Direction des systèmes d'information

TMA-DMF

Cahier des Clauses Techniques Particulières (CCTP)

Livret 1/2 du CCTP n°25362

Accord cadre n°25.14.030

Procédure sur marché ouvert
Accord-cadre passé en application des articles L2124-3, R2124-3 et R2124-4, et R2161-1 à R2161-14du Code de la commande publique auquel il sera fait référence sous le vocable « le Code » dans la suite du présent document

Objet : Ce document décrit les exigences fonctionnelles, techniques, d'intégration dans le SI, de sécurité et d'organisation des prestations pour la TMA DMF.

SOMMAIRE

1 CONTEXTE GÉNÉRAL 5
1.1 Objet de l'accord-cadre 5
1.2 Présentation synthétique du CNRS 5
1.3 Echéancier prévisionnel du projet 5
1.4 Lieu d'exécution de l'accord-cadre 5
1.5 Structure du CCTP et conventions de rédaction 5
2 CONTEXTE DU SI AU CNRS 7
2.1 Conformités règlementaires 7
2.1.1 Politique Générale de Sécurité des systèmes d'Information 7
2.1.2 Protection des données à caractère personnel (DCP) 8
2.1.3 Interopérabilité 9
2.1.4 Accessibilité numérique 9
2.2 Présentation des infrastructures du SI CNRS 10
2.2.1 Sites et utilisateurs du système d'information 10
2.2.2 Centres serveurs 11
2.2.3 Réseau 11
2.2.4 Infrastructures 11
2.3 Principes d'urbanisation et d'intégration dans le SI 12
2.3.1 Principes généraux 12
2.3.2 Principes d'échanges 12
2.3.3 Plateformes transverses et services proposés 13
2.3.4 Prise en compte des changements de l'organisation structurelle du CNRS 14
3 DESCRIPTION DE LA SOLUTION 15
3.1 Présentation de la solution 15
3.1.1 Présentation fonctionnelle 15
3.1.2 Intégration dans le SI 17
3.1.3 Présentation technique 19
3.1.4 Archivage 19
3.1.5 Serveurs développement 20
3.1.6 Environnements CNRS 20
3.1.7 Particularités de l'environnement SAP 21
3.2 Volumétrie 22
3.2.1 Volumétrie des anomalies 22
3.2.2 Volumétrie des évolutions 22
3.3 Evolutions potentielles à court ou moyen terme 22
4 CADRE DE COHÉRENCE TECHNIQUE DE LA SOLUTION 24
4.1 Exigences d'intégration dans le SI 24
4.1.1 Répartition fonctionnelle 24
4.1.2 Echanges de données 24
4.1.3 Authentification, comptes utilisateurs 27
4.1.4 Stockage des documents 30
4.2 Exigences techniques 30
4.2.1 Eléments techniques structurants 30
4.2.2 Services d'infrastructure 30
4.2.3 Architecture applicative 33
4.2.4 Base de données 40
4.2.5 Engagements de qualité de service pour l'application 40
4.3 Exigences d'ergonomie-graphisme 41
4.3.1 Charte graphique 42

4.3.2 Règles d'ergonomie 42
4.4 Exigences de sécurité 42
4.4.1 Auditabilité 43
4.4.2 Protection des applications web 43
5 CADRE D'ORGANISATION DES PRESTATIONS 45
5.1 Système qualité 45
5.2 Organisation des équipes projet 46
5.2.1 Organisation de l'équipe projet CNRS 46
5.2.2 Organisation et gestion des compétences de l'équipe projet du titulaire 46
5.3 Dispositifs de conduite de projet 47
5.3.1 Structures de pilotage projet 47
5.3.2 Pratiques de gestion de projet 48
5.3.3 Indicateurs de pilotage et qualité du projet 48
5.4 Méthode de développement 49
5.4.1 Cycle de vie 49
5.4.2 Activités de réalisation (à la charge du Titulaire) 50
5.4.3 Activités de recette (à la charge du CNRS) 51
5.5 Gestion des environnements 51
5.5.1 Postes de travail du titulaire 51
5.5.2 Environnement de développement 51
5.5.3 Environnements CNRS 52
5.6 Gestion des livraisons 52
5.7 Gestion de la documentation 53
5.8 Capitalisation des connaissances 54
5.9 Outillage de suivi et pilotage du projet 55
5.10 Mesures et clauses de sécurité 56
5.10.1 Gestion de la Sécurité par le titulaire 56
5.10.2 Protection des biens 56
5.10.3 Obligations du titulaire 58
5.10.4 Localisation des données 59
5.10.5 Audit 60
5.10.6 Application des plans gouvernementaux 61
6 ANNEXES 62
6.1 Documents joints 62
6.2 Présentation détaillée du CNRS 62
6.2.1 La présidence-direction générale 62
6.2.2 La direction générale déléguée à la science (DGD-S) 62
6.2.3 La direction générale déléguée aux ressources (DGD-R) 63
6.2.4 La direction générale déléguée à l'innovation (DGD-I) 65
6.2.5 Les délégations régionales (DR) 65
6.2.6 Les unités (laboratoires) 66
6.3 Référence des exigences 66
6.4 Abréviations et Glossaire 67
6.4.1 Abréviations 67
6.4.2 Glossaire 69

TABLE DES ILLUSTRATIONS

Figure 1 : Réseau RENATER 11
Figure 2 : Présentation de la solution DMF 16

Figure 3 : Flux de la solution DMF 17
Figure 4 : Architecture technique de la solution DMF 19
Figure 5 : Environnements non productifs de la solution DMF 20
Figure 6 : Environnements productifs de la solution DMF 21
Figure 7 : Présentation de la forge logicielle 37
Figure 8 : Organisation du projet au CNRS 46
Figure 9 : Cycle de vie en cascade itératif et incrémental 49
Figure 10 : Le CNRS en région 66

1 CONTEXTE GÉNÉRAL

1.1 OBJET DE L'ACCORD-CADRE

Le présent accord-cadre a pour objet la fourniture de prestations de maintenance et d'évolutions du système d'information DMF (Dématérialisation des Factures), y compris les prestations annexes rendues nécessaires par les évolutions du système (formations, conduite du changement, expertises, …).

1.2 PRÉSENTATION SYNTHÉTIQUE DU CNRS

Le Centre national de la recherche scientifique est un organisme public de recherche (Établissement public à caractère scientifique et technologique) pluridisciplinaire placé sous la tutelle du Ministère de l'Enseignement supérieur et de la Recherche (MESR). Sa mission est de faire progresser la connaissance et être utile à la société.

Avec près de 33 000 personnes, un budget de presque 4 milliards d'euros, plus de 1100 laboratoires répartis en France et à l'étranger, le CNRS exerce son activité dans tous les champs de la connaissance qu'il s'agisse de biologie, chimie, écologie et environnement, homme et société, ingénierie et systèmes, mathématiques, nucléaire et particules, physique, sciences de l'information ou terre et univers.

Ces domaines de recherche sont regroupés au sein de dix instituts (cf. § 6.2.2.1).

Sa gouvernance est assurée par le président-directeur général du CNRS, assisté de la directrice de cabinet et de trois directeurs généraux délégués à la science, aux ressources et à l'innovation.

Des informations plus complètes sont disponibles en annexe (cf. § 6.2) et sur le site Web, à l'adresse suivante : https://www.cnrs.fr/fr/le-cnrs/organisation.

1.3 ECHÉANCIER PRÉVISIONNEL DU PROJET

Le projet démarre dès la notification de l'accord-cadre.

1.4 LIEU D'EXÉCUTION DE L'ACCORD-CADRE

La réalisation et maintenance de l'application s'effectue dans les locaux du titulaire.

Les comités, réunions ou ateliers de spécifications et de conception, nécessitant la présence du CNRS, se tiennent sur sites CNRS à Toulouse, Paris et Nancy, la visioconférence entre ces sites est à privilégier.

Les modalités pratiques sont définies au démarrage de l'accord-cadre.

Les locaux du CNRS se situent :

à Paris (Siège du CNRS) :

CNRS
3 rue Michel-Ange
75794 PARIS CEDEX 16

à Nancy (SCD) :

CNRS – SCD
2 rue Jean Zay
54519 VANDOEUVRE-LES-NANCY

à Toulouse (DSI) :

CNRS - DSI
358 rue Pierre Gilles de Gennes
31670 LABEGE

1.5 STRUCTURE DU CCTP ET CONVENTIONS DE RÉDACTION

Le livret 1 du CCTP est composé essentiellement des chapitres suivants :

- contexte du SI au CNRS : contexte dans lequel s'inscrit la réalisation et la maintenance de la solution, en terme de conformité règlementaire, d'infrastructure, d'urbanisation et d'intégration dans le système d'information existant,

- description de la solution : caractéristiques fonctionnelles, techniques et volumétrie de la solution existante à maintenir,
- cadre de cohérence technique de la solution : exigences applicables à la solution initiale et à toute évolution lors de la maintenance de la solution,
- cadre d'organisation des prestations : exigences applicables aux processus de conduite de projet, développement et maintenance de la solution, ainsi que mesures de sécurité encadrant les prestations.

Le livret 2 du CCTP contient la description des prestations et unités d'œuvre, objets de la commande.

Les exigences vis-à-vis du titulaire sont décrites dans le présent document dans des tableaux de la forme ci-dessous. La référence est composée de 3 ou 4 lettres définissant le groupe d'exigences (cf. « Référence des exigences » en annexe) et de 3 chiffres (pas nécessairement consécutifs). Les exigences sont classées selon 3 niveaux :

- Priorité 0 : exigence impérative à satisfaire obligatoirement par le titulaire
- Priorité 1 : exigence très fortement souhaitée, à justifier si non satisfaite
- Priorité 2 : exigence souhaitée, pouvant être satisfaite, partiellement ou pas par le titulaire (avec justification)

Référence	Libellé exigence	Priorité
XXX_NNN	Libellé de l'exigence	0/1/2

La solution en place actuellement n'est pas intégralement conforme à toutes les exigences présentées dans ce document. Les mises en conformité nécessaires sont déclenchées à l'initiative du CNRS lorsqu'elles sont nécessaires, sous la forme de demandes d'évolutions. Les nouveaux développements réalisés dans le cadre de ce marché doivent être conformes aux exigences sauf dérogation expresse du CNRS.

2 CONTEXTE DU SI AU CNRS

2.1 CONFORMITÉS RÈGLEMENTAIRES

Les applications mises en œuvre par le CNRS sont soumises à des conformités règlementaires définies dans des référentiels interministériels présentés dans les paragraphes suivants.

Référence	Libellé exigence	Priorité
REGL_001-a	Les téléservices (applications destinées à la communication inter administration ou destinées à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public) sont mis en œuvre conformément aux référentiels interministériels. Les téléservices sont conformes au RGS (sécurité) : https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs	0
REGL_001-b	Les téléservices (applications destinées à la communication inter administration ou destinées à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public) sont mis en œuvre conformément aux référentiels interministériels. Les téléservices sont conformes au RGI (interopérabilité, selon le profil choisi par le CNRS) : https://www.numerique.gouv.fr/offre-accompagnement/reference-interoperabilite-rgi/	0
REGL_001-c	Les applications sont mises en œuvre conformément au RGAA (Référentiel général d'amélioration de l'accessibilité) : https://accessibilite.numerique.gouv.fr/	0
REGL_002-a	Pour les applications qui ne sont pas des téléservices, l'objectif de conformité au référentiel RGS est poursuivi.	2
REGL_002-b	Pour les applications qui ne sont pas des téléservices, l'objectif de conformité au référentiel RGI est poursuivi.	2
REGL_003	La page d'accueil de la solution permet d'accéder aux mentions légales : licence d'utilisation du logiciel, point de contact éditorial et technique, éventuelles mentions légales règlementaires concernant les données à caractère personnel, l'utilisation des cookies.	0
REGL_008	La gestion des cookies est conforme à la règlementation en vigueur. La solution permet d'afficher la liste des cookies nécessaires à son fonctionnement et la manière de les supprimer dans les navigateurs supportés.	0
REGL_009	La solution s'interface avec ou gère une plateforme de gestion des consentements (consent management platform) permettant de débrayer le positionnement des cookies non essentiels.	1

2.1.1 Politique Générale de Sécurité des systèmes d'Information

Concernant les aspects sécurité, les objectifs de la Politique Générale de Sécurité des systèmes d'Information (PGSI[1]) du CNRS sont les suivants :

- Protéger le savoir-faire du CNRS et les données permettant de valoriser la recherche ;
- Assurer la protection du potentiel scientifique et technique et le respect des engagements internationaux ;
- Garantir la disponibilité des moyens opérationnels du CNRS ;
- Assurer le respect par le CNRS de ses obligations légales, règlementaires et contractuelles ;
- Eviter les accidents qui résulteraient de la perte de contrôle d'un processus ou tout au moins en limiter les conséquences ;
- Conserver au CNRS un statut de partenaire de confiance.
- Toute certification cybersécurité type ISO 27001, sera considérée comme un plus dans la candidature .

A ces fins, le CNRS applique les principes de politique générale suivants (issus de la PGSI du CNRS) :

- L'ensemble du périmètre placé sous la responsabilité du CNRS doit être couvert ;

[1] **PGSI :** document diffusable sur demande à l'équipe sécurité de la DSI du CNRS

- Toutes les exigences légales et règlementaires doivent être prises en compte ;
- La gestion des risques doit être réalisée de façon systématique suivant la règlementation Française et les normes internationales en vigueur ;
- L'organisation qui est mise en place pour piloter et mettre en œuvre cette politique doit disposer des moyens humains compétents en nombre suffisant ;
- Les mesures de protection devront être complétées par des mesures de défense active efficaces ;
- L'application de cette politique est contrôlée.
- Le CNRS fera valider en interne les profils des personnels ayant des droits d'accès sur les infrastructures opérées par le CNRS.

D'un point de vue contractuel, le titulaire doit respecter au minimum les exigences sécurité du présent CCTP.

