée	Préconisée
Low-code	• Simplicité 5.x	

2. Composant d'application

2.1. Technologie



2.1.1. Tiers de Présentation ([1/3 = P] Interface / Boundary / Front-End)

Cette catégorie représente les composants logiciels nécessaires à la couche de présentation d'une application en architecture N/tiers.

Exigence(s) - Tiers de Présentation ([1/3 = P] Interface / Boundary / Front-End)
RGAA & Handicap : Respect des principes d'accessibilités aux services numériques accessibles à toutes et à tous. L'accessibilité numérique consiste à rendre les contenus et services numériques compréhensibles et utilisables par les personnes en situation de handicap. Dans le cas de site internet, et en application de la loi n° 2005-102 du 11 février 2005 ; complété du décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne, la DINUM a publié la 4e version du RGAA (Référentiel Général d'Amélioration de l'Accessibilité) - https://accessibilite.numerique.gouv.fr/. L'obtention d'un audit d'accessibilité se réalise depuis cette adresse - https://ara.numerique.gouv.fr/
Google Angular - Politique de version : Compte tenu de l'importante fréquence d'apparition des versions ; l'AFD ne retiendra que les versions paires de la technologie Angular.

Description	Acceptée	Préconisée
Angular		**• Google Angular 20.x • Framework-AFD v3 IHM (Angular 20.x)**
PHP	• PHP 8.x (RHEL) sur dérogation	

2.1.2. Tiers d'Application ([2/3 = A] Business-Rule / Back-End)

Cette catégorie représente les composants logiciels nécessaires au développement et à l'exécution d'une application en architecture N/tiers.

Exigence(s) - Tiers d'Application ([2/3 = A] Business-Rule / Back-End)
Le composant "Java (Runtime)" est utilisable pour l'exécution mais pas pour le développement d'application.

Description	Acceptée	Préconisée
.Net (Win & Linux)	• Microsoft .Net 8.x (LTS)	**• Microsoft .Net 10.x (LTS)** **• Framework-AFD v3 APP (.Net 8.x)**
Java (Framework)	• Spring Boot 3.5.x	
Java (Runtime)	• Open JDK 17 (RHEL LTS)	**• Open JDK 21 (RHEL LTS)**

2.1.3. Tiers de Donnée ([3/3 = D] Donnée / Data / Back-End)

Cette catégorie représente les composants logiciels nécessaires à la persistance et à l'accès aux données d'une application en architecture N/tiers.

Exigence(s) - Tiers de Donnée ([3/3 = D] Donnée / Data / Back-End)
(Nota) Se reporter à la rubrique "Stockage de données" pour le détail des versions recommandées.

Description	Acceptée	Préconisée
Data / Accès		**• Framework-AFD v3 BDD (PostgreSQL 16.x)**
Data / Persistance		**• Voir rubrique "Stockage de données"**

2.2. Analyses, Rapports et Statistiques

2.2.1. Communication de données (Reporting)

Cette catégorie représente les outils et composants logiciels nécessaires à la réalisation de rapports sur les données.

Description	Acceptée	Préconisée
Reporting	• JasperReports Server 9.0.x (LTS)	**• SAP Business Objects BI 4.3**

2.2.2. Affichage dynamique des données (Dashbording & Data Vizualisation)

Cette catégorie représente les outils et composants logiciels nécessaires à la réalisation d'analyses dynamique sur les données.

Description	Acceptée	Préconisée
Dashbord & DataViz		**• Microsoft Power BI Desktop 2025/05**
Elasticsearch / DataVis	• Elastic Kibana 8.18.x	

2.2.3. Analyse des usages

Cette catégorie représente les outils et composants logiciels nécessaires à la réalisation d'analyses des usages d'applications tel que l'analyse des audiences d'un site Internet

Description	Acceptée	Préconisée
Web Analytics		**• Piano Analytics (SaaS)**

2.3. Automatisation et gestion des processus

2.3.1. Gestion des processus

Cette catégorie représente les applications et logiciels de gestion des processus métier.

