

POUVOIR ADJUDICATEUR

Agence Française de Développement (AFD)

5 rue Roland Barthes
75598 PARIS Cedex 12

OBJET DE LA CONSULTATION

Intitulé du marché :

Prestation pour un service bureau de paiement

**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES
(C.C.T.P.)**

1. Présentation de l'AFD et de son organisation	4
2. Présentation du Service Métier - Utilisateur	4
Objet du marché	6
3. 6	
3.1. Interfaces logicielles et services associés	6
3.2. Assistance et support fonctionnel	6
3.3. Sécurité et conformité	6
3.4. Audit et traçabilité	6
3.5. Contraintes et exigences macroscopiques	6
4. Présentation du Besoin	7
4.1. Contexte du besoin	7
4.2. Enjeu du besoin	7
5. Description des exigences fonctionnelles	7
5.1. Exigences fonctionnelles	7
5.1.1. Les messages	7
5.1.2. Gestion des contreparties	8
5.1.3. Relationship Management Application (RMA)	8
5.1.4. 4. Canaux de communication SWIFT	8
5.1.5. Disponibilité du service	8
5.1.6. Conformité et mises à jour SWIFT	9
5.1.7. Traçabilité et supervision	9
5.1.8. Sécurité et conformité	9
Description des exigences sécurité	9
6. 9	
6.1. Exigences de sécurité	9
6.1.1. Sécurité et conformité	9
6.1.2. Sécurisation des flux	9
6.1.3. Authentification et gestion des accès	10
6.1.4. Conformité SWIFT et gouvernance de la sécurité	10
6.1.5. Journalisation et traçabilité	10
6.1.6. Environnements et garantie PUPA	10
6.1.7. Continuité et récupération des données	10
6.1.8. Sous-traitance	11
6.2. Exigences sur les compétences attendues	11
6.2.1. Exigences de compétences du prestataire	11
6.2.2. Compétences fonctionnelles et techniques	11
6.2.3. Expertise métier	11
6.2.4. Dispositif de support et d'assistance	11
6.2.5. Compétences transverses et comportementales	12
6.2.6. Continuité des compétences	12
6.3. Exigences sur la protection des données personnelles	12
7. Type de prestation et forme de prix	13
7.1. Type de prestation	13
7.2. Forme de prix	13
8. Intégration de l'outil et mise en œuvre dans le système AFD	14
8.1. Principes généraux	14
8.2. Planning et délais	14
8.3. Environnements	14
8.4. Phase de tests et de recette	14
8.4.1. Tests d'intégration	14

8.4.2.	Recette fonctionnelle.....	14
8.4.3.	Tests en production (penny tests)	15
8.4.4.	Accompagnement et responsabilités	15
8.4.5.	Livrables attendus	15
8.4.6.	Vérification de Service Régulier (VSR).....	15
9.	Prestations de maintenance et support	16
9.1.	Répartition des responsabilités entre le prestataire et l'AFD en phase de maintenance	16
9.1.1.	Prise en charge de la TMA par l'intégrateur	16
9.1.2.	Responsabilités du prestataire	16
9.1.3.	Responsabilités de l'AFD	17
9.1.4.	Principes de collaboration	17
9.1.5.	Niveau de service.....	17
	1. Périmètre du SLA.....	17
	2. Engagement de disponibilité.....	17
	3. Gestion des incidents.....	17
	4. Support et communication	18
	5. Maintenance.....	18
	6. Indicateurs de performance (KPI)	18
	Règle de sécurité.....	19
10.	19	
11.	Réversibilité du service	20