Référence	Libellé exigence	Priorité
REGL_004	Le titulaire se conforme au cadre réglementaire applicable en termes de SSI, à savoir (de façon non exhaustive) : - les annexes techniques du Référentiel Général de Sécurité (RGS) - la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSI-E) - l'instruction interministérielle 901 (II 901) portant sur les informations sensibles marquées « diffusion restreinte » - la PSSI du CNRS (PSSI-C). RGS : https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs PSSI-E : https://www.legifrance.gouv.fr/circulaire/id/38641 II 901 : https://cyber.gouv.fr/instruction-interministerielle-n901 PSSI-C : document non public, disponible sur demande	0
REGL_005	D'un point de vue technique, le titulaire applique les différents guides de l'ANSSI : https://cyber.gouv.fr/publications?field_type_de_publication_target_id%5B934%5D=934	1

2.1.2 Protection des données à caractère personnel (DCP)

La politique de protection des données personnelles au CNRS se conforme à la règlementation en vigueur (Règlement européen sur la protection des données – Règlement UE 2016/679 et Loi informatique et libertés modifiée).

Pour l'ensemble des processus mobilisant son SI, le CNRS est responsable des traitements de données, qui sont inscrits dans le registre tenu par la déléguée à la protection des données (DPD) de l'établissement.

Le titulaire est informé que le transfert de données sensibles ou personnelles vers le SI du titulaire est interdit dans le cadre des prestations de cet accord-cadre.

Le titulaire est informé que s'il a lui-même recours à des sous-traitants, les dispositions qui lui sont applicables le sont automatiquement à ses sous-traitants, et qu'il fait son affaire de leur information et de la contractualisation écrite de ces obligations. Le CNRS demande communication de ces engagements lors de la phase de consultation et est à tout moment autorisé à vérifier, conformément à la clause d'audit, la réalité de cet engagement.

Le titulaire est responsable, dans les limites imposées par la loi, de la sécurité (confidentialité, intégrité et disponibilité) des DCP qu'il traite et auxquelles il a accès.

Prise en compte de la sécurité et du respect de la vie privée par défaut dans les développements

Le titulaire répond aux exigences de sécurité du présent cahier des charges, et complète sa réponse en décrivant la démarche industrielle qu'il met en œuvre pour répondre aux exigences de l'article 252 du RGPD. Il indique quels outils et quelles méthodes il met en œuvre pour atteindre l'objectif de conformité. Ces éléments peuvent faire l'objet d'un contrôle par le CNRS.

Obligation d'information du CNRS en cas de faille de sécurité impactant le SI du titulaire

En cas d'incident de sécurité touchant le SI du titulaire et pouvant mettre en péril les DCP confiées par le CNRS (notamment, compromettant les accès au SI CNRS utilisés pour la réalisation des prestations), le titulaire informe immédiatement et de manière exhaustive le CNRS de l'événement.

Le CNRS peut demander tout complément d'information pour lui permettre d'apprécier la portée de l'incident, afin d'apprécier la nécessité d'informer l'autorité de régulation et/ou les personnes concernées dans les cas prévus par la règlementation.

2.1.3 Interopérabilité

Le référentiel général d'interopérabilité (RGI) est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration.

Ces recommandations constituent les objectifs à atteindre pour favoriser l'interopérabilité. Elles permettent aux acteurs cherchant à interagir et donc à favoriser l'interopérabilité de leur système d'information, d'aller au-delà de simples arrangements bilatéraux.

Le RGI est défini dans l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Dans l'article 11 de cette ordonnance, le « RGI fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publications de ce référentiel sont fixées par décret ».

Le référentiel général d'interopérabilité applicable est disponible en libre accès :

https://www.numerique.gouv.fr/offre-accompagnement/reference-interoperabilite-rgi/

Le titulaire respecte les dispositions du profil d'interopérabilité P1 et P4 choisi par le CNRS conformément aux objectifs du présent accord cadre.

2.1.4 Accessibilité numérique

2.1.4.1 *Contexte*

Comme le définit l'article 47 de la loi 2005-102 du 11 février 2005, est concerné par l'obligation légale d'accessibilité tout type d'information sous forme numérique quels que soient le moyen d'accès, les contenus et le mode de consultation.

Sont donc concernés tous les services publics de type internet, intranet, extranet, applications web (développement spécifique ou progiciels intégrés au SI), applications mobiles ainsi que les documents émanant de tous ces services (PDF…).

2.1.4.2 *Niveau attendu pour l'accessibilité numérique*

La solution prend en compte le niveau légalement attendu pour l'accessibilité numérique qui est à ce jour le niveau double A (AA).

Le référentiel d'accessibilité applicable est disponible en libre accès :

https://accessibilite.numerique.gouv.fr/

Les critères à retenir du référentiel général d'amélioration de l'accessibilité (RGAA) dans sa version 4.1 sont donc tous ceux permettant de répondre aux niveaux déduits [A] et [AA] du WCAG (Web Content Accessibility Guidelines).

Niveaux de conformité WCAG :

Niveau	Définition de la conformité	Critères
A (niveau minimal)	La page web satisfait à tous les critères de succès de niveau A ou une version de remplacement est fournie.	Critères de succès essentiels pouvant raisonnablement s'appliquer à toutes les ressources web.
AA	La page web remplit tous les critères de succès de niveau A et AA ou une version de remplacement conforme au niveau AA est fournie.	Critères de succès pouvant raisonnablement s'appliquer à toutes les ressources web.

Le titulaire s'assure du niveau de conformité avec des outils appropriés et fournit ses résultats sur demande du CNRS.

2.1.4.3 *Déclaration de conformité*

Référence	Libellé exigence	Priorité
ACC_001	Dans les applications déjà existantes, toute nouvelle page est, a minima, navigable et utilisable en désactivant la CSS (synthèse vocale et navigation clavier).	1
ACC_002	Pour un progiciel, le titulaire s'assure que le progiciel fourni ou distribué est accompagné d'une déclaration d'accessibilité valide. Cette déclaration est consultable via un lien conforme au RGAA.	1

Référence	Libellé exigence	Priorité
ACC_003	A minima la page d'accueil de chaque application doit contenir un lien dont le nom reflète le niveau de conformité (« Accessibilité : totalement conforme » ou « Accessibilité : partiellement conforme » ou « Accessibilité : non conforme »). Ce lien pointe vers la déclaration d'accessibilité fournie par le CNRS (PDF ou page html) ou le titulaire (cas des progiciels). La mise à jour de l'intitulé du lien et de la déclaration d'accessibilité doit être possible sans nouveau déploiement de l'application. Dans la mesure du possible, il est demandé de mettre le lien dans un pied de page (footer) visible sur toutes les pages de l'application.	0
ACC_004	Le titulaire est informé que le CNRS conduit des audits de conformité, par ses propres équipes ou par celles de tiers désignés par lui, ayant pour objectifs : ▪ de vérifier le respect par le titulaire de ses engagements initiaux mis en œuvre concernant le RGAA sur un ensemble de pages représentatives de l'application ainsi que les pages règlementaires obligatoires ▪ de publier la déclaration de conformité (créée ou mise à jour selon l'audit). Le résultat des audits conduit à la rédaction d'un plan d'action de la part du titulaire. Les actions inscrites ne conduisent pas à facturation supplémentaire de la part du titulaire si elles découlent directement d'un constat de non-conformité par rapport : ▪ à ses engagements initiaux ou ▪ à la règlementation en vigueur à la date de notification de l'appel d'offre. Dans tous les autres cas (évolution de la règlementation, évolution d'une application...), le titulaire propose une cotation pour la réalisation des prestations de mise en conformité.	0

L'échantillon sur lequel est réalisé l'audit de conformité porte **au moins** sur les pages listées sur le site RGAA (https://accessibilite.numerique.gouv.fr/obligations/evaluation-conformite/).

2.1.5 Principes de réalisation numérique responsable

Le CNRS a pour ambition de mettre à disposition de ses utilisateurs des applications conçues dans une démarche écoresponsable afin de réduire au maximum ses gaz à effet de serre (GES) et ses besoins en ressources énergétiques. Les principaux leviers sont listés ci-dessous :

- Limiter les solutions proposées dans les applications aux besoins réels des utilisateurs (frugalité des besoins) ;
- Accroître la durée de vie des applications en améliorant leur urbanisation et leur maintenance ;
- Favoriser la mutualisation et l'utilisation de briques transverses ;
- Dimensionner de façon juste les infrastructures ;
- Privilégier des solutions techniques simples et peu coûteuses vis-à-vis des données échangées (*ex : poids des pages, formats utilisés …*) ;
- Choisir des composants libres et pérennes, reconnus et maintenus par la communauté ;
- Améliorer la sécurisation des applicatifs pour limiter l'occurrence des incidents et leur coût de gestion.

Le titulaire respecte au mieux ces grands principes qui doivent guider ses choix de conception.

Ces principes peuvent être complétés par les préconisations du chapitre « Services numériques » du guide « Bonnes pratiques numérique responsable pour les organisations » de la Direction Interministérielle du Numérique (DINUM) :

https://ecoresponsable.numerique.gouv.fr/docs/2023/guide-de-bonnes-pratiques-numerique-responsable-version-1.pdf.

2.2 PRÉSENTATION DES INFRASTRUCTURES DU SI CNRS

2.2.1 Sites et utilisateurs du système d'information

Les utilisateurs du système d'information du CNRS sont principalement répartis :

- dans les 17 délégations, en régions et en Ile de France et sur le siège parisien de l'établissement. Ils représentent environ 3000 agents, dotés principalement de poste de travail de type PC sous Windows ;
- dans l'ensemble des laboratoires, répartis sur l'ensemble du territoire. Ils représentent plus de 120 000 personnes potentiellement utilisateurs du système d'information dont plus de 30 000 agents CNRS.

2.2.2 Centres serveurs

Toutes les applications du SI et services techniques associés sont hébergés sur des centres serveurs mutualisés qui disposent des caractéristiques physiques, techniques et organisationnelles pour ce type d'activité.

Le centre principal d'hébergement, situé à VILLEURBANE (69), est géré par une entité interne au CNRS.

2.2.3 Réseau

Les sites CNRS sont très majoritairement connectés au réseau national de la recherche : RENATER.

RENATER offre plusieurs points de présence (Nœud de Raccordement) sur le territoire national à l'ensemble de la communauté enseignement supérieur et recherche.

Il permet de connecter les sites de la recherche, directement ou au travers de réseaux métropolitains.

On trouvera sur le site du groupement d'intérêt public (GIP) en charge de ce réseau tous les éléments d'informations disponibles : https://www.renater.fr/

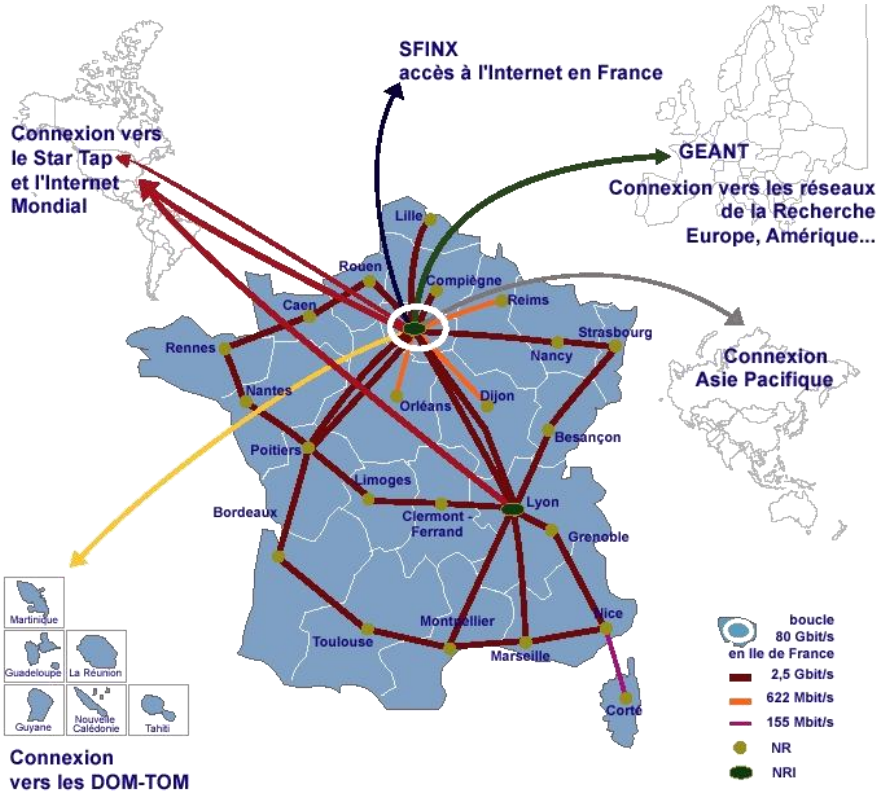


Figure 1 : Réseau RENATER

Afin d'avoir la maîtrise des flux spécifiques du système d'information du CNRS, la DSI a construit un réseau dédié, Sires, qui fédère l'ensemble des sites administratifs et des centres serveurs. Sires s'appuie sur l'infrastructure de RENATER et il est opéré au travers d'un marché d'infogérance.

Les centres serveurs sont directement reliés sur RENATER.

Tous les flux du SI sont aujourd'hui de type IPV4. La gestion du réseau s'appuie largement sur les technologies de réseaux privés virtuels (VLAN), de translation d'adresses IP (NAT) et de chiffrement (via une technologie de type VPN ou autre).

La sécurisation des flux est basée sur du filtrage de flux et des technologies de firewall standards.

2.2.4 Infrastructures

Les infrastructures matérielles utilisées sur les centres serveurs sont normalisées. La construction de ces architectures a été basée sur deux préoccupations majeures :

- Mettre en œuvre des technologies capables de répondre aux exigences de qualité de service du SI CNRS, en termes de performances, disponibilité, intégrité et sécurité.

- Rationaliser et homogénéiser les équipements pour favoriser la maîtrise technique et minimiser les coûts de possession.

Les applications du SI CNRS sont hébergées sur une infrastructure virtualisée, sauf en cas de contraintes spécifiques.

2.3 PRINCIPES D'URBANISATION ET D'INTÉGRATION DANS LE SI

2.3.1 Principes généraux

La démarche d'urbanisation mise en œuvre à la DSI du CNRS doit accompagner, faciliter et maîtriser la transformation continue et progressive du SI en le rendant de plus en plus agile et en assurant sa pérennité pour en tirer le maximum de plus-value, en cohérence avec les orientations stratégiques, métiers et opérationnelles de l'organisme.