Description	Acceptée	Préconisée
BPM / Low-code		**• Bonitasoft Bonita 2024.x**
RPA		**• UiPath Orchestrator 2022.10**

2.4. Communications unifiées et collaboration

2.4.1. Outillage collaboratif

Cette catégorie représente les applications et logiciels qui permettent de faciliter la collaboration au sein d'une entreprise et avec des tiers. Ce type d'outil permet de partager des fichiers de travail entre les collaborateurs internes de l'entreprise et d'éventuels partenaires externes. Chacun est en mesure de modifier et d'ajouter des informations en ligne.

Description	Acceptée	Préconisée
Collaboratif		• **Jalios JCMS 10.x**

2.5. Gestion des documents et du contenu

2.5.1. Système de gestion documentaire (GED)

(GED) Gestion Electronique de Document. Cette catégorie représente les applications ou composants logiciels utilisés pour suivre, stocker et récupérer des documents électroniques et/ou des images de documents papier.

Description	Acceptée	Préconisée
GED	• Microsoft SharePoint 2019	

2.5.2. Gestion de contenu Web (CMS)

Cette catégorie représente les applications ou composants logiciels prenant en charge la création de contenu, la révision, l'approbation de contenu, le balisage, l'agrégation, la publication, la livraison de contenu et la gestion de la syndication.

Description	Acceptée	Préconisée
CMS	• Jalios JCMS 10.x • Microsoft SharePoint 2019	• **Drupal 11.x**

2.5.3. Réseau Social Entreprise (RSE)

Cette catégorie représente les applications ou composants logiciels prenant en charge le réseau social d'entreprise ou RSE est un réseau social classique mais décliné et adapté pour le cadre professionnel en entreprise.

Description	Acceptée	Préconisée
RSE		• **Jalios JCMS 10.x**

3. Intégration / Middleware

3.1.1. Bus d'entreprise

Cette catégorie représente les applications ou composants logiciels utilisés pour concevoir et mettre en œuvre l'interaction et la communication entre des applications logicielles.

Description	Acceptée	Préconisée
ESB		• **Red Hat Fuse 7.x**

3.1.2. Echange de fichiers

Cette catégorie représente les applications ou composants logiciels permettant la transmission de fichiers entre différents systèmes et actifs informatiques.

Description	Acceptée	Préconisée
Transferts externes		• **Axway Transfer CFT 3.x**

3.1.3. Echange de messages

Cette catégorie représente les applications ou composants logiciels permettant la transmission de messages d'information entre différents systèmes et actifs informatiques à l'aide de différentes technologies de communication de type Queue.

3.1.3.a. Broker de messages

Description	Acceptée	Préconisée
MOM	• Apache ActiveMQ 6.x	

3.1.3.b. Streaming données distribuées

Description	Acceptée	Préconisée
Connecteur Java/Kafka		• **Kafka Java Client 3.3** • **Spring Kafka 3.3.x**
Connecteur autre		• **Kafka Streams 3.6**
MOM		• **Kafka Confluent Community 7.6.x** • **Kafka Confluent Entreprise 7.6.x**

3.1.4. API Management

Cette catégorie représente une plateforme mettant en oeuvre un ensemble de processus, composants techniques et de pratiques visant à créer, publier, sécuriser, surveiller et gérer l'utilisation des API

3.1.4.a. APIM

Description	Acceptée	Préconisée
APIM		• **Gravitee 4.9.x**

4. Gestion des données

4.1.1. Extraction, transformation & chargement (ETL)

Cette catégorie représente les logiciels qui prennent en charge l'extraction de données, la transformation de données puis le chargement de données.

Description	Acceptée	Préconisée
ETL		• **Informatica PowerCenter 10.5.x**
Elasticsearch / Logs & Métrics		• **Elastic Logstash 8.18.x**

4.1.2. Master Data Management (MDM)

Cette catégorie représente les applications et logiciels prenant en charge un ensemble de processus et d'outils qui définissent et gèrent de manière cohérente les données de référence.