1. Présentation de l'AFD et de son organisation

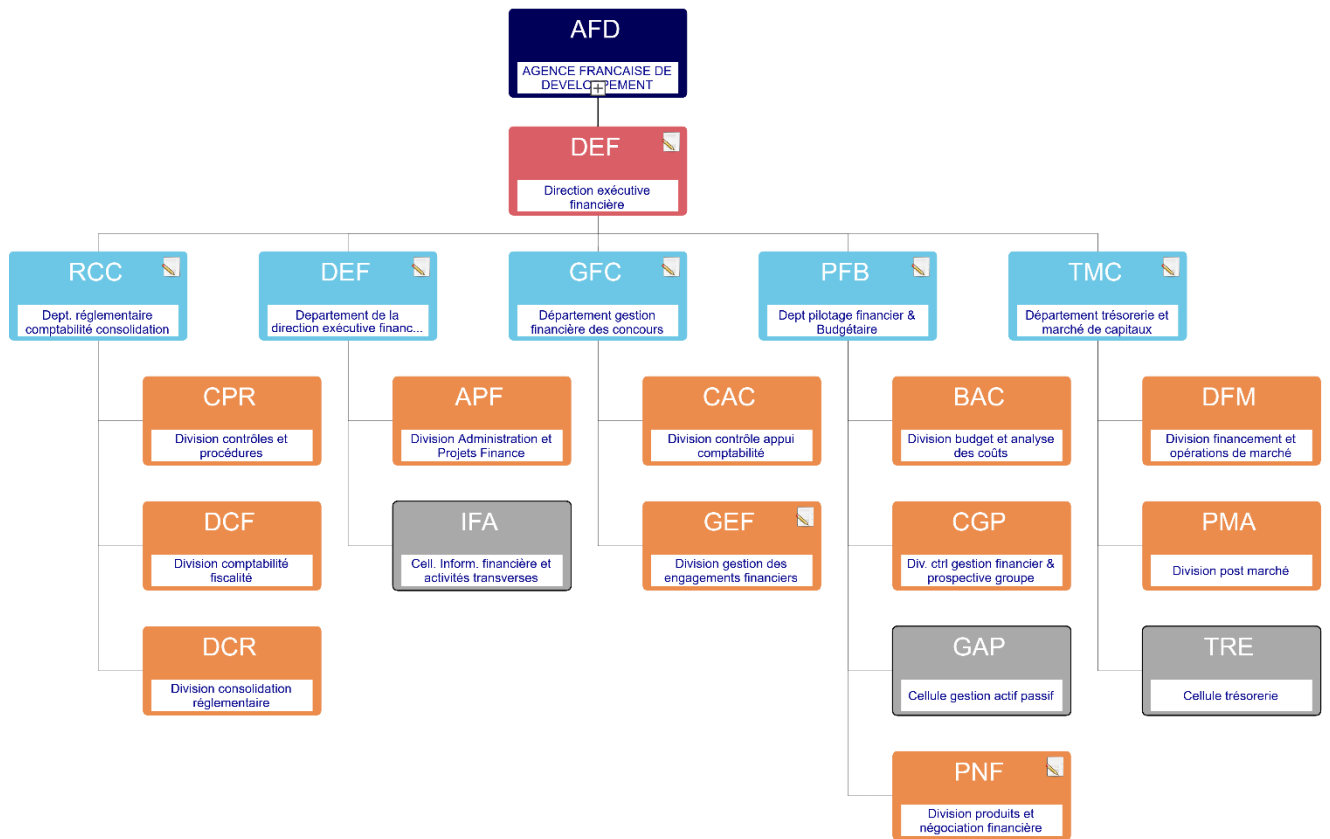
- Le site institutionnel www.afd.fr propose si besoin un niveau d'information plus approfondi.
- Le service prescripteur du présent marché est le Département des Systèmes Informatiques (DSI) rattaché au Secrétariat Général (SGN).
- Entité métier : Le service prescripteur du présent marché est la Direction Exécutive Financière (DEF).
- Le Département Trésorerie et Marchés de Capitaux (DEF/TMC) est le sponsor de l'outil.
- La direction est appuyée par la division Administration et Projet Finance qui joue le rôle de maîtrise d'ouvrage.

2. Présentation du Service Métier - Utilisateur

La Direction exécutive financière (DEF) a pour mission :

- De définir et formaliser les normes, principes et indicateurs applicables au groupe en matière financière (normes de contrôle de gestion, de gestion actif-passif, comptables, etc.),
- De produire l'information financière, comptable, fiscale et réglementaire du groupe et en assurer la fiabilité et la complétude,
- D'analyser la performance des métiers, alimenter la réflexion stratégique et produire les informations et les analyses utiles à la prise de décisions au niveau groupe et au sein des métiers,
- D'être garante de la solidité et la sécurité financière en proposant une politique financière groupe puis en la pilotant et en l'exécutant sur les marchés,
- De définir, modéliser et piloter la politique de gestion de bilan du groupe AFD,
- Gérer la communication externe en matière financière,
- D'assurer la relation du groupe avec ses différents investisseurs et autorités de contrôles en matière réglementaire,
- De définir l'architecture et développer la performance et la pertinence du système d'information de la fonction Finance,
- D'accompagner les opérationnels sur tous les aspects financiers de l'instruction à la contractualisation et de sécuriser la gestion des concours financiers de l'AFD et délégués.

DEF est organisée en quatre départements et une division attachée à la direction comme suit :



3. Objet du marché

Le présent CCTP définit les besoins de l'AFD pour la fourniture de prestataire et la mise à disposition d'un service bureau de paiement permettant l'intégration, le traitement et la supervision des flux financiers via le réseau SWIFTNET.