Cette démarche doit aider l'évolution du SI par une optimisation de l'existant, tournée vers les objectifs suivants :

- capitaliser sur les socles existants ;
- poursuivre l'intégration des différents systèmes dans l'optique d'une gestion modernisée ;
- garantir la fiabilité des données de référence dans le système d'information global.

Plus particulièrement, 4 grands principes sont mis en avant par la démarche d'urbanisation et d'intégration dans les SI :

1. Principe de cohérence forte pour aider à répartir les contours fonctionnels et informationnels entre les applications du SI dans le but d'éviter toute redondance fonctionnelle et de limiter les flux entre applications participant au même processus métier. Un modèle informationnel et un modèle des processus métier sont fortement recommandés, voire attendus, pour aider à ces choix de répartition applicative ;
2. Principe de couplage faible entre applications pour réduire les dépendances entre applications et ainsi limiter les impacts sur le SI en cas d'évolution d'une partie de ce SI ;
3. Développer l'utilisation de briques numériques, fonctionnelles et/ou applicatives communes et mutualisées dans une logique de plateformes transverses ;
4. Prendre en compte la dimension « laboratoire » et ainsi découpler de façon modulaire (modules applicatifs disjoints) autant que faire se peut les fonctionnalités « Etablissement » des fonctionnalités « Laboratoire » dans la perspective de futures mutualisations potentielles des fonctionnalités « Laboratoire » et d'éventuelle répartition dans des SI distincts des fonctionnalités « Etablissement » et « Laboratoire » ; le tout en cohérence avec les actions parallèles éventuelles sur les mêmes sujets par les SI des établissements partenaires du CNRS.

L'architecture proposée par le titulaire est soumise à la validation de la DSI du CNRS.

2.3.2 Principes d'échanges

Pour mettre en œuvre le principe de couplage faible, des protocoles d'échanges sont établis, préconisant l'utilisation de :

- systèmes d'intermédiation (cf. § 2.3.3.1) pour éviter les échanges point à point entre deux applications en procédant par ½ flux via ces systèmes d'intermédiation ;
- formats d'échange communs sous la forme de format pivot par objet métier échangé. Le format pivot, indépendant des applications et de leur modèle de données, est une représentation partagée et intrinsèque d'un objet (métier ou technique), tenant compte de l'ensemble de ses cas d'usages. Il précise aussi les référentiels et nomenclatures communs et partagés à utiliser éventuellement pour ses attributs ;
- fonctions d'intégration (ou services applicatifs) de ces formats pivots dans le cadre des flux entrants ;
- fonctions d'exposition (ou services applicatifs) des informations vers ces formats pivots dans le cadre des flux sortants.

Ces échanges sont conçus en respectant le principe de frugalité des données échangées (échanges limités aux données strictement nécessaires) dans un souci de conception écoresponsable et de limitation des ressources utilisées.

Ces principes s'appliquent aussi bien aux échanges de données et informations internes au SI qu'aux échanges avec l'extérieur.

2.3.3 Plateformes transverses et services proposés

2.3.3.1 *Systèmes d'intermédiation*

Actuellement les systèmes d'intermédiation mis en œuvre dans le SI du CNRS sont :

- un gestionnaire applicatif d'échanges et de services « outil EAI/ESB CNRS » (découpage en ½ flux, format pivot des objets métiers échangés) qui a la responsabilité et la gestion des échanges en termes d'orchestration, de chronologie des flux le cas échéant, de transcodification des données vers les SI cibles ou depuis les SI sources ;
- un proxy de services web ;
- une exposition de services web de données de référence (mise à disposition des formats pivots persistés des objets métiers de référence)

2.3.3.2 *Gestion des données de référence*

La DSI du CNRS dispose d'un outil MDM – Master Data Management (GDR – Gestion des Données de Référence) nommé Réséda et proposant des services de gouvernance afin d'assurer la qualité, l'intégrité et l'exactitude des données de référence tout au long de leur cycle de vie.

L'usage de cette plateforme est fortement préconisé pour les référentiels structurants et partagés pour lesquels une gouvernance métier est attendue entre différents acteurs métiers.

Actuellement Réséda gère les référentiels suivants (liste non exhaustive) :

- Structures organisationnelles du CNRS ;
- Personnels (CNRS et non CNRS) des structures du CNRS ;
- Fournisseurs ;
- Partenaires ;
- Contacts.

Ainsi qu'un certain nombre de nomenclatures.

La mise à disposition, au reste du SI CNRS, des données de ces référentiels se fait par les services web de données de référence (cf. plus haut).

2.3.3.3 *Fournisseurs d'identité*

Les services d'authentification web centralisée du CNRS (web SSO) via le protocole SAML 2.0, sont regroupés sous la dénomination de Janus. Ils consistent en plusieurs fournisseurs d'identités (IdP) dépendants de la population à authentifier (Personnel des unités CNRS, Prestataires et usagers des unités CNRS, Externes) et du niveau d'authentification nécessaire.

Dans le cas où plusieurs fournisseurs d'identités peuvent être utilisés pour accéder à la solution, un mécanisme de sélection par l'utilisateur du fournisseur d'identité est mis en place. Ce mécanisme est nommé WAYF (Where Are You From).

Ils s'appuient sur le référentiel des comptes utilisateurs du SI CNRS alimenté par le service IAM (cf. § 2.3.3.4).

2.3.3.4 *Service référentiel des comptes utilisateurs et gestion des accès et habilitations (IAM)*

Ce service recouvre des outils qui permettent la mise à jour du référentiel de comptes utilisateurs du SI CNRS à partir des données du référentiel des personnels des structures du CNRS.

Les données du référentiel des comptes utilisateurs sont exposées par des services Web à l'usage des applications. Elles sont également pour certaines transmises à l'application via le processus d'authentification.

Une gestion des accès applicatifs est également en place et va continuer à dans le futur pour prendre en compte une plus grande automatisation et de nouvelles fonctionnalités pour l'attribution de rôles applicatifs à des comptes utilisateurs.

2.3.3.5 *Gestion électronique de document (GED) et archivage*

La GED du CNRS propose des services dédiés aux applications pour stocker, gérer, mettre à disposition voire archiver les documents nécessaires et/ou produits par ces applications.

La plateforme de dématérialisation offre aussi des services :

- d'archivage (courant, intermédiaire et pérenne).

- de parapheur électronique, incluant des fonctionnalités de signature électronique.

2.3.3.6 *Services de recueil et de mise à disposition des consentements (RGPD) (bientôt disponible)*

Le CNRS propose un service de gestion des consentements, au sens du Règlement général sur la protection des données (RGPD), dont les principales fonctions sont la captation, la conservation, l'historisation et la diffusion des consentements des personnes sur les traitements de leurs données personnelles.

Les entrants de ce service sont la définition des populations cibles (en extension ou en compréhension), les documents d'information des personnes, la liste des traitements concernés, et éventuellement les consentements pour ceux recueillis par ailleurs.

2.3.4 Prise en compte des changements de l'organisation structurelle du CNRS et de son environnement (Enseignement Supérieur et Recherche – ESR)

Dans le cadre de la transformation progressive et continue vers un système d'information qui permet un alignement sur les stratégies de l'établissement, les outils proposés pour les SI et applications doivent prendre en considération, le plus nativement possible, les différentes restructurations du CNRS :

- Chaque année, une partie des unités de recherche est renumérotée, fusionnée, éclatée, … (changement de référence métier) ;
- Les instances (conseils scientifiques du CNRS et des instituts, sections et commissions interdisciplinaires) du Comité national de la recherche scientifique (changement de périmètre sans changement systématique de référence métier) renouvelées tous les 5 ans ;
- Les restructurations des établissements de l'ESR (COMUE, établissements expérimentaux, fusion d'établissements, …)
- Les restructurations organisationnelles du CNRS (exemple : en 2023, la fusion de la délégation Normandie avec la délégation Paris Michel Ange ; en 2020 le remplacement des certains types d'unités et des catégories des structures de recherche ; en 2009, le remplacement des départements scientifiques par des Instituts nationaux…)

Référence	Libellé exigence	Priorité
URB_001	La solution est en capacité de fournir une continuité de service fonctionnelle dans le temps, en tenant compte des différents types de restructuration de l'organisation CNRS et de l'ESR, impactant les SI et applications. Le choix des mécanismes à implémenter est étudié et validé entre le titulaire et le CNRS (équipes projet et transverses).	1

Le référentiel d'organisation du CNRS est géré via l'outil GDR, et plus particulièrement dans le référentiel Réséda Structure.

Le référentiel des établissements de l'ESR partenaires du CNRS est lui-aussi géré dans cet outil, et plus particulièrement dans le référentiel Réséda Contact (y compris la description des restructurations ponctuelles des établissements de l'ESR) s'appuyant sur le référentiel Réséda Partenaire. Les restructurations cycliques de l'organisation du CNRS, tout comme les éventuelles restructurations ponctuelles des établissements sont prises en compte dans la plateforme Réséda puis sont diffusées à l'ensemble du SI à partir de ces référentiels, au travers de web services disponibles depuis les systèmes d'intermédiation.

Référence	Libellé exigence	Priorité
URB_002	La solution s'alimente du référentiel d'organisation structurelle du CNRS, ainsi que, si utile ou nécessaire, du référentiel des établissements de l'ESR partenaires du CNRS, à partir de ses services web dédiés.	1

3 DESCRIPTION DE LA SOLUTION

3.1 PRÉSENTATION DE LA SOLUTION

3.1.1 Présentation fonctionnelle

La solution DMF (Dématérialisation des Factures) est la composante SI du projet d'établissement P2D2 (projet de dématérialisation et de pilotage de la dépense) et s'inscrit dans la démarche de modernisation de l'état et dans un processus visant la dématérialisation et l'automatisation complète du circuit de la dépense.

Elle constitue l'étape de dématérialisation et d'automatisation du traitement des factures fournisseurs (environ 500 000 documents par an). Elle permet d'optimiser le processus de la dépense, de proposer un accès plus performant aux données de facturation à tous les acteurs concernés par la chaîne achat/dépense et de diminuer les délais de paiement.

La solution DMF est interfacée avec le portail de l'état Chorus Pro (CPP) - plateforme de dématérialisation des factures de l'état, des collectivités territoriales et des établissements publics, qui est devenu progressivement depuis janvier 2017 le canal obligatoire pour les émetteurs de facture à destination de ces derniers. Dans le contexte CNRS, cette solution permet de traiter les documents suivants :

- Factures fournisseur, en référence à une ou plusieurs commandes, ou à un marché
- Acomptes fournisseur qui sont gérés à l'identique des factures
- Avoirs fournisseur, en référence à une et une seule facture
- Factures de travaux

Lien vers la documentation du portail Chorus Pro : https://portail.chorus-pro.gouv.fr/aife_documentation

En 2024, cela représente environ 400 000 documents/an. Les factures « papiers » étaient à la marge et sont gérées depuis 2025 par une solution intégrée à l'application DMF dite de « saisie rapide ».

Le nombre total peut être porté à 800 000 documents si les factures « Carte logée » déposées sur le portail Chorus PRO sont considérées. Ces factures ne font pas, dans ce cas, l'objet de contrôles automatisés dans la solution. Elles sont comptabilisées directement dans le SI finance via un relevé d'opérations bancaires. Les flux pivots correspondant à ces factures seront uniquement à archiver dans le coffre-fort électronique.

Les utilisateurs de la solution sont :

- Le SCD : Service Centralisé de la Dépense situé à Vandoeuvre les Nancy, responsable du traitement des factures et de la gestion du référentiel fournisseur : environ 40 gestionnaires
- Les gestionnaires dépense des Services Financier et Comptable (SFC) en Délégation Régionale qui assure le support aux unités, environ 200 utilisateurs.
- Les gestionnaires financiers des unités qui effectuent les commandes et réceptionnent les marchandises. Environ 3000 utilisateurs.

La solution DMF est constituée des modules suivants :

- KOFAX PDAP – Process Director Account sous forme d'addon SAP : pour l'intégration, les contrôles, le rapprochement et la comptabilisation des documents dans SAP.
- Traitement des litiges : pour l'automatisation de la validation et des workflows de gestion des litiges
  - Work Cycle ; intégré à un portail SAP : pour le traitement des workflows destinés aux gestionnaire des services financiers en Délégation Régionale.
  - PD Web ; Version web : pour les gestionnaires d'unité.
- DMF-Consult (module intégré à la plateforme de DEMAT) : application web pour le partage des informations de factures, la visualisation des factures à destination des gestionnaires d'unité (et des SFC).

Les factures et avoirs dématérialisés issues du portail Chorus Pro sont récupérés en mode API par le système d'intermédiation EAI/ESB qui les archive dans un coffre-fort électronique hébergé par CDC Arkhineo avant de les intégrer dans le module PDAP (SAP).