Description	Acceptée	Préconisée
MDM		• **Semarchy xDM 2024.1.x (LTS)**

5. Appareils de l'utilisateur final

5.1. Matériel

5.1.1. Espace de travail & Ergonomie

L'espace de travail correspond à l'emplacement où s'effectue une activité d'un travail et qui nécessite généralement des équipements nécessaires à l'accomplissement de cette tâche.

Exigence(s) - Espace de travail & Ergonomie
Un espace de travail 'Standard AFD' est équipé d'un écran d'au moins 23 pouces ; avec résolution minimale de 1024x768.
Complément d'information : • Utilisation de la résolution 1024x768 (minimale) pour les applications client/serveur • Site WEB en mode « responsive design » : - 960x640 (DVGA) - 1024x720 (HD / WXGA) - 1280x1024 (SXVGA) - 1920x1080 (PC fixe 23'' ou supérieur) - 1366x768 (PC 13'' pour les portables)

5.1.2. Ordinateur (fixe, portable) ou tablette

Cette catégorie représente les appareils technologiques destinés aux utilisateurs finaux.

Exigence(s) - Ordinateur (fixe, portable) ou tablette
Un ordinateur 'Standard AFD' est équipé : • d'un CPU de type Intel® Core • d'au minimum 8 Go de mémoire

Description	Acceptée	Préconisée
Portable		• **Hewlett-Packard EliteBook x**

5.1.3. Téléphone portable (Smartphone)

Un téléphone cellulaire (Smartphone) exécute de nombreuses fonctions d'un ordinateur, ayant généralement une interface à écran tactile, un accès Internet et un système d'exploitation capable d'exécuter des applications téléchargées.

Exigence(s) - Téléphone portable (Smartphone)
Un téléphone cellulaire 'Standard AFD' est généralement de type iPhone, équipé : • d'un système d'exploitation de type iOS • d'un terminal disposant d'un écran < 7" • d'une connectivité au réseau de téléphonie
Conteneurisation des applications téléphonique : • La flotte de téléphonie portable AFD dispose du système de gestion d'appareil mobile « BlackBerry Enterprise Mobility Suite » • Les applications mobiles déployées sur ces téléphones doivent être conteneurisées au sein du « MDM BlackBerry »

Description	Acceptée	Préconisée
Smartphone		• **Apple iPhone**

5.2. Système d'exploitation

5.2.1. Ordinateur (fixe, portable) ou tablette

Cette catégorie représente les systèmes d'exploitation intégrés aux appareils technologiques destinés aux utilisateurs finaux.

Exigence(s) - Ordinateur (fixe, portable) ou tablette
Un ordinateur 'Standard AFD' est équipé d'un système d'exploitation Microsoft Windows 64 bits (Nota) Se reporter aux paragraphes technologiques concernés pour le détail des versions recommandées.

Description	Acceptée	Préconisée
Windows		• **Microsoft Windows 11 Entreprise 24H2**
iPAD		• **Apple iOS**

5.3. Logiciel embarqué

5.3.1. Ordinateur (fixe, portable) ou tablette

Cette catégorie représente les composants intégrés aux appareils technologiques destinés aux utilisateurs finaux.