La solution attendue devra couvrir les volets suivants :

3.1. Interfaces logicielles et services associés

- Mise à disposition de licences pour des interfaces logicielles permettant la connexion au réseau SWIFTNET.
- Les interfaces devront prendre en charge les services suivants :
 - FIN, FINplus, MX, FileAct, SWIFTNet Browse / WebAccess, SWIFTNet Instant.
- La solution devra assurer l'interopérabilité avec les outils de communication bancaire existants ou futurs.

3.2. Assistance et support fonctionnel

Le prestataire devra fournir un support opérationnel et fonctionnel couvrant notamment :

- la traçabilité et le suivi des paiements,
- la création, modification ou suppression de contreparties bancaires,
- l'activation et la désactivation de canaux,
- l'ajout ou la suppression de services.

3.3. Sécurité et conformité

La solution devra respecter :

- les exigences réglementaires et de sécurité de l'AFD,
- les recommandations et normes SWIFT,
- les règles de sécurité de l'État pour les systèmes d'information sensibles (Instruction 901 / PSSIE).

3.4. Audit et traçabilité

Le prestataire devra permettre :

- la production de rapports d'activité,
- l'audit des opérations et des accès,
- la conservation des journaux conformément aux obligations légales et réglementaires.
- L'audit sécurité

3.5. Contraintes et exigences macroscopiques

- Calendrier de déploiement : mise en œuvre complète, incluant l'intégration, avant le 30 juin 2026.

- Adaptabilité : la solution devra pouvoir s'interfacer avec un large éventail d'outils de communication bancaire.
- Lieu d'hébergement des serveurs : en France, conformément aux exigences réglementaires et de sécurité de l'AFD.

4. Présentation du Besoin

4.1. Contexte du besoin

Dans le cadre de l'évolution de son dispositif de gestion des flux financiers et de messagerie bancaire, l'AFD met en concurrence une solution de service bureau SWIFT permettant l'intégration, le traitement et la supervision des paiements, messages et relevés bancaires. La solution attendue devra permettre à l'AFD de faire transiter, via des canaux sécurisés tels que FIN et FileAct, l'ensemble des flux nécessaires à ses opérations courantes, en s'appuyant sur les standards de messagerie bancaire en vigueur.

À ce titre, l'AFD souhaite disposer d'un service bureau capable de prendre en charge différents types de messages et fonctionnalités, notamment :

- les messages de paiement au format ISO 20022 (pain.001.001.02 / 03 / 09),
- les messages de reporting et de relevés (MT950, CAMT.053),
- les services associés à SWIFT GPI.

La solution proposée devra s'inscrire dans un cadre pérenne, sécurisé et conforme aux normes SWIFT, et être en mesure d'accompagner les évolutions futures des formats, des volumes et des besoins fonctionnels de l'AFD.

4.2. Enjeu du besoin

L'AFD recherche un partenaire capable de fournir un service bureau fiable et évolutif, garantissant la continuité de service, la sécurité des échanges et un haut niveau de qualité opérationnelle tout en assurant une disponibilité, traçabilité et confidentialité des données transitant.

5. Description des exigences fonctionnelles

5.1. Exigences fonctionnelles

5.1.1. Les messages

Le service bureau doit permettre l'émission, la réception et le traitement des types de messages suivants :

- Messages de reporting et de relevés
 - CAMT.053
 - MT940
 - MT950
 - BANSTA
 - AFB120
 - CAMT.052
 - CAMT.054
 - CAMT.056

- CAMT.029
 - pacs.002 (statut) et pacs.008 (paiement interbancaire direct)
- Messages de paiement
 - pain.001.001.03
 - pain.001.001.09
- Messages et services SWIFT
 - SWIFT GPI

Le service bureau devra supporter l'ensemble des messages SWIFT MT et ISO 20022 nécessaires aux opérations de trésorerie, de paiement, de reporting, d'investigation et de conformité, y compris les messages de statut, d'annulation et de suivi, même s'ils ne sont pas explicitement listés.

Le prestataire devra donc présenter l'ensemble des messages disponibles à date et un planning des futurs messages qui seront intégrés.

5.1.2. Gestion des contreparties

Le service bureau doit permettre la gestion d'un nombre illimité de contreparties, sans restriction technique ou contractuelle.

5.1.3. Relationship Management Application (RMA)

Le service bureau doit intégrer une fonctionnalité de gestion des autorisations RMA, permettant :

- la création,
- la modification,
- la suppression,
- et le suivi des relations RMA avec les contreparties.

5.1.4. 4. Canaux de communication SWIFT

Le service bureau doit proposer les canaux de communication suivants :

- FIN
- FileAct

Ces canaux doivent être disponibles pour l'ensemble des messages pris en charge.