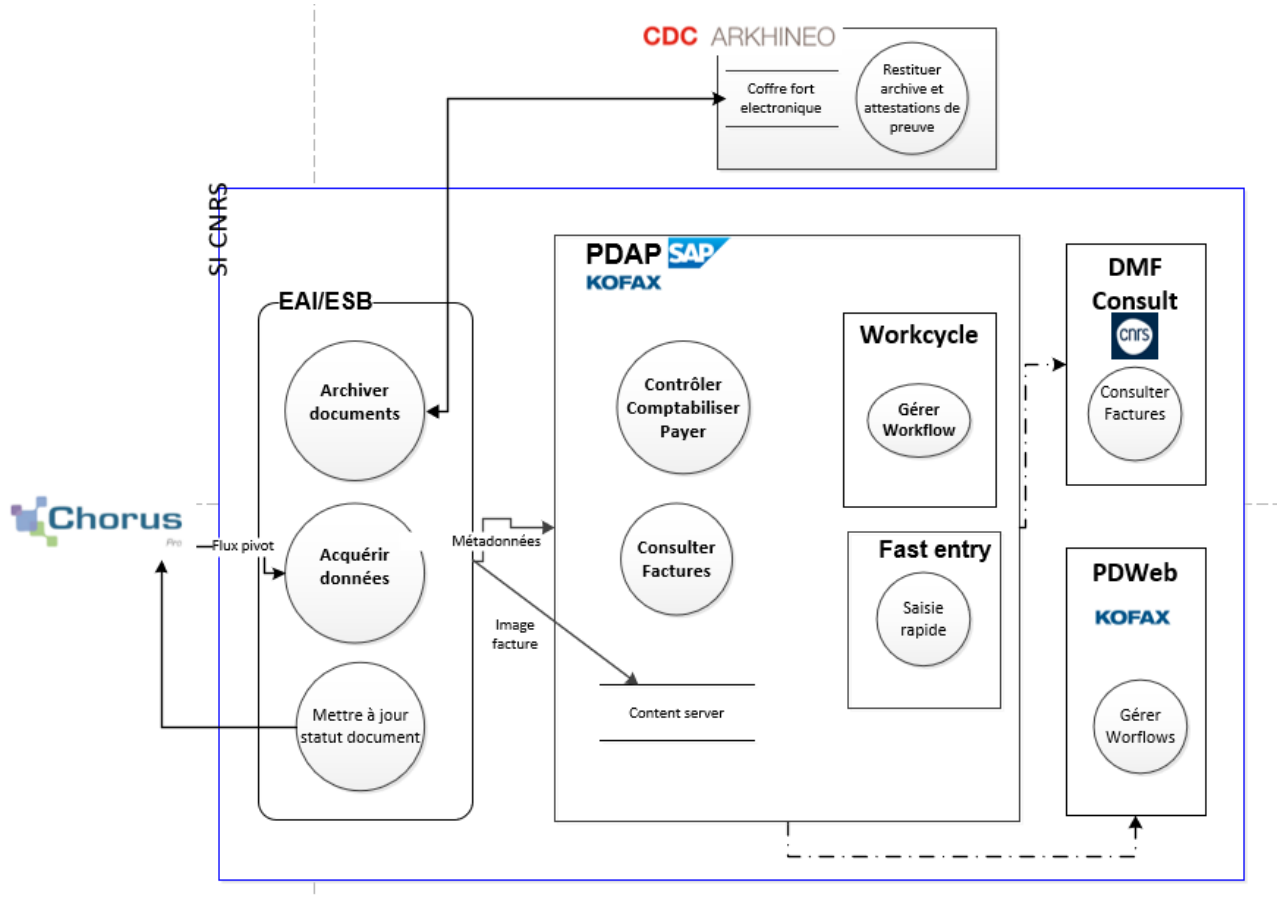


Figure 2 : Présentation de la solution DMF

3.1.2 Intégration dans le SI

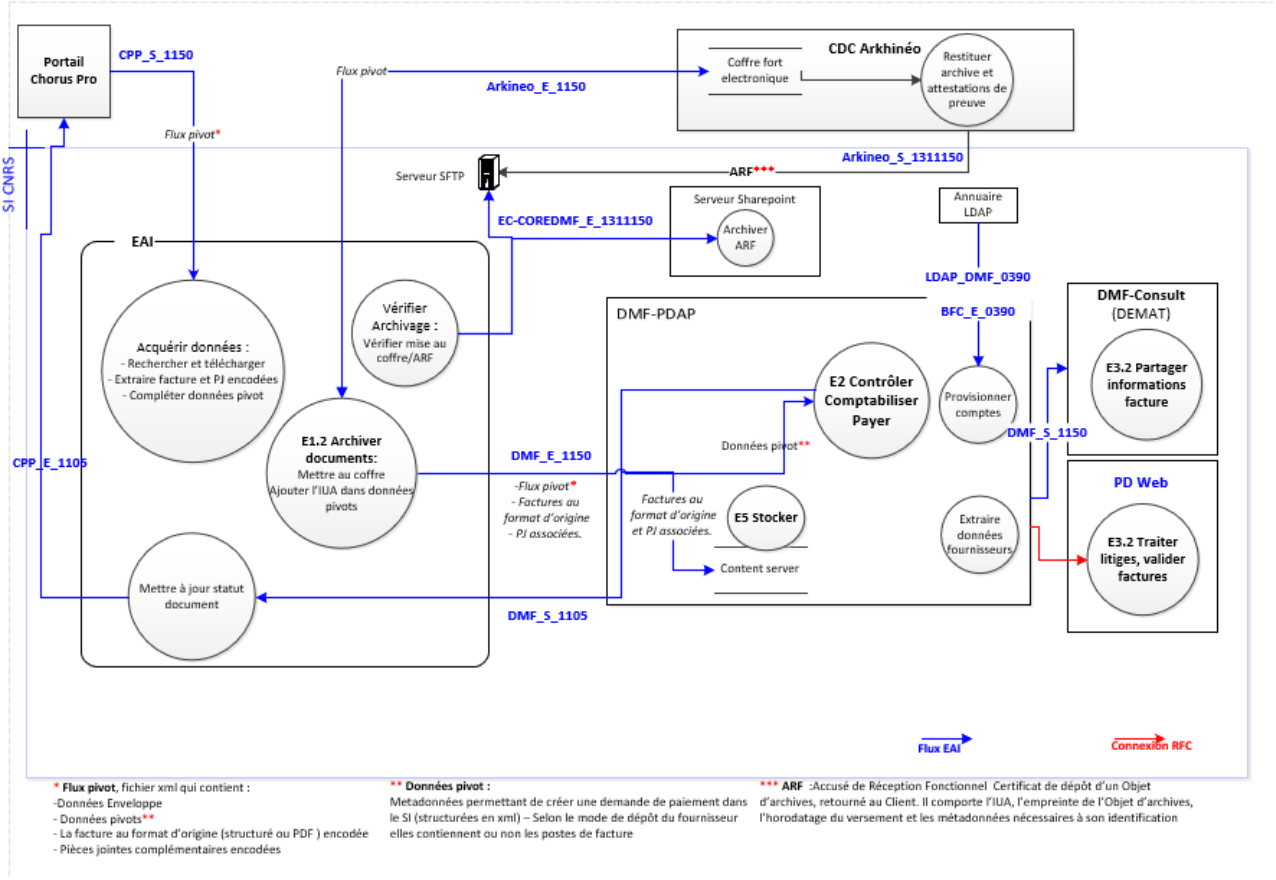


Figure 3 : Flux de la solution DMF

3.1.2.1 *Traitement des factures papiers (E1.1)*

Les données des factures papier sont manuellement saisies dans PDAP SAP via un formulaire de saisie dédié.

Le fichier correspondant à l'image facture est ajouté manuellement sur PDAP SAP puis déposé automatiquement sur le content Server SAP et associé au document crée dans PDAP.

3.1.2.2 *Archiver Documents (E1.2)*

Le flux pivot issu du Portail Chorus Pro est un fichier au format xml contenant les métadonnées relatives au document (de type facture, facture de travaux ou avoir) la facture au format d'origine et les pièces jointes associées encodées sont récupérées sur le portail Chorus Pro en mode API par le système d'intermédiation EAI/ESB. Deux API sont utilisées (« RechercherFactureParRecipiendaire » et « TelechargerGroupeFacture »)

Le système d'intermédiation EAI/ESB extrait les fichiers encodés et enrichi les données pivots. (**Flux CPP_S_1150**)

Le flux pivot d'origine (y compris les pièces justificatives) est déposé dans un coffre-fort électronique hébergé par CDC Arkhineo. (Flux **Arkineo_E_1150)**

Les métadonnées sont intégrées à la solution Process Director de Kofax (PDAP) via idoc (EDI cockpit) et permettent la création d'un document PDAP. Les factures/avoirs et pièces jointes sont associées à ce document sont stockées sur le content server SAP. (**Flux DMF_E_1150**)

Le statut des documents traité (rejet, recyclage, paiement) dans PDAP sont transmis par le système d'intermédiation EAI/ESB au portail Chorus Pro via l'appel de l'API « MiseAjourStatutFacture ») (**Flux DMF_E_1150**)

3.1.2.3 *Contrôle et comptabilisation des documents (E2)*

PDAP matérialise le document fournisseur par un document PD (document Process Director) qui porte le processus jusqu'à la prise en charge. Ce document PD est composé de l'entête et des postes de la facture.

Process Director effectue les tâches suivantes :

- Le garnissage des documents (détermination du fournisseur, détermination de la commande, détermination des postes de commande, détermination des codes TVA, coordonnées bancaires et autres alimentations automatiques)
- Les contrôles (bloquants ou non)
- Le lancement des workflow (automatiques déclenchés sur la base des contrôles ou manuels)
- La comptabilisation dans BFC (solution SAP implémentée au CNRS pour gérer les processus financiers)

Le statut des documents traités (rejet, recyclage, paiement) dans PDAP est transmis par le système d'intermédiation EAI/ESB pour mises à jour sur le portail Chorus Pro (**Flux DMF_E_1150**)

3.1.2.4 *Traitement des litiges (E3.1)*

Les litiges et validation des documents sont gérés via un module dédié qui est une extension de Process Director.

Il véhicule le document PDAP auprès des différentes parties prenantes du processus de décision à l'aide de workflow(s).

Deux moyens d'accès au traitement des litiges sont exploités. Les gestionnaires en SFC se connectent directement à BFC et accèdent à WORKCYCLE au travers d'un portail SAP NetWeaver. Les gestionnaires d'unités se connectent via l'application Web (PD Web).

3.1.2.5 *Consultation des factures (E3.2)*

La consultation des factures pour les utilisateurs non SAP (gestionnaires d'unité) s'effectue au travers de la plateforme de DEMAT et l'outils DMF Consult.

Il restitue les informations facture (dont le statut de traitement), l'image facture et les pièces jointes associées. Il restitue également des données relatives aux commandes et aux fournisseurs.

Pour les utilisateurs SAP (uniquement avec un profil SFC), l'accès s'effectue via BFC.

3.1.2.6 *Etats de pilotage (E4)*

Le reporting est fourni par la solution Performance Analytics Readsoft. Il collecte les données issues de Process Director et les restituent au travers de requêtes préconçues. Cet outil s'appuie sur la plateforme SAP BI de la solution BFC.

3.1.2.7 *Stockage des fichiers (E5)*

Les fichiers correspondants à la facture au format d'origine (PDF ou format structuré), l'image facture reconstituée (pour les factures au format structuré) et les pièces jointes associées sont archivés via une configuration dédiée de SAP Archivelink sur le CONTENT SERVER.

Lors du transfert du document fournisseur dans Process Director via idoc pour les factures Chorus Pro ou via saisie manuelle pour les factures « papier », les fichiers sont archivés automatiquement dans le Content Server SAP via Archivelink, et rattachés au document Process Director. La visualisation de ces documents est disponible depuis Process Director, Work Cycle /PDWeb et la plateforme de DEMAT – DMF-Consult.

3.1.2.8 *Archivage dans un coffre-fort électronique*

Les flux pivot des factures issues du portail CPP comportant les fichiers encodés (facture au format d'origine (pdf ou xml), l'image facture reconstituée -si la facture est au format structurée- et les éventuelles pièces jointes complémaitres) sont archivés via le système d'intermédiation EAI/ESB dans le SAE My Arkhinéo proposé par CDC Arkhinéo.

3.1.3 Présentation technique

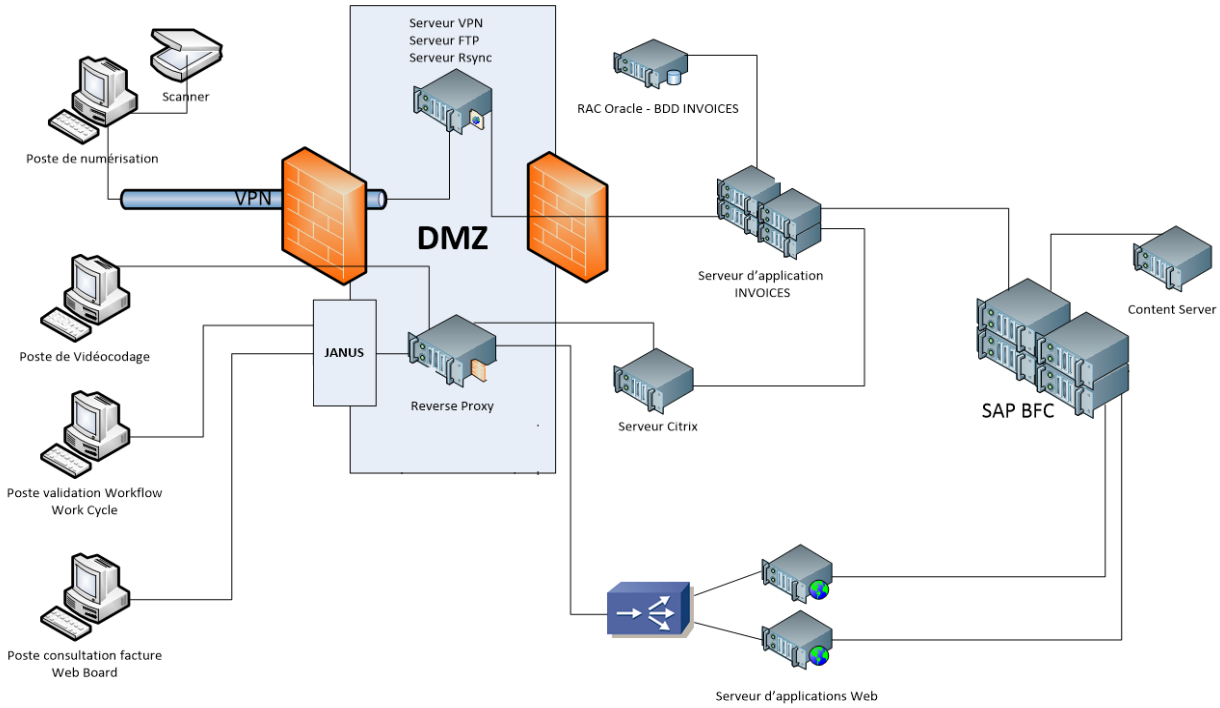


Figure 4 : Architecture technique de la solution DMF

Cf. Documents :

DMF-DARC-TRV-Description de solution technique DMF-V1.9_EXP

Au niveau applicatif, la solution DMF est composée :

- D'une application web : PD Web, accessible par les unités et par les administrateurs ;
- D'Add-On SAP, installées sur l'instance SAP BFC (Budget – Finance – Comptabilité) du CNRS. Les accès sont réservés aux membres du SCD, aux SFC et aux administrateurs ;
- Du SAE CDC Arkhineo pour l'archivage à valeur probatoire des documents. L'accès aux documents archivés est effectué grâce à la solution MyArkhineo et il est réservé aux membres du SCD et de l'équipe projet (DSI/DCIF) soit une dizaine de personnes.