Exigence(s) - Ordinateur (fixe, portable) ou tablette
Un ordinateur 'Standard AFD' est équipé : • d'un système d'exploitation Microsoft Windows • du navigateur Microsoft Edge Chromium • de l'outil de Messagerie Microsoft Outlook • d'un package bureautique Microsoft Office 64 Bits • d'un environnement JRE Java • d'un environnement Microsoft .NET Framework (Nota) D'autres logiciels sont présents sur le poste (Compression, Antivirus, Acrobat Reader, Chiffrement de données, ...) et ne sont pas spécifiquement mentionnés ici. Ils n'ont pas d'impact sur les choix des logiciels Métiers et/ou sur les développements spécifiques liés aux postes de travail. Se reporter aux paragraphes technologiques concernés pour le détail des versions recommandées.
Les postes de travail AFD sont protégés par la mise en œuvre de stratégies système qui restreignent les droits d'accès au système de fichiers des postes. En conséquence, les applications doivent respecter les contraintes suivantes : • Aucune écriture ne doit être effectuée dans les répertoires systèmes, ni dans les parties « système » de la base de registre des postes • L'utilisation des logiciels doit pouvoir être exécutée avec un profil « Utilisateur » au maximum • L'installation des produits doit être indépendante de l'architecture interne de la machine (organisation des disques de données, …) ; les répertoires d'installation doivent donc être paramétrables • L'utilisation de plug-in de type <Applet Java>, <Contrôle active X>, <Flash>, <Flex>, etc.. n'est pas autorisée
L'Authentification Multifacteur (MFA) devient obligatoire à partir du 22/01/2024 pour tout accès au SI de l'AFD depuis un réseau-externe. A partir de cette date ; pour que l'interconnexion soit fonctionnelle ; l'application 'TrustBuilder Authenticator' doit impérativement être installée sur le device (version précisée ci-dessous)

5.3.1.a. Bureautique

Description	Acceptée	Préconisée
Bureautique		• **Microsoft Office LTSC 2024 Professional Plus**
Lecteur PDF		• **Adobe Acrobat Reader DC**

5.3.1.b. Communication

Description	Acceptée	Préconisée
Messagerie Instantanée		• **Microsoft Skype Entreprise LTSC 2024**
Visioconférence		• **Pexip Meetings**
Webinars		• **Livestorm**

5.3.1.c. Navigateur

Description	Acceptée	Préconisée
Microsoft Edge		• **Microsoft Edge-Chromium**
Mozilla	• Mozilla Firefox (ESR)	

5.3.1.d. Sécurité

Description	Acceptée	Préconisée
(MFA) Authentification Multifacteur		• **TrustBuilder Authenticator 6.x (PC)**

5.3.2. Téléphone portable (Smartphone)

Cette catégorie représente des logiciels intégrés à la téléphonie portable destinés aux utilisateurs finaux de l'entreprise (ex: Bulle Goods)

Exigence(s) - Téléphone portable (Smartphone)
L'Authentification Multifacteur (MFA) devient obligatoire à partir du 22/01/2024 pour tout accès au SI de l'AFD depuis un réseau-externe. A partir de cette date ; pour que l'interconnexion soit fonctionnelle ; l'application 'TrustBuilder Authenticator' doit impérativement être installée sur le téléphone (version précisée ci-dessous)

5.3.2.a. Sécurité

Description	Acceptée	Préconisée
(MFA) Authentification Multifacteur		• **TrustBuilder Authenticator 6.x (Tel.)**

6. Plate-forme de services

6.1. Matériel

6.1.1. Virtualisation

Cette catégorie représente les éléments de virtualisation (création d'une version virtuelle plutôt que réelle) qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation.

Exigence(s) - Virtualisation
Dans le système d'information AFD, les serveurs sont virtualisées via la technologie 'VMware ESX Server' excepté les serveurs de bases de données ORACLE virtualisées via la technologie 'Nutanix'.

Description	Acceptée	Préconisée
Linux / Windows		• **VMware ESXi Server 8.0**
Linux	• Nutanix 5.x	

6.2. Système d'exploitation

6.2.1. Serveur

Cette catégorie représente les systèmes d'exploitation intégrés aux serveurs (physiques ou virtuels).

Exigence(s) - Serveur
Un serveur 'Standard AFD' est équipé au minimum d'un système d'exploitation 64 bits.
(*) Attention : le nouvel OS Windows Server 2025 n'est pas compatible avec l'orchestration ITPAM actuellement déployée. Pour un besoin d'orchestration ; il est donc nécessaire d'utiliser une souche Windows Serveur 2022.