5.1.5. Disponibilité du service

Le service bureau doit assurer une disponibilité opérationnelle :

- 7 jours sur 7
- 24 heures sur 24

Les modalités de maintenance planifiée devront être précisées.

5.1.6. Conformité et mises à jour SWIFT

Le service bureau doit être conforme aux normes SWIFT en vigueur, et assurer le suivi des montées de version :

- des standards de messagerie SWIFT,
- des bibliothèques de formats de messages,
- des exigences réglementaires associées.

5.1.7. Traçabilité et supervision

Le service bureau doit assurer une traçabilité complète des échanges, incluant :

- le suivi du cycle de vie des messages,
- la gestion des statuts (émis, reçus, rejetés, en erreur),
- l'historisation et l'archivage des messages,
- la mise à disposition de journaux consultables.

Le prestataire devra présenter les certifications dont ils disposent (ex : ISO 27001)

5.1.8. Sécurité et conformité

Le service bureau doit garantir :

- la sécurité des échanges,
- l'authentification des accès,
- la gestion des droits utilisateurs,
- la conformité au SWIFT Customer Security Programme (CSP).

6. Description des exigences sécurité

6.1. Exigences de sécurité

6.1.1. Sécurité et conformité

Le service bureau doit garantir un niveau de sécurité conforme aux exigences bancaires et aux standards SWIFT, couvrant l'ensemble des flux, des accès et des données échangées.

6.1.2. Sécurisation des flux

Le service bureau doit assurer la sécurisation complète des flux de messagerie, notamment par :

- le chiffrement des données en transit,
- l'utilisation de certificats de sécurité conformes aux standards SWIFT,
- la protection contre toute interception, altération ou accès non autorisé.

L'ensemble des échanges via les canaux FIN et FileAct doit être réalisé sur des flux sécurisés de bout en bout.

6.1.3. Authentification et gestion des accès

Le service bureau doit mettre en œuvre une gestion des accès robuste, incluant :

- l'authentification forte des utilisateurs et des systèmes,
- la gestion des rôles et habilitations,
- la séparation des droits (administration, exploitation, consultation),
- la gestion des certificats et des clés de sécurité.

Les accès doivent être strictement limités aux utilisateurs autorisés, selon le principe du moindre privilège.

6.1.4. Conformité SWIFT et gouvernance de la sécurité

Le service bureau doit être conforme au SWIFT Customer Security Programme (CSP) et s'inscrire dans une démarche de gouvernance de la sécurité, incluant notamment :

- des politiques et procédures de sécurité formalisées,
- une organisation claire des responsabilités en matière de sécurité,
- la gestion des risques et des incidents de sécurité,
- la prise en compte des évolutions des exigences SWIFT et réglementaires.

6.1.5. Journalisation et traçabilité

Le service bureau doit assurer la journalisation complète :

- des accès utilisateurs,
- des actions réalisées sur la plateforme,
- des échanges de messages.

Les journaux doivent être :

- horodatés,
- protégés contre toute modification,
- conservés selon une durée définie,
- consultables à des fins d'audit, de contrôle ou d'investigation.

6.1.6. Environnements et garantie PUPA

Le service bureau doit garantir la séparation et la sécurisation des environnements, incluant a minima :

- un environnement de production,
- un environnement de recette / UAT,
- un dispositif de continuité ou de reprise d'activité (PRA/PCA).

En cas de test sur le PRA/PCA le prestataire devra envoyer le rapport découlant des tests.

Cette organisation doit permettre d'assurer la continuité du service, la protection des données et la reprise des activités en cas d'incident majeur.

6.1.7. Continuité et récupération des données

Le service bureau doit mettre en place des mécanismes de sauvegarde et de récupération des données, permettant :

- la restauration des messages et journaux,
- la reprise du service après incident,
- la limitation des pertes de données.
- RPO et RTO exigé inférieur à 4heures es modalités de sauvegarde et de restauration (fréquence, périmètre, délais) devront être documentées.

6.1.8. Sous-traitance

Les sous-traitants sont soumis aux mêmes exigences de sécurité que le titulaire.
Le titulaire demeure pleinement responsable des actes et manquements de ses sous-traitants

6.2. Exigences sur les compétences attendues

6.2.1. Exigences de compétences du prestataire

Le prestataire doit disposer des compétences humaines, fonctionnelles et techniques nécessaires à la mise en œuvre, à l'exploitation et au support du service bureau, afin de garantir la continuité, la qualité et la sécurité des services fournis.

6.2.2. Compétences fonctionnelles et techniques

Le prestataire doit démontrer une expertise avérée sur :

- les fonctionnalités du service bureau proposé,
- les standards de messagerie bancaire (SWIFT MT, ISO 20022),
- les canaux FIN et FileAct,
- les processus de traitement, de contrôle et de supervision des flux financiers.