Les serveurs sont tous localisés sur des sites d'hébergement en France : serveurs d'application et de base de données, serveur SAP ECC et BW, ainsi que les serveurs WEB : PD Web et Work Cycle.

Le titulaire devra posséder des compétences pointues sur ces environnements. Il aura un devoir de conseil auprès du CNRS, notamment en ce qui concerne la définition des configurations et l'optimisation des briques techniques sur lesquelles s'appuient les applications du présent marché.

3.1.4 Archivage

Les documents reçus au format numérique sont stockés sur la solution CDC Arkhineo. Une archive est créée et envoyée dans le coffre-fort électronique

Le Versement est effectué par le système d'intermédiation EAI/ESB en mode API selon le protocole HTTPS.

L'authentification s'effectue par certificat Client X.509 (en HTTPS).

Il y a deux accusés de réception mis en œuvre dans ce processus d'archivage :

- **ART** (accusé technique) : c'est un accusé synchrone. Il confirme la bonne réception de l'archive.
- **ARF** (accusé fonctionnel) : journal des accusés de réception fonctionnels (preuve de dépôt) qui est mis à disposition quotidiennement par CDC Arkhineo et déposé sur un serveur SFTP chez le titulaire et au CNRS.

3.1.5 Serveurs développement

La plate-forme de développement et de tests unitaires est mise en œuvre par le titulaire pour son besoin propre. Elle doit être compatible avec l'environnement cible qui fait référence.

La plate-forme de développement doit couvrir l'ensemble des composants de l'application hors SAP.

Elle doit pouvoir se connecter aux services d'authentification gérés par le CNRS. Par contre le CNRS ne fournit pas d'outils permettant de simuler une connexion aux services du système d'intermédiation EAI/ESB (« bouchons »). Le titulaire, si nécessaire, reproduit les fonctionnalités du système d'intermédiation EAI/ESB et/ou des services d'authentification pour ses développements.

3.1.6 Environnements CNRS

Le CNRS fournit et administre l'ensemble des plates-formes serveurs de la solution DMF à l'exception de la plate-forme de développement et de test du titulaire (à l'exception des environnements de développement SAP qui sont fournis).

Aucune donnée du CNRS n'existe à aucun moment sur les plateformes hébergées par le titulaire.

Le CNRS met à la disposition du projet :

- Un environnement de Recette : le CNRS installe en recette les livraisons du titulaire sur un environnement dédié aux recettes. La configuration logicielle de ce serveur de recette est la même que celui de production hébergeant l'application opérationnelle, alors que la configuration matérielle est au mieux proportionnelle à celle de l'environnement de production.
- Un environnement de Production : cet environnement héberge les applications DMF de production.
- Un environnement de Formation.

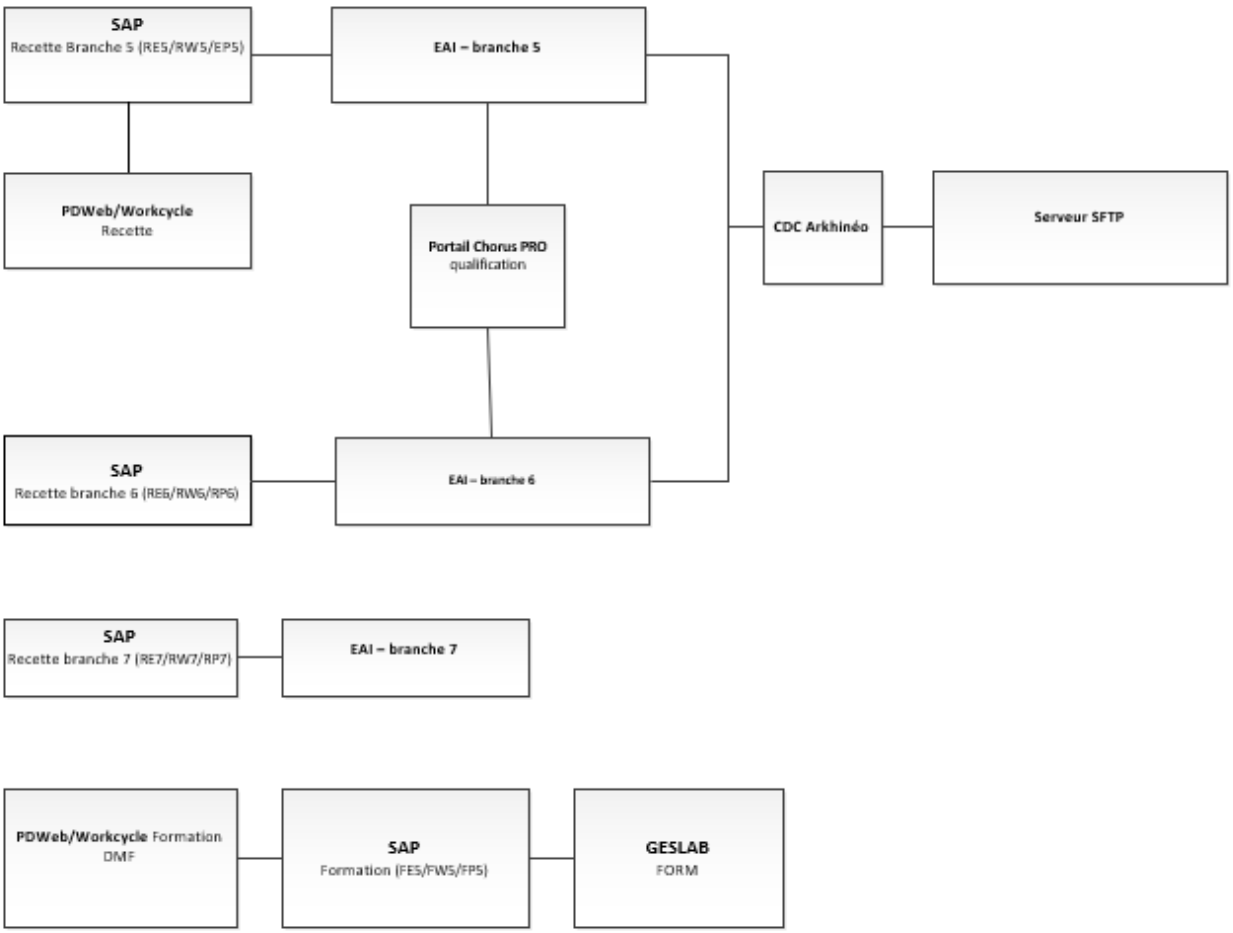


Figure 5 : Environnements non productifs de la solution DMF

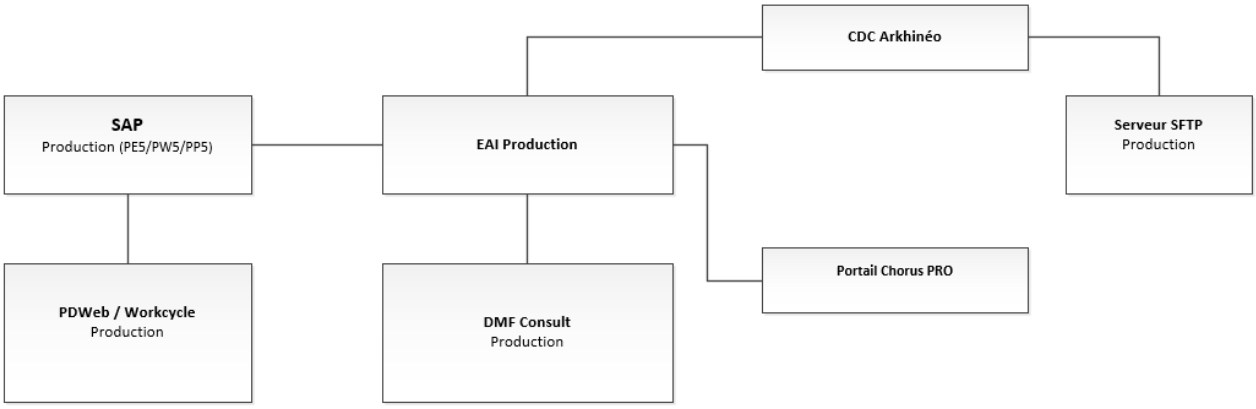


Figure 6 : Environnements productifs de la solution DMF

L'installation sur les serveurs de recette, de production et de formation est assurée par les équipes du CNRS à partir de procédures d'installation et d'exploitation rédigées par le titulaire, avec une assistance sur site CNRS du titulaire lors de la première installation.

Il est donc demandé au titulaire une grande vigilance lors de la préparation des livraisons et de la rédaction des procédures d'installation et d'exploitation.

Si le fonctionnement de l'application nécessite la mise en œuvre d'outils tiers, le titulaire assure une aide à la mise en œuvre de ces outils auprès de l'équipe CNRS.

Les environnements de recette, de formation et de production sont accessibles au titulaire sur demande expresse du CNRS et sur site CNRS uniquement.

Pour information, la plate-forme de développement SAP est gérée par un autre prestataire, dans le cadre du marché d'infogérance BFC.

La versions des composants SAP sont les suivantes :

- ECC 6 EhP 8
- BI : BW 7.50
- SAP Net Weaver 7.5 pour ECC et BW

3.1.7 Particularités de l'environnement SAP

Les composants SAP de la solution DMF sont intégrés à la solution BFC (SAP). BFC est infogérée par un prestataire nommé infogérant BFC dans la suite du paragraphe.

3.1.7.1 *Partage de responsabilité entre titulaire du marché d'infogérance BFC et le titulaire du marché DMF*

L'infogérant BFC autorise le titulaire DMF à accéder aux environnements de développement et d'intégration dont il a la charge.

L'accès à ces environnements est conditionné à l'application des processus et/ou procédures applicables qui seront décrites dans le Plan d'Assurance Qualité.

Les mises en production applicatives sont de la responsabilité du titulaire du marché d'infogérance BFC.

L'infogérant BFC a la responsabilité de :

- L'exécution de la mise en production des composants applicatifs en environnement d'intégration de recette et de production ;
- La vérification de la mise en production (installation, complétude des données en cas de chargement, fonctionnement, reprise du service en cas d'interruption, check-list transmise, etc.) ;
- Le reporting et la synchronisation avec le futur titulaire DMF et le CNRS (contenu, déroulement, statut, Incidents et dysfonctionnements éventuels rencontrés)

L'infogérant BFC créé, administre, exploite et maintien tous les environnements du Périmètre applicatif et technique, en concertation avec le CNRS. L'infogérant BFC assure notamment les activités suivantes pendant toute la durée de l'Accord Cadre :

- La maintenance et la remise à niveau (ex : installation des sources et chargement de données, des jeux de tests, rafraîchissement d'environnements, application de patchs et montées de version, …)
- La gestion des profils et des accès des utilisateurs (de l'infogérant, du CNRS et du titulaire DMF) dans les environnements de son ressort, étant entendu que le CNRS demeure le seul et unique décisionnaire final concernant les autorisations d'accès.

Concernant l'architecture matérielle, bien que l'infogérant BFC ne soit pas responsable des Add-On ReadSoft liés au système DMF implémentés sur le périmètre, l'infrastructure prend en compte les besoins de DMF en termes de puissance machine, stockage et archivage.

3.1.7.2 *Livraisons des composants applicatifs SAP*

Pour les composants SAP, les transports d'OT sur les différents environnements sont pris en charge par l'Infogérant BFC.

Les demandes de transport sont, elles, à la charge du titulaire. Ce dernier doit s'assurer de la bonne gestion de configuration des différents environnements (développement, recette intégration, production et formation) pour ce qui concerne les Add-On ReadSoft liés au système DMF et sous leur responsabilité. Notamment lors des demandes de transport en suivant le schéma en vigueur transmis par le CNRS.

3.2 VOLUMÉTRIE

L'application DMF a été mise en production au courant de l'année 2013.

3.2.1 Volumétrie des anomalies

Indiquer par année ou par période de TMA le nombre d'anomalies déclarées sur l'environnement de production depuis la mise en production de l'application.

L'application a donné lieu à la correction des anomalies[2] suivantes sur l'environnement de production :

	2022	2023	2024	2025
Anomalies bloquantes	0	0	0	0
Anomalies majeures	NA	0	1	1
Anomalies mineures	NA	4	6	8

3.2.2 Volumétrie des évolutions

Indiquer par année ou par période de TMA le nombre de jours d'évolutions de l'application depuis sa mise en production

Depuis sa mise en production, l'application a donné lieu au nombre d'évolutions suivantes :

	2022	2023	2024	2025
Nombre d'évolutions/versions	3	4	6	4 (dont une montée de version)
Nombre de jours de réalisation	15	15	32	60

3.3 EVOLUTIONS POTENTIELLES À COURT OU MOYEN TERME

Les principales évolutions identifiées à ce jour (mais restant à confirmer) portent sur les points suivants :

- Changement de système d'archivage au coffre avec migration des documents déjà archivés sur CDC Arkhineo

[2] La définition et la typologie des anomalies sont décrites dans le glossaire du Livret 2 du CCTP.

- Montée de version SAP avec passage vers SAP Hana et SAP Fiori
- L'interfaçage vers un système de gestion dématérialisée des factures et leurs PJ
- L'interfaçage avec le service référentiel de comptes et gestion des accès et habilitations (IAM).
- Un éventuel déport de fonctionnalités vers d'autres SI

4 CADRE DE COHÉRENCE TECHNIQUE DE LA SOLUTION

Ce chapitre donne les exigences applicables à tout nouveau développement, que ce soit lors de la mise en œuvre d'une nouvelle application ou dans le cadre d'évolutions d'une application existante.

4.1 EXIGENCES D'INTÉGRATION DANS LE SI

L'architecture de la solution est compatible avec l'architecture générale du SI du CNRS.