Description	Acceptée	Préconisée
Linux	• Red Hat Enterprise Linux 8.x	• **Red Hat Enterprise Linux 9.x**
Windows	• Microsoft Windows Server 2025 (*)	• **Microsoft Windows Server 2022**

6.3. Containerisation

6.3.1. Moteur de Containers

Cette catégorie représente les composants en capacité d'empaqueter une application et ses dépendances dans un conteneur isolé. Ce dernier pourra être exécuté sur n'importe quel serveur de manière indépendante de l'OS. Cette approche permet d'accroître la flexibilité et la portabilité d'exécution d'une application, laquelle va pouvoir tourner de façon fiable et prévisible sur une grande variété de machines hôtes, que ce soit sur la machine locale, un cloud privé ou public, une machine nue, etc

Description	Acceptée	Préconisée
Container		• **Podman 5.4.x (Souche RHEL)**

6.3.2. Registry d'images

Cette catégorie représente les composants nécessaires au stockage des images de conteneurs informatique

Description	Acceptée	Préconisée
Registry		• **GitLab Entreprise Edition Repo. 18.x**

6.3.3. Reverse Proxy et présentation de certificats

Cette catégorie représente les composants nécessaires au routage des flux dans les conteneurs et la présentation des certificats machines

Description	Acceptée	Préconisée
Admin. Container		• **Nginx Proxy Manager 2.12.x**

6.3.4. Console d'administration

Cette catégorie représente les composants nécessaires à l'administration des solutions de Containerisation

Description	Acceptée	Préconisée
Admin. Container		• **Portainer Community Edition 2.33.x (LTS)**

6.4. Serveur

6.4.1. Serveur Web ou d'Application

Cette catégorie représente les logiciels d'infrastructure offrant un contexte d'exécution pour des composants applicatifs.

Description	Acceptée	Préconisée
HTTP / ASP(x)	• Microsoft Internet Info. Services 10	
HTTP / Java	• Apache Tomcat 10.1.x	• **Red Hat JBoss Enterprise App.Platform 8**
HTTP	• Apache HTTPD 2.4 (RHEL8/9/10)	• **Nginx 1.24.x (RHEL8/9)**

6.4.2. Serveur de data-visualisation

Cette catégorie représente les logiciels d'infrastructure offrant un contexte d'exécution spécifiquement dédié à l'affichage dynamique des données (Dashbording & Data Vizualisation)

Description	Acceptée	Préconisée
Dashbord & DataViz		• **Microsoft Power BI Server 2025/05**

6.4.3. Serveur de communication

Cette catégorie représente les logiciels d'infrastructure offrant des services de communication ; tel que : téléphonie, messagerie, communication instantanée ou visioconférence.

Description	Acceptée	Préconisée
Messagerie Instantanée		• **Microsoft Skype for Business Server SE**
Messagerie		• **Microsoft Exchange Server SE**

6.5. Stockage de données

6.5.1. Base de données SQL (SGBDR)

(SGBDR) Système de Gestion de Base de données Relationnelles. Cette catégorie représente les systèmes de stockage de la donnée ; assurant la sécurité, le partage et la cohérence des données.

Description	Acceptée	Préconisée
PostgreSQL		• **PostgreSQL 16.x (RHEL)**
SQL Server	• Ms SQL Server 2019 (Si 2022 KO) • Ms SQL Server 2022 (Prioriser 2022)	

6.5.2. Base de Données No-SQL (SGBD)

Cette catégorie représente les bases de données non-relationnelles ; où l'information est organisée de manière optimisée selon des axes différents ; comme les bases de type colonne ou graph (Cassandra, HBase, MongoDB, DataStax, DB2 ..)