Il doit être en mesure de :

- analyser et corriger les anomalies fonctionnelles et techniques courantes (interfaces, fichiers, contrôles, calculs, rejets),
- identifier rapidement les causes d'incident,
- proposer des solutions pérennes et documentées.

6.2.3. Expertise métier

Le prestataire doit disposer d'une connaissance suffisante des métiers financiers, notamment :

- des opérations financières et de trésorerie,
- des produits de couverture et de gestion du risque,
- des mécanismes de règlement/livraison,
- des processus comptables associés.

Cette expertise doit permettre une compréhension rapide des impacts métier en cas d'incident ou d'anomalie.

6.2.4. Dispositif de support et d'assistance

Le dispositif de support doit s'appuyer sur des équipes qualifiées, capables de :

- fournir des réponses fiables et exploitables dans des délais adaptés,
- intervenir sur des incidents de différents niveaux de complexité,
- collaborer efficacement avec les équipes métiers et les équipes techniques du client (DSI, production, architecture, support).

Les niveaux de support, les délais de prise en charge et les modalités d'escalade devront être définis tels que présentés en paragraphe 8.1.2.

6.2.5. Compétences transverses et comportementales

Les équipes du prestataire doivent présenter les qualités suivantes :

- capacité d'analyse et de synthèse,
- rigueur et méthode dans le traitement des demandes et incidents,
- qualité de la communication écrite et orale,
- capacité à interagir avec des interlocuteurs de niveaux hiérarchiques et de profils variés,
- efficacité dans la collaboration avec l'ensemble des parties prenantes.

6.2.6. Continuité des compétences

Le prestataire doit garantir la continuité des compétences sur la durée du contrat, notamment par :

- la limitation du turn-over sur les rôles clés,
- la transmission et la capitalisation des connaissances,
- la formation continue de ses équipes.

6.3. Exigences sur la protection des données personnelles

Le prestataire doit justifier d'une gouvernance en matière de protection des données personnelles lui permettant de respecter les obligations et instructions en la matière telles que décrites à l'Annexe 2 du CCAP.

Le prestataire décrira ladite gouvernance en incluant dans son mémoire technique ses réponses au questionnaire RGPD et en fournissant toute documentation utile en appui des réponses apportées. Le prestataire devra a minima justifier, au plus tard avant l'attribution du marché :

- De la désignation d'un DPO ou des motifs pour lesquels il a jugé que l'obligation d'une telle désignation ne lui était pas applicable
- De la tenue d'un registre des activités de traitement
- D'une politique en matière de protection des données ou toute documentation équivalente en la matière

La solution logicielle doit intégrer des fonctionnalités permettant la gestion du cycle de vie des données personnelles de manière automatisée et conforme aux pratiques de place ainsi que des obligations légales et réglementaires.

7. Type de prestation et forme de prix

7.1. Type de prestation

Le prestataire devra proposer une offre de services complète, couvrant l'ensemble des prestations nécessaires à la mise en œuvre, à l'exploitation et au support du service bureau. Ces prestations incluent notamment :

- la mise en place et le paramétrage du service,
- l'intégration avec le système d'information du client,
- l'exploitation courante du service bureau,
- la maintenance corrective et évolutive,
- le support fonctionnel et technique,
- l'accompagnement lors des montées de version et évolutions réglementaires.

La prestation pourra être proposée sous la forme d'un service récurrent, assorti, le cas échéant, de prestations ponctuelles complémentaires.

7.2. Forme de prix

La tarification devra être clairement définie et détaillée, et comprendra :

- Au forfait : intégration et mise en œuvre de l'outil,
- Sur prix unitaire : une redevance récurrente mensuelle pour l'exploitation du service et les maintenances sur la base d'un système de tranche avec pour sous-jacent le nombre de messages transitant mensuellement via le service bureau :

Tranche	Nombre de message/fichier
1	0 à 500
2	501 à 1000
3	1001 à 2000
4	2001 à 3000
5	3001 à 4000
6	4001 à 5000
7	5001 à 6000
8	6001 à 7000
9	7001 à 8000
10	...

Les prix devront être exprimés de manière transparente, en précisant :

- sur la base de la volumétrie (nombre de messages, contreparties, flux),
- les éventuelles options ou services additionnels,
- sans conditions de révision des prix

A titre d'information l'AFD envoie/reçoit mensuellement près de 6500 messages avec un ratio de 1/6 (message envoyé versus reçu).

8. Intégration de l'outil et mise en œuvre dans le système AFD

8.1. Principes généraux

Le titulaire devra assurer une prestation d'intégration clé en main de la solution de service bureau objet du présent marché.