4.1.1 Répartition fonctionnelle

Référence	Libellé exigence	Priorité
URB_003	Pour assurer que l'architecture des solutions nationales va dans le sens d'une répartition urbanisée des fonctionnalités entre les applications selon le principe de cohérence fonctionnelle et informationnelle forte, l'équipe projet et le titulaire font valider le périmètre fonctionnel et informationnel de la solution par l'équipe urbanisation de la DSI.	1
URB_004	Lors de la conception et de la réalisation de la solution, les architectures transverses sont privilégiées, entre autres par l'utilisation des plateformes mutualisées et la réutilisation des briques applicatives (notion de service, voire micro-service). Ceci afin de ne pas implémenter ou développer une fonction ou un contrôle métier déjà outillé dans une autre application ou service.	1
URB_005	Lors de la conception et de la réalisation de la solution, les fonctions restant à développer pour la solution sont prévues autant que possible pour être mutualisées, voire transformées en (micro-)services utilisables par d'autres applications.	1
URB_006	L'architecture de la solution découple les fonctionnalités « Etablissement » des fonctionnalités « Laboratoire » dans des modules applicatifs distincts qui proposent des interfaces de communication (interface - programmation orientée objet, webservices, API REST, etc.). Le choix des mécanismes pour ces interfaces de communication à implémenter est étudié et validé entre le titulaire et le CNRS (équipes projet et transverses).'	1

4.1.2 Echanges de données

4.1.2.1 *Modalités générales*

Les interfaces entrantes ou sortantes entre la solution et les autres applications du SI peuvent s'effectuer de plusieurs façons dont voici les principales : échanges de fichiers (XML, JSON, CSV, …), échanges de messages (Broker), et services Web de type REST, tout en passant systématiquement par un des systèmes d'intermédiation du CNRS (cf. § 2.3.3.1).

L'objectif du CNRS est la mise en œuvre du principe de couplage faible entre les systèmes d'intermédiation et l'application.

Les échanges de données entre le gestionnaire d'échanges et de services CNRS et la solution DMF (flux entrants et flux sortants), se font au travers d'une couche d'abstraction (matérialisée par des services) pour permettre au gestionnaire d'échanges et de services CNRS d'assurer la gestion chronologique des échanges (quotidien, à la demande, …) tout en disposant de services, portés par la solution DMF, appelables par le gestionnaire d'échanges et de services CNRS à tout moment (en journée, en traitement batch).

Dans le cas des flux par appel de services web, le passage par le gestionnaire d'échanges et de services du CNRS n'est pas obligatoire, toutefois, afin de garder un découplage des échanges, ces appels de services web passent à travers un proxy de service web (de manière transparente pour l'application appelante). Dans certains cas justifiés, la mise en œuvre des services web peut être réalisée via le gestionnaire d'échanges et de services du CNRS.

Au final, la solution d'échange pour chacun des flux est définie conjointement avec le CNRS dans le cadre d'ateliers de travail dans la limite des règles prévalant au CNRS sur l'intégration des SI.

Pour les flux entrants, le CNRS détermine et met à disposition, en fonction des besoins, les données échangées nécessaires à la solution DMF.
Cependant dans le cas où certains flux entrants sont à développer par le CNRS pour les besoins spécifiques de la solution, le titulaire doit déterminer son besoin au plus tôt, ajuster son planning le cas échéant, pour permettre au CNRS la mise à disposition du nouveau flux avant la livraison de la solution.

Référence	Libellé exigence	Priorité
URB_007	Le titulaire prévoit le bon fonctionnement et la continuité de service fonctionnel de la solution qu'il développe, y compris des éventuels outils d'intégration proposés, au regard de l'architecture générale du SI, et en particulier vis-à-vis des systèmes d'intermédiations retenus au CNRS. En particulier, la solution : ▪ tient compte des arrêts de services de la solution, avec éventuellement l'émission d'un message de non disponibilité, afin de ne pas provoquer d'erreur (technique) pour les services appelants ; ▪ prend en compte et pallie la non réponse d'un service appelé en passant, par exemple, dans un mode dégradé non bloquant.	1
URB_008	Si la solution fait appel à des services fonctionnels portés par un autre SI ou application, ou met à disposition des services fonctionnels, la gestion de ces communications passe par les systèmes d'intermédiation du CNRS.	1
URB_009	La solution a la responsabilité de réaliser les services d'intégration des données et les services d'exposition des informations dont elle est propriétaire. La conception de ces services est validée par le CNRS (équipes projet et transverses).	1
URB_010	Les échanges entre la solution et le reste du SI se font via des formats pivots.	1
URB_011	Les formats pivots non fournis par le CNRS sont basés sur des formats pivots existants et reconnus par la communauté. Le choix des formats pivots est validé par le CNRS (équipes projet et transverses).	1
URB_012	Les formats pivots sont facilement évolutifs en limitant les impacts sur leurs usages déjà en cours.	1
URB_013	La description des formats pivots spécifiquement développés pour le CNRS respecte un formalisme prescrit par la DSI du CNRS.	1
URB_014	Si la mise en œuvre d'échange nécessite la transcodification de certaines données (nomenclatures par exemple), celle-ci est effectuée par les systèmes d'intermédiation au cours du flux, à partir de tables de transcodification administrées par le gestionnaire de données de référence du CNRS. Les systèmes d'intermédiations prennent seulement en compte une transcodification simple, de type valeur ou groupe de valeur vers une autre valeur, sans application de règles métier. Celles-ci sont éventuellement mises en place dans le gestionnaire de données de référence du CNRS qui héberge les tables de transcodification. A noter que si les échanges se font via les services web, ces derniers ne réalisent aucune transcodification.	2
URB_015	La solution va chercher les objets métiers, dont elle a besoin et en récupère, au moment où elle en a besoin, uniquement la population qui l'intéresse et uniquement le sous-ensemble des caractéristiques (partie du format pivot) qui lui est nécessaire. Autrement dit, seules les données / objets métiers nécessaires sont présents dans les flux entrants de la solution.	1
URB_016	En fonction des éléments d'analyse, le titulaire détermine l'ensemble des données strictement nécessaires dans le cadre de données personnelles (contrainte du règlement européen sur la protection des données – RGPD), au bon fonctionnement de la solution.	1
URB_017	L'utilisation de données extérieures à la solution n'implique pas un stockage de ces données dans la solution et est mis en balance avec le nombre, la fréquence et le volume des flux nécessaires pour consommer ces données, afin d'optimiser les ressources. Aussi, la nécessité de stocker les données externes dans la solution est étudiée et validée entre le titulaire et le CNRS (équipes projet et transverses).	1
URB_019	La solution expose toute la population des objets métier dont elle est maîtresse, avec le contenu complet du format pivot, y compris les règles de diffusion, et/ou niveau de sensibilité. Autrement dit, la solution ne fait aucune restriction sur l'exposition des objets métier qu'elle gère.	1

Référence	Libellé exigence	Priorité
URB_018	Pour chaque objet métier dont la solution est propriétaire, un service d'exposition permet au choix : ▪ une diffusion au fil de l'eau des objets métier modifiés par la solution ; ▪ une diffusion sous forme de flux à la demande ; ▪ un flux complet ou différentiel sur des critères à définir en conception détaillée (*par exemple, uniquement sur les objets modifiés depuis l'envoi précédent ou depuis une date définie, uniquement un sous ensemble des objets métier, uniquement un objet métier donné*). ▪ une sélection d'objets métier et/ou une partie de leurs caractéristiques, en fonction de critères à définir en conception détaillée. ▪ Le choix des mécanismes d'exposition à implémenter est étudié et validé entre le titulaire et le CNRS (équipes projet et transverses).	1
URB_021	Pour les objets métier dont la solution est propriétaire, et pour lesquels il y a une utilité, un service de recherche permet une recherche approchante, sur des caractéristiques à définir en conception détaillée.	2

4.1.2.2 *Modalités d'implémentation*

Les flux d'échange de données doivent techniquement adopter les règles d'implémentation suivantes :

Référence	Libellé exigence	Priorité
ECH_001	Les échanges inter-applicatifs passent par les systèmes d'intermédiation du CNRS. La solution ne communique qu'avec ces systèmes d'intermédiation, quel que soit le flux entrant ou sortant et propose des services permettant d'interagir avec eux.	1
ECH_002	La solution produit et reçoit des informations préformatées au format pivot défini par le CNRS. Les systèmes d'intermédiation ne portent pas les règles de gestion métier.	0
ECH_003	L'interfaçage avec les systèmes d'intermédiation est effectué via des services web du type REST. Pour la diffusion de ses données au reste du SI, la solution privilégie un appel à un service web CNRS de diffusion des données.	1
ECH_004	La fréquence de publication des données est faite au fil de l'eau, de façon quotidienne ou hebdomadaire.	1
ECH_005	L'encodage préconisé est UTF-8. Les formats utilisés pour les échanges de données sont XML, JSON et CSV, mais ces formats ne sont pas limitatifs. Le référentiel général d'interopérabilité (http://references.modernisation.gouv.fr/interoperabilite) gouverne le choix des formats.	1
ECH_006	Seuls des protocoles de transport de données chiffrés sont utilisés comme par exemple les protocoles « SSH » (scp, sftp, etc). Se référer au RGS 2.0 annexes B1, B2 et B3 pour les versions des protocoles et algorithmes de chiffrement autorisés (https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents).	0
ECH_007-a	Pour tous les types de flux, la confidentialité des données transmises est garantie. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_007-b	Pour tous les types de flux, l'intégrité des données transmises est garantie. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_007-c	Pour tous les types de flux, l'unicité des requêtes est garantie pour éviter les attaques par rejeux. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_007-d	Pour tous les types de flux, l'identité du client et du serveur de communication est garantie. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_008	Pour assurer la confidentialité et l'intégrité des données lors des échanges, le chiffrement des données en supplément du chiffrement des protocoles de transport (cf. ECH_006) est une mesure de protection dont l'opportunité est jugée au regard de la sensibilité. Ce chiffrement est réalisé à la source et le déchiffrement à la destination, sans possibilité d'interception par les systèmes d'intermédiation et de transport selon les normes de chiffrement en vigueur (cf. annexe B du RGS : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents). Il est cependant toléré que le système d'intermédiation du CNRS assure le chiffrement en cas d'impossibilité de le réaliser à la source.	0
ECH_009	L'authentification des appels à un service web, de type REST, est réalisée soit par certificat, soit par identifiant/mot de passe stocké de manière confidentielle.	0
ECH_010	Lorsque l'usage d'un broker est nécessaire, c'est celui du gestionnaire d'échange et de services du CNRS, via son API (JMS de préférence) qui est utilisé.	1

Référence	Libellé exigence	Priorité
SSI_COM_102	Les seuls flux entrants de production (hors flux techniques, ex. : DNS, ESB, etc.) légitimes sont les suivants : - Reverse proxy --> Serveur d'application - Serveur d'application --> Serveur de base de données	0
SSI_COM_103	Il existe une matrice de flux bilatéraux documentée et tenue à jour pour l'ensemble des serveurs et des postes clients impliqués dans la solution. Cette matrice de flux est techniquement implémentée sur des dispositifs de filtrage (pare-feux). Les flux non explicitement déclarés dans la matrice de flux sont techniquement interdits.	0
SSI_COM_104	Pour tous les types de flux, la confidentialité des données transmises est garantie par des moyens techniques décrits dans la documentation.	0
SSI_COM_105	Pour tous les types de flux, l'intégrité des données transmises est garantie par des moyens techniques décrits dans la documentation.	0
SSI_COM_106	Pour tous les types de flux, l'unicité des requêtes est garantie pour éviter les attaques par rejeu par des moyens techniques décrits dans la documentation.	0
SSI_COM_107	Pour les flux d'échange entre applications, l'identité du client et du serveur de communication est garantie par des moyens décrits dans la documentation.	0
SSI_COM_108	L'authentification des appels à un service web est réalisée par des mécanismes permettant de garantir la confidentialité des identifiants. Les moyens techniques utilisés sont décrits dans la documentation.	0
SSI_COM_109	Les flux sortants initiés depuis les serveurs de la solution sont limités au strict nécessaire. Lorsque ces flux sont établis vers une zone de sensibilité moindre (ex : SI usuel vers Internet, SI sensible vers SI usuel), ils passent obligatoirement par des serveurs mandataires spécifiques (ex : relais SMTP, DNS, NTP ou serveur mandataire HTTP). Ces serveurs assurent la rupture protocolaire et contrôlent la conformité et la destination des flux. Ils sont situés dans des zones réseaux cloisonnées et dédiées à cet usage (type DMZ). Les moyens techniques utilisés sont décrits dans la documentation. Précision : cette règle est valable quelles que soient les modalités d'hébergement et les maîtres d'œuvre.	0
SSI_COM_110	Les connexions VPN site à site sont effectuées en VPN IPSEC. Précision : se référer au RGS 2.0 annexes B1, B2 et B3 pour les versions des protocoles et algorithmes de chiffrement autorisés	0
SSI_COM_111	Les connexions VPN client à site sont effectuées en VPN IPSEC ou VPN SSL avec authentification du terminal et de l'utilisateur.	0
SSI_COM_112	L'émission de messages de type email par la solution doit être contrôlée afin d'éviter le détournement de la fonction (spam ou diffusion de contenu malveillant) : - L'émetteur doit être fixé de façon fiable sur une adresse et un nom d'expédition n'autorisant pas de réponse (« no-reply ») et identifiant clairement l'application émettrice. - La liste des destinataires doit également être maîtrisée (ex : listes pré-établies ou listes de diffusion, domaines cibles en liste blanche, nombre de destinataires limités etc.). - Le contenu des messages doit reposer sur des modèles préétablis et n'incluant pas de code pouvant être interprétés de façon détournée par les clients. A ce titre, l'envoi de messages au format « texte brut » et sans pièce jointe est à privilégier.	0

4.1.3 Authentification, comptes utilisateurs

Les services d'authentification CNRS (cf. § 2.3.3.3) sont disponibles sur plusieurs environnements :

- production : réservé à la production de la solution,
- recette : réservé à la recette de la solution,
- formation : réservé à la formation de la solution,
- test : seul environnement accessible au titulaire, ne contenant pas de données réelles et dont l'objectif est de permettre au titulaire de valider les aspects techniques liés aux briques d'authentification.