Description	Acceptée	Préconisée
Indexation en colonne	• Elastic Elasticsearch 8.18.x	

6.6. Services

6.6.1. Solution en tant que service (SaaS)

(SaaS) Solution as a Service. Cette catégorie représente les services de mise à disposition de solutions logicielles

Exigence(s) - Solution en tant que service (SaaS)
Une solution SaaS doit être accessible via un client léger (depuis un navigateur web) sans déploiement de logiciel tiers.
Une solution SaaS doit libérer automatiquement une connexion utilisateur au bout d'un certain temps d'inactivité paramétrable par l'administrateur.
Une solution SaaS doit permettre l'authentification et l'identification de l'utilisateur en SSO (Single Sign-On) via une connexion à la fédération d'identité de l'Agence Française de Développement par le protocole SAML v2. Pour plus de renseignement, se reporter au paragraphe "Sécurité de l'information / Gestion de la cybersécurité / Identification et authentification".
Une solution SaaS doit s'intégrer au type de poste de travail « standard » ; tel que décrit aux paragraphes "Appareils de l'utilisateur final / Matériel / Espace de travail et Ergonomie" et "Appareils de l'utilisateur final / Matériel / Ordinateur (fixe, portable) ou tablette".

6.6.1.a. Protection d'application

Description	Acceptée	Préconisée
(WAF) Web Application Firewall		• **Ubika Waap Cloud**

6.6.2. Bureau en tant que service (VDI / DaaS)

(VDI) Virtual Desktop Infrastructure / (DaaS) Desktop as a Service. Cette catégorie représente les services de fourniture d'un bureau virtuel à des utilisateurs finaux via une technologie de virtualisation

Exigence(s) - Bureau en tant que service (VDI / DaaS)
Les versions des systèmes mis à disposition via la plateforme de services doivent majoritairement correspondre à celles décrites à la rubrique 'Appareils de l'utilisateur final / Système d'exploitation / Ordinateur (fixe, portable) ou tablette'. La plateforme de services pourra néanmoins proposer des systèmes complémentaires qui ne sont pas nécessairement destinés aux utilisateurs finaux. Exemple : un écosystème AFD spécifiquement dédié aux développements.

Description	Acceptée	Préconisée
VDI		• **VMware Horizon 8.x**

6.6.3. Virtualisation d'application (RDS)

(RDS) Remote Desktop Services. Cette catégorie représente les services de mise à disposition d'application virtualisé ; particulièrement adapté pour les applications de type 'Client lourd'. Ce type de service permet de contourner une éventuelle problématique d'incompatibilité entre le poste de travail et la version du logiciel ou de l'un de ses composants embarqués.

Description	Acceptée	Préconisée
RDS		• **VMware Horizon 8.x**

7. Télécom

7.1.1. Infrastructure

Cette catégorie représente les systèmes d'infrastructure couvrant les diverses formes de matériel et de logiciel de base qui constituent la base d'un réseau.

Description	Acceptée	Préconisée
Load Balancer & Cache		• **F5-BIG-IP Local Traffic Manager 17.1.x**
Reverse Proxy		• **F5-BIG-IP Local Traffic Manager 17.1.x**

8. Sécurité de l'information

8.1. Gestion de la cybersécurité

8.1.1. Surveillance continue (SIEM)

Cette catégorie représente les composants du service de sécurité de l'information et de gestion des événements (SIEM). Cette surveillance continue fournit une analyse en temps réel des alertes de sécurité générées par les applications ou infrastructures serveurs et réseaux.

Description	Acceptée	Préconisée
Collecte logs & métrics		• **Suite-Elastic (voir rubrique "Logs & Métrics")**
SIEM		• **ITrust Reveelium**

8.1.2. Intégrité et confidentialité des données

Cette catégorie représente la gestion de l'intégrité et de la confidentialité des données implique la coordination de la collecte, du stockage, de la diffusion et de la destruction des données, ainsi que la gestion des politiques, des directives et des normes concernant la gestion des données, afin que la qualité des données soit maintenue et que les informations soient partagées ou disponibles conformément à la loi. et bonnes pratiques