Cette prestation comprend l'ensemble des activités nécessaires à la mise en service opérationnelle de la solution, depuis le lancement du projet jusqu'à la mise en production. Le titulaire s'engage à mettre en œuvre les moyens humains, techniques et organisationnels nécessaires à la réussite de l'intégration dans les délais impartis.

8.2. Planning et délais

L'AFD souhaiterait que la phase d'intégration soit réalisée sur une durée maximale d'un mois et demi, incluant l'ensemble des paramétrages, tests, recettes et actions préparatoires à la mise en production.

La mise en production devra, dans la mesure du possible, intervenir avant la fin du mois de juin 2026, sous réserve de la validation de la recette par l'AFD.

Un planning détaillé des différentes étapes d'intégration devra être fourni par le titulaire lors de la remise des offres et devra être validé par l'AFD.

8.3. Environnements

Le titulaire devra mettre à disposition de l'AFD, a minima, les environnements suivants :

- Un environnement de test, dédié aux phases d'intégration, de paramétrage, de tests fonctionnels et de recette ;
- Un environnement de production, destiné à l'exploitation courante du service.

Ces environnements devront être strictement séparés, sécurisés et conformes aux exigences de sécurité de l'AFD.

L'environnement de test devra être représentatif de l'environnement de production afin de garantir la fiabilité des tests et des validations.

8.4. Phase de tests et de recette

8.4.1. Tests d'intégration

Le titulaire devra accompagner l'AFD dans la réalisation des tests d'intégration portant notamment sur :

- la connectivité aux réseaux et canaux de communication bancaire ;
- l'émission, la réception et le traitement des messages ;
- la gestion des flux de paiement, de reporting et de suivi ;
- la traçabilité des opérations ;
- le respect des exigences de sécurité et de conformité.

8.4.2. Recette fonctionnelle

La recette sera réalisée sur la base de scénarios de tests définis par l'AFD.

Elle portera notamment sur :

- un panel de 10 banques partenaires ;
- environ une centaine d'opérations de test, couvrant les principaux cas d'usage ;
- la validation des flux de bout en bout (avec validation de réception de la banque partenaire et renvoi d'un relevé justifiant le paiement)

À l'issue de cette phase, une recette formelle sera prononcée par l'AFD, matérialisée par un procès-verbal de recette.

8.4.3. Tests en production (penny tests)

Après validation de la recette fonctionnelle, le titulaire devra accompagner l'AFD dans la réalisation de tests en production de type "penny tests" avec les banques partenaires, afin de confirmer le bon fonctionnement opérationnel de la solution en conditions réelles. La mise en production définitive sera conditionnée au succès de ces tests.

8.4.4. Accompagnement et responsabilités

Le titulaire devra assurer un accompagnement actif de l'AFD tout au long de la phase d'intégration, incluant :

- assistance aux paramétrages ;
- support lors des tests et de la recette ;
- correction des anomalies bloquantes ou majeures identifiées.

L'AFD restera responsable de la validation des livrables, des résultats de tests et de la décision de mise en production.

8.4.5. Livrables attendus

Les livrables attendus dans le cadre de la phase d'intégration incluent notamment :

- un planning détaillé d'intégration ;
- la documentation de configuration et de paramétrage (dont la procédure pour l'intégration de nouveaux services ou de nouvelles banques) ;
- les comptes rendus de tests ;
- le procès-verbal de recette signé ;
- les éléments nécessaires au passage en exploitation.

8.4.6. Vérification de Service Régulier (VSR)

À l'issue de la mise en production de la solution, une phase de Vérification de Service Régulier (VSR) sera mise en œuvre pour une durée de 1 mois.

Cette phase a pour objectif de confirmer le bon fonctionnement de la solution en conditions réelles d'exploitation, sur la base des usages courants de l'AFD, et de vérifier la stabilité, la performance et la conformité du service rendu.

Durant la période de VSR, le titulaire devra :

- assurer un suivi renforcé de l'exploitation ;
- analyser les incidents, dysfonctionnements ou écarts constatés ;
- corriger, dans les meilleurs délais, toute anomalie imputable à la solution ou à son intégration ;
- accompagner l'AFD dans l'utilisation opérationnelle du service.

La VSR portera notamment sur :

- la disponibilité et la continuité du service ;
- le bon acheminement et le traitement des flux ;

- la traçabilité des opérations ;
 - le respect des exigences de sécurité et des niveaux de service attendus.
- À l'issue de la période de VSR, un procès-verbal de VSR sera établi. La validation de la VSR par l'AFD conditionnera le passage définitif en régime nominal de maintenance et de support.