Le titulaire assure les développements applicatifs nécessaires pour s'interfacer avec le(s) fournisseur(s) d'identité du CNRS (cf. § 2.3.3.3). Si plusieurs fournisseurs peuvent être choisis, un WAYF doit être mis en place.

Pour les applications hébergées sur les infrastructures propres de la DSI du CNRS, le CNRS peut mettre en place un service intégré de service provider (SP) SAML 2.0 et de WAYF, de technologie Shibboleth[3].

Le titulaire reste responsable de la solution mise en œuvre qui doit respecter les principes de fonctionnement suivants :

- L'application délègue l'authentification des utilisateurs aux services d'authentification du CNRS (cf. § 2.3.3.3).
- Une fois le client SAML intégré à l'application, ce sont les fournisseurs d'identité qui se chargent d'authentifier l'utilisateur CNRS.
- L'authentification des utilisateurs par les services d'authentification CNRS est possible soit par certificats (AC CNRS / TCS), soit par email/mot de passe (en se basant sur les informations contenues dans le référentiel des comptes utilisateurs du CNRS), soit avec une solution d'authentification multi-facteurs.
- Le navigateur est toujours redirigé vers un des fournisseurs d'identité CNRS et c'est ensuite, lors de l'authentification sur ce fournisseur d'identité, que l'utilisateur peut fournir ses identifiants et authentifiants.
- Une fois l'utilisateur authentifié auprès d'un fournisseur d'identité CNRS, le navigateur de l'utilisateur envoie à l'application l'identifiant opaque dans un jeton de réponse SAML. Ce jeton contient aussi des attributs de l'utilisateur authentifié. La liste des attributs diffusés est spécifique à chaque application et limitée à ses besoins.
- Le contrôle d'accès à l'application effectué par le fournisseur d'identité CNRS se limite à dire si les informations d'authentification de l'utilisateur sont correctes. Il atteste juste que l'utilisateur est référencé dans le SI du CNRS. L'application doit assurer elle-même son contrôle d'accès à partir des rôles et droits applicatifs gérés dans l'application. Si nécessaire, les droits et profils applicatifs associés sont stockés dans la base de l'application.
- Le service provider (SP) fourni par la DSI du CNRS peut restreindre l'accès à l'application sur la base d'attributs retournés par le fournisseur d'identité.
- Le critère d'accès est donc l'appartenance ou non de l'utilisateur au référentiel des comptes utilisateurs du CNRS.
- Dans le cas d'une gestion des droits déléguée à la brique de gestion des accès et habilitations du CNRS (cf. § 2.3.3.4), les rôles applicatifs peuvent être gérés et calculés de manière centralisée. Ces rôles applicatifs sont disponibles dans les services web des données des utilisateurs. Dans certains cas ils peuvent aussi être transmis à l'application lors de l'authentification. Les droits fins sont stockés et gérés dans la solution.

Référence	Libellé exigence	Priorité
AUTH_001-a	L'authentification à la solution se fait à partir du fournisseur d'identité CNRS pour les utilisateurs des unités CNRS et sinon au moyen de la fédération RENATER.	1
AUTH_001-b	Pour les utilisateurs qui ne sont présents ni dans le fournisseur d'identité CNRS, ni dans la fédération RENATER, le CNRS étudie les modalités de gestion des comptes. L'utilisation de comptes locaux n'est possible que sur autorisation expresse du CNRS.	1
AUTH_002-a	Dans le cas de comptes locaux, la solution comprend des fonctionnalités de gestion de ces comptes.	0
AUTH_002-b	Dans le cas de comptes locaux, les mots de passe ne sont jamais stockés en clair mais dans une forme transformée par une fonction cryptographique non réversible conforme au Référentiel Général de Sécurité (https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs) et la transformation des mots de passe fait intervenir un sel aléatoire.	0
AUTH_003	Un service de découverte (WAYF) est mis en place lorsque le fournisseur d'identités CNRS n'est pas le seul fournisseur d'identité utilisé.	0
AUTH_004	La création d'un compte utilisateur pour accéder à la solution est effectuée par un mécanisme de provisioning et non par saisie manuelle. Le provisioning peut être effectué via l'utilisation du service web qui expose le référentiel des comptes utilisateurs (annuaire référentiel du CNRS), à la demande ou au fil de l'eau ou encore via les informations issues de l'authentification. La création automatique de compte sur demande de l'utilisateur directement dans l'application est interdite.	1
AUTH_005	Pour les personnels présents dans les unités du CNRS, l'origine des données pour la création et la modification des comptes utilisateurs est l'annuaire référentiel du CNRS.	0
AUTH_006	Un mécanisme de gestion du cycle de vie des comptes utilisateurs de la solution est mis en place.	1
AUTH_007	La modification d'un compte utilisateur dans la solution est effectuée via des services web ou via les systèmes d'intermédiation du CNRS.	1
AUTH_008	Les phases d'identification et d'authentification sont séparées de l'ensemble des actions applicatives de l'utilisateur dès la conception de la solution afin de permettre la plus grande modularité possible, et donc une facilité, quant au choix du mécanisme d'identification et d'authentification.	1

[3] Cf. définition dans le glossaire (cf. § 6.4.2)

Référence	Libellé exigence	Priorité
AUTH_009	Le contrôle d'accès à l'application est renforcé directement sur le reverse proxy hébergeant le Service Provider par la vérification d'un attribut spécifique exposé par le référentiel des comptes pour refuser l'accès aux utilisateurs authentifiés qui n'auraient pas de droits sur l'application. Dans ce cas, une page d'erreur spécifique est à prévoir pour indiquer de manière claire à l'utilisateur qu'il n'a pas les droits nécessaires pour accéder au service/à l'application. Ce contrôle s'ajoute mais ne se substitue pas aux contrôles de droits des utilisateurs réalisés par l'application.	1
SSI_AUTH_101	Lorsque la population utilisatrice est fédérée au sein du fournisseur d'identité CNRS (cas des utilisateurs des unités) ou de la fédération RENATER, la solution s'appuie sur ces services d'authentification pour l'authentification des utilisateurs.	0
SSI_AUTH_102	Lorsque la population utilisatrice n'est ni fédérée au sein du fournisseur d'identité CNRS (cas des utilisateurs des unités), ni de la fédération RENATER, les modalités de gestion des comptes permettent de garantir à tout moment : - la confidentialité des moyens d'authentification, - que seules les personnes légitimes disposent des accès. La gestion des comptes locaux lorsqu'elle est incontournable, est explicitement autorisée et documentée.	0
SSI_AUTH_103	Dans le cas de comptes locaux, les mots de passe ne sont jamais stockés en clair mais dans une forme transformée par une fonction cryptographique non réversible et la transformation des mots de passe fait intervenir un sel aléatoire. Précisions : se référer au RGS 2.0 annexes B1, B2 et B3 pour les fonctions cryptographiques conformes.	0
SSI_AUTH_104	La création d'un compte utilisateur, hormis pour les fonctionnalités de type téléservice, pour accéder à la solution est effectuée par un mécanisme de provisioning (et non par saisie manuelle ou par création automatique sur demande de l'utilisateur directement dans la solution). Dans le cas de téléservice, la création automatique de compte à l'initiative de l'utilisateur est étudiée et validée entre le titulaire et le CNRS Précisions : le provisioning peut être effectué via l'utilisation du service web qui expose le référentiel des comptes utilisateurs (annuaire référentiel du CNRS), à la demande ou au fil de l'eau ou via les informations issues de l'authentification.	1
SSI_AUTH_105	Un mécanisme de gestion du cycle de vie des comptes utilisateurs de la solution est mis en place (y compris pour les comptes locaux le cas échéant). Précision : la gestion du cycle de vie inclut, entre autres, des mécanismes outillés d'ajout, de suppression, et de suspension de comptes et la possibilité de gestion d'une durée de vie pour les comptes	0
SSI_AUTH_106	La solution permet de définir différents rôles applicatifs selon les fonctions métier et les responsabilités des utilisateurs. Ces rôles applicatifs sont limités au strict nécessaire en application du principe du moindre privilège.	0
SSI_AUTH_107	Lorsque des comptes par défaut existent, la solution permet de les désactiver, les renommer, modifier le mot de passe ou les supprimer sans impact sur le service fourni.	0
SSI_AUTH_108	Les privilèges accordés aux comptes de service utilisés par la solution sont limités au strict nécessaire en application du principe du moindre privilège. Précision : il s'agit des comptes d'accès aux bases de données, au système de fichiers, etc.	0
SSI_AUTH_109	Des comptes d'administration dédiés (différents des comptes utilisateurs affectés aux personnels administrateurs techniques) sont les seuls utilisés pour réaliser les actions d'administration technique ou pour effectuer des diagnostics techniques.	0
SSI_AUTH_110	L'administration technique de la solution passe par un bastion d'administration assurant la traçabilité des actions.	0

Référence	Libellé exigence	Priorité
HAB_001	La solution permet de définir différents rôles applicatifs selon les fonctions métier et les responsabilités des utilisateurs.	0
HAB_002	La solution permet de définir des rôles applicatifs en fonction des fonctions métier et du domaine d'appartenance, ainsi que des accès associés (lecture, écriture, etc.). Ces rôles sont associés à des périmètres correspondant au besoin et/ou au droit d'en connaître pour les populations considérées.	1
HAB_003	La solution permet de définir ou provisionner des comptes d'accès permanents et temporaires (définition d'une date de début et une date de fin de la validité du compte).	1
HAB_004	La solution permet la désactivation des comptes utilisateurs.	0
HAB_005	Lorsque des comptes par défaut existent, il est possible de les désactiver, les renommer, modifier le mot de passe ou les supprimer sans impact sur l'application.	1

4.1.4 Stockage des documents

Référence	Libellé exigence	Priorité
DOC_005	Les documents gérés par la solution sont stockés sur la plateforme de GED du CNRS. Dès lors, les fonctionnalités d'ajout/modification/lecture/suppression de documents invoquées depuis la solution sont réalisées à travers des services web proposés par la GED du CNRS par l'intermédiaire des systèmes d'intermédiation.	1

4.2 EXIGENCES TECHNIQUES

4.2.1 Eléments techniques structurants

Les applications PDAP, WorkCycle, DMF Consult et PD Web sont des applications ouvertes sur Internet.

La solution DMF est ouverte à environ 3500 utilisateurs authentifiés.

On estime les fréquentations des applications à :

- 1500 utilisateurs par jour pour PD Web
- 500 utilisateurs par jour pour DMF Consult

Il n'y a pas de fonctionnement par campagne.

4.2.2 Services d'infrastructure

4.2.2.1 *Architecture générale*

La solution est construite sur une architecture logicielle intégrée, c'est-à-dire :

- s'appuyant sur une gestion des données unique,
- s'appuyant sur des mécanismes d'accès, d'authentification et de gestion de la confidentialité proposant une ergonomie homogène pour l'ensemble des fonctionnalités,
- disposant d'un outillage d'administration dédié.

Référence	Libellé exigence	Priorité
INF_001	Partout où cela est possible, les privilèges accordés aux comptes de service utilisés par la solution sont minimisés au strict nécessaire. *Exemple : accès BDD, accès au système de fichiers, …*	0
INF_002	L'exploitation et l'administration « fonctionnelle » de la solution est réalisée par une IHM spécifique, si possible dédiée, avec des comptes nominatifs dédiés. Elle ne nécessite pas de connexions en SSH ou d'actions nécessitant une console (*ex : récupération de logs récurrente, édition de fichiers de paramétrage pour lancer une campagne, etc*.).	0
INF_003	La solution ne peut pas être proposée en mode SaaS.	0

4.2.2.2 *Caractéristiques système*

Les exigences système suivantes doivent être respectées :

Référence	Libellé exigence	Priorité
INF_004	Le serveur HTTP de référence est Apache sur Linux. L'autre plateforme acceptée est la solution IIS sous Windows.	0
INF_005	Dans le cas où la solution nécessite un serveur d'application Java préinstallé, la référence est Tomcat. Une autre solution peut être acceptée sur dérogation.	1
INF_006	Le système d'exploitation serveur de référence est Red Hat Enterprise Linux, le système d'exploitation Windows serveur est toléré.	0
INF_007	La configuration d'un serveur PHP exécute uniquement les modules nécessaires à la solution, qui sont les seuls actifs. Cette liste est définie et communiquée par le titulaire. Certains modules sont explicitement interdits (notamment ceux permettant un appel direct au système d'exploitation). Certaines fonctions sont interdites : disable_functions = system, exec, shell_exec, passthru, phpinfo, show_source, highlight_file, popen, proc_open, fopen_with_path, dbmopen, dbase_open, putenv, move_uploaded_file, chdir, mkdir, rmdir, chmod, rename, filepro, filepro_rowcount, filepro_retrieve, posix_mkfifo.	0
INF_008	Toutes les montées de versions mineures pour les OS serveurs (de type Linux), les modules serveurs applicatifs et bases de données, sont effectuées avec un déclenchement automatique, pour tout ce qui a été installé par le gestionnaire de paquets.	0

De plus, le titulaire a pris en compte dans son offre les exigences sur la sécurité des applications définies au chapitre 4.4.

4.2.2.3 *Caractéristiques réseau*

La solution mise en œuvre s'appuie impérativement sur l'infrastructure réseau existante et intègre les aspects suivants :

- tous les échanges sont compatibles avec les protocoles IPv4 et IPv6 ;
- tous les flux du système d'information sont recensés et maîtrisables, en terme de capacité à appréhender le mode de fonctionnement protocolaire associé, et à assurer le filtrage par des équipements de type « pare-feu » ; le titulaire fournit une matrice des flux de l'application, indiquant clairement les protocoles, ports et sens de communication utilisés par ces flux ;
- le serveur applicatif n'est pas directement visible des navigateurs clients, des éléments de type « reverse-proxy » étant intercalés dans le flux (Navigateur ⇦ [HTTPS] ⇨ Reverse Proxy ⇦ [HTTP] ⇨ Serveur applicatif) ;
- le fonctionnement de l'application intègre la mise en œuvre de composantes techniques souvent déployées dont notamment les réseaux privés virtuels (VLAN), la translation d'adresses IP (NAT), l'utilisation de serveurs de type Reverse Proxy, les « pares-feux », le chiffrement (via une technologie de type VPN ou autre) ;
- la solution est parfaitement inter opérante avec les principaux services Internet (DNS, SMTP, FTP, NTP, SNMP, etc.), dans leurs versions chiffrées quand elles existent. Elle respecte en particulier les principaux RFC associés à chacun des protocoles, et les règles en usage dans la communauté Internet.