Exigence(s) - Intégrité et confidentialité des données
Coffre-fort - Protection des secrets • La conservation d'éléments de référence supportant l'authentification (identifiants, mots-de-passe, etc..) doit être stockés chiffrés • Un contrôle d'accès préliminaire doit être effectué pour tout utilisation de ces éléments
Chiffrement des données au repos - Selon le niveau de confidentialité des données métier ; la solution doit mettre en place des mesures assurant la confidentialité des données au repos : • Les fichiers concernés ; véhiculés et/ou stockés devront être chiffrés • Quand nécessaire ; le système de stockage devra lui même être chiffré (File-Système et/ou BDD)
Chiffrement des flux - Selon le niveau de confidentialité des données métiers véhiculés ; la solution doit mettre en place des mesures assurant la confidentialité des données en transit.

8.1.2.a. Anonymisation et pseudonymisation

Description	Acceptée	Préconisée
(RGPD) Données		• **Anonimatron**

8.1.2.b. Chiffrement des données/flux

Description	Acceptée	Préconisée
Données		• **(PGP) Gpg4win 4.x**
Flux	• (TLS) Transport Layer Security 1.2	• **(TLS) Transport Layer Security 1.3**

8.1.2.c. Protection des secrets

Description	Acceptée	Préconisée
Coffre fort		• **HashiCorp Vault 1.17.x**

8.1.3. Identification et authentification

Cette catégorie représente les composants nécessaires à la prise en charge et la gestion des autorisations de connexion à un ordinateur, une application, un service ou un réseau et inclut la gestion des utilisateurs et la gestion des rôles/privilèges.

Exigence(s) - Identification et authentification
(SSO) Single Sign-On. Authentification des utilisateurs • Dans le SI de l'AFD, la mise en place d'une authentification SSO est exigée. En dessous de 10 utilisateurs une demande de dérogation pourra effectuée auprès du département sécurité qui évaluera sa pertinence en fonction des enjeux sécurité.

8.1.3.a. Authentification des accès

Description	Acceptée	Préconisée
(MFA) Authentification Multifacteur		• **InWebo TrustBuilder 6.x**
(SSO) Auth. Utilisateurs	• Kerberos	• **SAML v2**
Access Management		• **PingIdentity PingAM 7.3.x (ForgeRock AM)**
Web Cookies	• Shibboleth Service Provider 3.5.x	

8.1.3.b. Identification (utilisateurs ou systèmes)

Description	Acceptée	Préconisée
Demande de certificats		• **Evertrust Horizon v2.7.x**
Gestion des certificats		• **Evertrust Stream v2.1.x**
Identity Management		• **PingIdentity PingIDM 7.3.x (ForgeRock IDM)**
Identité Linux		• **Red Hat Identity Management**
Identité Windows		• **Microsoft Active Directory**

8.2. Contrôles sécurité

8.2.1. Authentification et autorisation

Cette catégorie représente les logiciels prenant en charge l'obtention d'informations sur les parties (personne ou système) tentant de se connecter à un système ou à une application à des fins de sécurité et la validation de ces utilisateurs.

Description	Acceptée	Préconisée
Lecteur de carte		• **AET Europe SafeSign 3**

8.2.2. Protection antivirale

Cette catégorie représente les logiciels utilisés pour empêcher, détecter et supprimer les programmes d'auto-réplication qui s'exécutent et se propagent en modifiant d'autres programmes ou fichiers.

Description	Acceptée	Préconisée
Antivirus		• **GLIMPS Malware**

9. Gestion des systèmes informatiques

9.1.1. Gestion des configurations

Cette catégorie représente les logiciels prenant en charge le processus de gestion des configurations système d'un ordinateur cible hébergé en DataCenter ou dédié à un utilisateur final.

9.1.1.a. Systèmes

Description	Acceptée	Préconisée
Windows		• **Microsoft Configuration Manager (SCCM) 2503**

9.1.2. Surveillance des systèmes

Cette catégorie représente les outils en charge de la surveillance des performances et des événements systèmes.