9. Prestations de maintenance et support

Le prestataire doit assurer la maintenance du service bureau pendant toute la durée du contrat, afin de garantir la continuité, la fiabilité et la conformité du service.

La maintenance devra couvrir a minima :

- la maintenance corrective, incluant la correction des anomalies, dysfonctionnements et incidents affectant le service (incluant les anomalies de sécurité et vulnérabilité) ;
- les mises à jour liées aux évolutions des standards de messagerie bancaire (notamment SWIFT et ISO 20022), aux exigences réglementaires et aux évolutions techniques de la solution ;
- la maintenance préventive, visant à anticiper les incidents et à maintenir un niveau de performance et de sécurité conforme aux exigences.

Les opérations de maintenance devront être réalisées dans le respect des contraintes de disponibilité du service, et faire l'objet d'une communication préalable auprès de l'AFD en cas d'impact potentiel.

9.1. Répartition des responsabilités entre le prestataire et l'AFD en phase de maintenance

9.1.1. Prise en charge de la TMA par l'intégrateur

La répartition des responsabilités entre le prestataire et l'AFD en phase de maintenance doit être clairement définie et formalisée, afin d'assurer une gestion efficace des incidents, des évolutions et des opérations de maintenance.

Toute responsabilité non explicitement attribuée au client est réputée relever du prestataire.

9.1.2. Responsabilités du prestataire

Le prestataire est responsable notamment :

- de la maintenance corrective, préventive et évolutive de la solution de service bureau ;
- de la correction des anomalies imputables à la solution ou à son exploitation ;
- de la mise à disposition des mises à jour, correctifs et montées de version nécessaires, notamment celles liées aux évolutions des standards SWIFT et réglementaires ;
- de l'information préalable de l'AFD en cas d'opérations de maintenance susceptibles d'impacter le service ;
- de la fourniture du support technique et fonctionnel associé à la maintenance.

9.1.3. Responsabilités de l'AFD

L'AFD est responsable notamment :

- de la mise à disposition des informations nécessaires à l'analyse et au traitement des incidents ;
- de la validation des évolutions et mises à jour dans les environnements de recette ou de test, lorsque cela est requis ;
- de la gestion de ses propres systèmes, interfaces et données en amont et en aval du service bureau ;
- du respect des prérequis techniques et organisationnels définis par le prestataire.

9.1.4. Principes de collaboration

Les parties s'engagent à :

- coopérer de manière active et transparente en phase de maintenance ;
- respecter les processus de déclaration, de qualification et de traitement des incidents ;
- désigner des interlocuteurs référents pour le suivi des opérations de maintenance.

9.1.5. Niveau de service

1. Périmètre du SLA

Les présents accords de niveau de service (SLA) s'appliquent aux prestations d'exploitation, de support et de maintenance du service bureau SWIFT, incluant les canaux FIN et FileAct, ainsi que l'ensemble des flux de messagerie pris en charge.

Les SLA sont applicables pendant les heures de service :

- 7 jours sur 7
- 24 heures sur 24

2. Engagement de disponibilité

Le prestataire s'engage à assurer une disponibilité minimale du service de :

- 99,9 % sur la plage de service

La disponibilité est mesurée hors périodes de maintenance planifiée notifiées à l'avance.

3. Gestion des incidents

3.1 Classification des incidents

Niveau	Description	Exemple
Critique (P1)	Service indisponible ou flux bloqués	Impossibilité d'émettre ou recevoir des messages
Majeur (P2)	Dégradation significative du service	Retards importants, rejets multiples
Mineur (P3)	Anomalie sans impact bloquant	Anomalie d'affichage, retard ponctuel

3.2 Délais de prise en charge et de résolution

Niveau	Prise en charge	Délai de résolution cible
P1 – Critique	≤ 1 heure	≤ 4 heures
P2 – Majeur	≤ 2 heures	≤ 1 jour ouvré
P3 – Mineur	≤ 1 jour ouvré	Planifié / prochain correctif

3.3 Pénalités en cas de non-respect des engagements de disponibilité sur la base des anomalies P1/P2

Disponibilité réelle de la solution sur le mois calendaire concerné	Pourcentage de réduction de la redevance mensuelle due à l'AFD pour le mois calendaire suivant
Inférieure à 99,9 % et supérieure ou égale à 99,5 %	5%
Inférieure à 99,5 % et supérieure ou égale à 95,0 %	10%
Inférieure à 95,0 %	20%

Formule de calcul du taux d'indisponibilité= nombre d'heures sans résolution de l'anomalie/720h (nombre heures dans le mois)

4. Support et communication

Le prestataire doit :

- accuser réception de toute demande de support,
- fournir des points d'avancement réguliers pour les incidents P1 et P2,
- informer l'AFD de la résolution et des actions correctives mises en œuvre.

5. Maintenance

5.1 Maintenance planifiée

- Les opérations de maintenance planifiée doivent être notifiées au minimum 10 jours ouvrés à l'avance en cas de coupure de service et 5 jours sans coupure de service.
- Elles doivent être réalisées en dehors de la plage horaire suivante : 8h-19h du lundi au vendredi, sauf urgence ou accord explicite de l'AFD.

5.2 Maintenance corrective

- Les corrections liées aux incidents P1 et P2 sont incluses dans le périmètre du SLA.
- Les correctifs doivent être déployés dans des délais compatibles avec les engagements de résolution

6. Indicateurs de performance (KPI)

Les indicateurs suivants devront être suivis et partagés via des reporting trimestriels :

- taux de disponibilité du service,
- nombre d'incidents par niveau,
- respect des délais de prise en charge et de résolution,
- temps moyen de résolution.

10. Règle de sécurité

Rappel du contexte d'application des règles de Sécurité, en lien avec les annexes Sécurité

L'AFD est un établissement public industriel et commercial et une société de financement. A ce titre, l'AFD est notamment soumise à la réglementation bancaire et aux règles édictées par l'Etat en matière de SSI.

En raison des liens de l'AFD avec deux ministères régaliens, son système d'information est homologué au niveau « DIFFUSION RESTREINTE », conformément aux exigences de l'Instruction Générale Interministérielle relative à la Protection des Systèmes d'information Sensibles n°901/SGDSN/ANSSI « Instruction 901 » et de la Politique de Sécurité des Systèmes d'Information de l'Etat « PSSIE ».

Dans son article 16 relatif à l'externalisation, l'Instruction 901 prévoit qu'en cas d'externalisation d'une prestation qui met en œuvre un système d'information « Diffusion Restreinte », l'entité et son prestataire tiennent compte des recommandations figurant dans le guide de l'ANSSI relatif à l'externalisation.

Ce Guide de l'ANSSI, « Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information », prévoit à son article 2.1.1 : « Il convient de s'assurer que l'ensemble des lieux d'hébergement (site principal, site(s) de secours, de sauvegarde, etc.) répondent d'une part aux exigences de sécurité du donneur d'ordres, et d'autre part aux obligations légales et réglementaires, notamment en ce qui concerne la protection des données à caractère personnel.

Il en va de même des sites de télémaintenance s'ils peuvent accéder aux données.

Par ailleurs, l'article 5.6 de cette même ordonnance prévoit que les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité du donneur d'ordres et aux dispositions de la loi du 6 janvier 1978 modifiée, relative à la protection des données personnelles. Le prestataire doit communiquer la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence peut s'avérer délicate dans le cadre d'architectures distribuées, il peut être demandé au prestataire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident. Ces obligations doivent également être respectée en cas de recours au « télétravail ».

Le prestataire s'engage à respecter toutes les règles et consignes de sécurité, écrites ou orales, que lui communiquera l'AFD pour l'exercice du service rendu. Il en assurera, si nécessaire, la transmission à ses employés intervenant sur la prestation et s'assurera de leur engagement à respecter les exigences de sécurité de l'AFD comme si c'étaient celles de leur employeur.

Le titulaire prendra toutes les dispositions nécessaires pour la sécurité et la confidentialité des données, des logiciels et des documents. Le titulaire appliquera l'ensemble des exigences exposées dans l'« Annexe - Sécurité » du CCAP ainsi que l'ensemble des règles et consignes de sécurités AFD.

Dans le **cadre de réponse**, le soumissionnaire présentera sa politique en termes de gestion de la sécurité et de la confidentialité selon les formats prévus à cet effet (Annexe - Plan d'Assurance Sécurité »).

11. Réversibilité du service

Le prestataire doit garantir la réversibilité du service bureau en fin de contrat, ou en cas de rupture de contrat, afin de permettre à l'AFD de reprendre ou de transférer le service vers un autre prestataire dans des conditions maîtrisées.

À ce titre, le prestataire s'engage à :

- restituer l'ensemble des données, messages, historiques et journaux liés au service, dans des formats standards et exploitables dans un délai de 2 mois à partir de la notification du changement de prestataire ;
- fournir l'assistance nécessaire à la reprise du service par l'AFD ou par un prestataire tiers ;
- assurer la continuité du service pendant la phase de transition
- supprimer ou anonymiser les données de l'AFD à l'issue de la réversibilité, conformément aux exigences réglementaires.

Les modalités opérationnelles et financières de la réversibilité devront être précisées contractuellement.