9.1.2.a. Logs & Métrics

Description	Acceptée	Préconisée
Agent de collecte		• ELK - Agents Elastic
Collecte logs Unix-Linux		• Rsyslog
Indexation des logs		• Elastic Elasticsearch 8.18.x
Normalisation des logs		• Elastic Logstash 8.18.x
Surveillance		• Centreon

9.1.3. Automatisation des processus (IT)

Cette catégorie représente les outils en charge de l'automatisation des processus IT (Intégration, déploiement, orchestration technique).

Description	Acceptée	Préconisée
Déploiement		• Red Hat Ansible Autom. Platform 2.4.x • GitLab Entreprise Edition CD 18.x • Microsoft Configuration Manager (SCCM) 2503
Gestion des artefacts		• Sonatype Nexus-repository 3.87.x
Infrastructure as Code		• Terraform 1.14.x
Intégration		• GitLab Entreprise Edition CI 18.x
Ordonnanceur		• Broadcom IT Process Autom. Manager

10. Développement et test

10.1.1. Structure logicielle (cadriciel / framework)

Cette catégorie représente les principes d'architecture logiciel ou de règles liées à la réalisation des applications du système d'information.

Exigence(s) - Structure logicielle (cadriciel / framework)
Patterns d'Architecture logicielle pour la réalisation d'applications pour l'AFD : • Pattern 3-n tiers - L'Architecture de référence AFD est basée sur un pattern 3-tiers (Présentation/Métier-Application/Persistance). Ce pattern est à privilégier dans l'architecture cible. Une architecture n-tiers (n>3) est envisageable si la solution le justifie. • Pattern Client Léger/Web - Le pattern client léger/web est privilégié à l'AFD. • Pattern Client Lourd - Le pattern client lourd ne sera retenu qu'en cas de contrainte forte et devra obligatoirement faire l'objet d'une validation de la part d'un comité d'Architecture. (Nota) Se reporter aux paragraphes technologiques concernés pour le détail des versions recommandées.
Principes et normes pour les interfaces Web. Les interfaces Web devront respecter les standards en termes de normes et standards émis par le W3C.

Description	Acceptée	Préconisée
Framework		• Framework-AFD v3

10.1.2. Outils de développement (IDE)

(IDE) Integrated Development Environment. Cette catégorie représente les environnements de programmation ou outils de développement.

10.1.2.a. Editeur

Description	Acceptée	Préconisée
.Net, C#		• Microsoft Visual Studio
Angular / PHP		• Microsoft Visual Studio Code
Java		• Eclipse

10.1.3. Gestion des configurations et versions

Cette catégorie représente les logiciels nécessaires pour suivre et contrôler les

changements dans la réalisation d'une application.

Description	Acceptée	Préconisée
Versioning		• GitLab Entreprise Edition Repo. 18.x

10.1.4. Validation et tests

Cette catégorie représente les logiciels prenant en charge les tests à travers les différents niveaux de test, types de test et processus/méthodologies de test. Les outils collectent ou génèrent également divers artefacts de test, y compris, mais sans s'y limiter, la matrice de traçabilité, les cas de test et les scripts de test.

10.1.4.a. Tests de non-régression (TNR)

Description	Acceptée	Préconisée
TNR		• Henix Squash TM 6.0.x

10.1.4.b. Tests de performance

Description	Acceptée	Préconisée
Perf. & Accéssibilité		• Google Lighthouse
Perf. & Charge aux limites		• NeoLoad 7.x

10.1.4.c. Tests qualité des développements

Description	Acceptée	Préconisée
Qualimétrie		• CAST Code Analysis 8.3.x

11. Datacentre & local technique

11.1. Infrastructure

11.1.1. Continuité de service

Cette catégorie représente les logiciels utilisés pour la sauvegarde de données, la reprise après sinistre, etc.

11.1.1.a. Sauvegarde des données

Description	Acceptée	Préconisée
Sauvegarde		• Rubrik 9.4.x