Référence	Libellé exigence	Priorité
INF_009	Les flux entre les postes clients et le(s) serveur(s) applicatif(s) passent par une DMZ avec rupture de flux effectuée par des reverse proxy.	1
INF_010	Les seuls flux « réseau » (hors flux techniques comme "DNS", "EAI", …) légitimes sont les suivants : ▪ reverse proxy → serveur d'application ▪ serveur d'application → serveur de base de données	1
INF_011	Les flux entrants de systèmes externes sont soumis à autorisation de la sécurité. Dans le cas où ils sont autorisés, ils passent par des services en DMZ.	0
INF_012	Les flux sortants sont chiffrés conformément aux dispositions réglementaires (cf. RGS Annexe B1, B2, B3 https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents), passent un proxy HTTP et sont initiés par le CNRS.	1
INF_013	La compatibilité IPv6 est assurée de façon native. En production, les communications se font en IPv4 sauf décision expresse du CNRS.	2
INF_014	Les connexions VPN sont obligatoirement effectuées en site à site IPSEC IKEv2, le roaming user SSL avec chiffrement au niveau règlementaire requis est toléré avec identification du terminal et de l'utilisateur	0

Référence	Libellé exigence	Priorité
INF_015	Un filtrage protocolaire L4 au minimum est mis en service sur les systèmes d'exploitation, s'appuyant sur une matrice de flux documentée, permettant de limiter au strict nécessaire : ▪ les ports d'écoute ▪ les sources pouvant joindre chaque port (*exemple : un port d'écoute destiné à un échange inter applicatif n'est joignable que par l'autre pair de communication*) ▪ les destinations légitimes lorsqu'il s'agit de flux sortants. Par défaut, un serveur n'initie pas de trafic réseau, en dehors du trafic nécessaire à sa mise à jour. Le titulaire fournit la matrice des flux en tant que livrable.	0
INF_016	L'administration de la solution est compatible avec des solutions d'administration de type bastion.	0
INF_017	La prise de main depuis l'extérieur passe par un VPN puis un bastion.	0

4.2.2.4 *Exploitabilité de la solution*

L'application doit être techniquement paramétrable à souhait, et elle doit être facilement exploitable par les équipes qui la maintiennent en condition opérationnelle. En particulier, les exigences suivantes sont à respecter par l'application :

Référence	Libellé exigence	Priorité
INF_018	Les solutions applicatives permettant d'assurer la continuité d'activité (*ex. serveurs d'application redondants*) sont nécessaires lorsque le besoin est confirmé par les besoins de continuité de la solution. Dans ce cas, la scalabilité du service peut se faire par l'ajout de nœud(s) sur les différentes couches (tiers) de la solution (hors base de données).	0
INF_019	L'hébergement en production bénéficie d'une politique de sauvegarde définie en fonction des besoins de reprise d'activité de la solution. Les sauvegardes sont déportées pour être suffisamment isolées du site de production.	0
INF_020	Les technologies à base de containers (de type Docker) ne sont pas préconisées tant que le CNRS ne s'est pas doté de l'outillage adapté.	1
INF_021	L'application est compatible avec un environnement d'exécution durci selon les règles définies par le CNRS, ces règles sont issues des profils SCAP d'une version 1.3 ou supérieure publiés par le NIST pour les systèmes d'exploitation.	1
SSI_EXP_101	La prise de main à distance d'un actif quelconque de la solution (serveur, actif réseau, poste de travail…) depuis l'extérieur passe par un VPN puis un bastion.	0
SSI_EXP_102	Les ressources (matériels - inclut les solutions appliances, les équipements réseau, systèmes - inclus les OS, les firmwares et les hyperviseurs, middlewares et applications, etc.) composant la solution génèrent des traces relatives aux activités de connexion, aux requêtes, aux actions et événements importants relatifs à la solution, quelle que soit la source (utilisateur, administrateur, scripts ou processus particulier), au niveau de détail requis par la réglementation.	0
SSI_EXP_103	Les traces générées par la solution sont dans un format structuré dont les champs couvrent a minima : - l'adresse IP ou la source à l'origine (en cas d'interaction distante) - le compte utilisateur ou processus associé - le libellé intelligible de l'évènement ou l'action - le code retour de l'action le cas échéant - un identifiant unique de corrélation le cas échéant - la taille de la requête le cas échéant	0
SSI_EXP_104	Les traces générées par la solution sont horodatées de manière fiable et synchronisées sur une même source de temps en indiquant notamment le fuseau horaire si les traces ne sont pas établies en heure UTC.	0
SSI_EXP_105	Les traces produites par la solution sont exportées dès leur génération hors du système générateur, de manière fiable et intègre vers un système central de collecte.	0
SSI_EXP_106	Toutes les montées de versions mineures pour les OS serveurs, les modules serveurs applicatifs et bases de données, sont effectuées avec un déclenchement automatique, pour tout ce qui a été installé par le gestionnaire de paquets.	0

Référence	Libellé exigence	Priorité
SSI_EXP_107	Les ressources matérielles et logicielles composant la solution sont intégrées dans un processus de veille en vulnérabilités et correctifs pendant la durée de vie de la solution. Précision : cette exigence porte sur l'existence d'un processus de veille en vulnérabilités. Pour être conforme à l'exigence, le processus de gestion de vulnérabilité est connu, documenté et appliqué.	0
SSI_EXP_108	Des moyens d'administration dédiés sont utilisés pour réaliser les actions d'administration technique ou pour effectuer des diagnostics techniques. Précision : les moyens d'administration incluent les postes d'administration et leur environnement (VLAN, etc.)	0
SSI_EXP_109	Les configurations des matériels (inclus les solutions appliances les équipements réseau) et des systèmes (inclus les OS, les firmwares et les hyperviseurs) embarqués dans la solution sont durcies.	1
SSI_INF_101	Les sauvegardes sont déportées pour être suffisamment isolées du site de production.	0
SSI_INF_102	Les sauvegardes font l'objet de dispositions de protection physiques et logiques permettant d'assurer le même niveau de disponibilité, de confidentialité et d'intégrité que l'environnement de production.	0

4.2.2.5 *Caractéristiques d'observabilité*

Le CNRS effectue la supervision de ses applications en collectant les informations suivantes :

- métriques techniques du système d'exploitation et composants,
- logs des composants de bas niveau (système d'exploitation, base de données, serveur web, …),
- logs applicatifs issus de fichiers de logs fournis par l'application avec un format facilitant leur analyse.

4.2.3 Architecture applicative

4.2.3.1 *Normes d'architecture*

Les exigences et recommandations techniques concernant l'architecture applicative sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_001	L'architecture sépare bien les aspects essentiels de la solution (présentation, aspects métiers, accès aux données) afin de faciliter la testabilité et l'extensibilité de la solution. Une attention particulière est portée à l'abstraction de la base de données, afin de permettre la mise en place de l'intégration continue du code et faciliter les éventuels changements de base de données.	0
DEV_002	La haute disponibilité est mise en place pour les solutions identifiées comme ayant le besoin de disponibilité attendu le plus élevé.	0
DEV_003	L'architecture est de type client léger, les clients lourds ou riches basés sur des technologies de plugins dans les navigateurs (tels que les applets, Flash, ActiveX, ...) sont interdits. Tous les traitements et vérifications sont réalisés au moins du côté serveur : aucune entrée cliente n'est considérée comme fiable par défaut.	0
DEV_004	L'usage de Java WebStart est temporairement toléré lorsqu'il n'existe aucune alternative (par exemple si besoin de signature numérique)	1
DEV_005	Il est interdit de déployer sur les postes de travail des logiciels créant des adhérences autres que le navigateur, en dehors de certaines exceptions à justifier.	1
DEV_006	La solution est utilisable à partir d'un navigateur Web sur un protocole de transport TLS aussi bien pour les solutions à visibilité internet que les solutions internes. Le CNRS impose les technologies Web natives (HTML5, CSS3…) limitant les interactions avec le système d'exploitation et le respect des standards du W3C.	1
DEV_007	L'architecture n'est pas monoposte.	0
DEV_008	En plus du français, la gestion d'au moins une langue étrangère (l'anglais) est fournie.	1
DEV_009	Les libellés (messages d'erreur, champs, texte, ...) sont externalisés, soit en base soit via un fichier de propriétés. *Par exemple, les nomenclatures ne sont pas stockées dans le code applicatif mais sont externalisées.*	1

Référence	Libellé exigence	Priorité
DEV_010	Toute émission de mails respecte les règles suivantes : 1. L'expéditeur (« from » de l'entête ET de l'enveloppe) utilise un sous-domaine de cnrs.fr dédié à l'application (ex : @monappli.cnrs.fr). 2. L'application utilise le relai SMTP local du serveur pour l'envoi des mails, soit de manière implicite, soit en spécifiant l'usage du relai localhost « 127.0.0.1:25 » si nécessaire. Ce relai local acheminera alors les mails vers les relais centralisés qui assureront l'émission externe, en cohérence avec le SPF du domaine d'émission. 3. Le domaine de sortie est choisi parmi ceux autorisés par les relais de la DSI 4. La solution n'utilise pas l'adresse mail des utilisateurs pour les domaines non gérés par la DSI comme clause FROM, sous peine d'usurpation d'identité et blacklistage (par exemple, il est interdit d'envoyer des mails de type john.doe@google.com) 5. Le nombre maximum de mails envoyés par unité de temps est paramétrable au niveau de l'application	0
SSI_PCA_103	Les mécanismes de redondance et de haute disponibilité sont mis en œuvre sur les ressources de la solution le nécessitant pour répondre au besoin de disponibilité et de continuité de service de la solution.	0

4.2.3.2 *Langages*

Les exigences et recommandations techniques concernant les langages utilisés sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_011	L'ensemble des langages et des composants nécessaires à la solution sont utilisés dans les versions mentionnées dans le document CCT_Versions-cibles (ce document est mis à jour régulièrement). Le document, dans sa version courante est applicable à tout moment, ce qui implique des mises à jour régulières des applicatifs en conséquence. L'utilisation de langages ou composants non mentionnés dans le document CCT_Versions-cibles doit être validé en amont par le CNRS.	1
DEV_012	Sauf contrainte contractuelle, le choix du langage et des frameworks est le résultat d'un consensus entre la DSI et le titulaire en charge de la réalisation de la solution.	0
DEV_013	Les frameworks de développement sont ouverts, éprouvés, avec une large communauté active, maîtrisés par le titulaire en charge de la réalisation de la solution, et permettent d'automatiser les tests unitaires. Leur choix est justifié en regard des gains attendus en termes de développement et d'évolutivité. Les versions utilisées sont systématiquement celles qui sont les plus récentes et qui présentent la durée de support la plus longue.	1
DEV_014	Pour une solution Java, le framework utilisé est Spring Boot avec le serveur web embarqué (la solution ne requiert donc pas d'être installée dans un conteneur de servlets).	1
DEV_015	Pour une solution PHP, le framework utilisé est Symfony.	1
DEV_016	Le nombre de composants externes complémentaires est limité au strict minimum. L'utilisation de composants externes, progiciels, logiciels tiers respecte les règles suivantes : 1. Son fournisseur est engagé sur le maintien dans la durée d'une réelle API de communication 2. Les évolutions de la solution peuvent être menées sans avoir systématiquement recours à des consultants experts de ces composants tiers. 3. Les développements spécifiques n'ont pas d'impact sur les montées de version, ou bien ces impacts sont intégrés comme un coût additionnel en début de projet 4. Le code tiers utilisé dispose d'une licence d'utilisation bien identifiée, n'induisant pas pour le CNRS de contraintes d'acquisition ou d'aliénation de ses droits. Les licences libres sont recommandées.	0

4.2.3.3 *Normes de développement*

En fonction de la technologie retenue, des préconisations concernant les méthodologies et règles de développement sont applicables et s'appliquent notamment pour le code spécifique développé pour le CNRS.

Les recommandations ci-après s'appliquent de manière plus générale à l'ensemble des technologies.

Le CNRS est attentif à la qualité logicielle de l'application et à ses capacités d'évolution.

D'une manière générale, le titulaire doit utiliser autant que possible des standards pérennes normalisés ou reconnus du marché.

Les exigences et recommandations techniques concernant les normes de développement sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_017	Les développements sont modulaires afin de faciliter la maintenance et l'évolutivité du code.	0
DEV_018	Les erreurs sont traitées de manière à assurer la sécurité dans les développements (toutes les erreurs levées lors de l'exécution sont traitées en conséquence).	0
DEV_019	Les librairies de logs utilisées sont ouvertes, éprouvées, avec une large communauté active, et maîtrisées par le titulaire. Les logs sont paramétrables et gèrent à minima les niveaux suivants : ▪ ERROR : une erreur technique non récupérable est survenue dans la solution ; en général, la solution n'est plus opérationnelle ensuite ▪ WARN : un point d'attention a été soulevé, ou une erreur récupérable est survenue ▪ INFO : permet de suivre le fonctionnement métier de l'application, plus les étapes importantes de la vie de l'application ▪ DEBUG : permet de voir le fonctionnement technique de la solution.	0
DEV_020-a	La solution journalise des événements permettant l'audit des connexions effectuées à la solution, et le suivi des opérations importantes. Les opérations à tracer ainsi que le format du contenu de ces journaux sont définis conjointement entre le titulaire et le CNRS. Les logs issus de l'application sont dans des fichiers textes dans un format permettant leur analyse.	0
DEV_020-b	L'application utilise une librairie de logs qui permet de paramétrer la destination des événements de logs (par exemple syslog).	0
DEV_022	La solution ne récupère pas de code externe (en dehors de sa phase de construction), sauf si la dépendance a été définie explicitement, intégralement et statiquement dans son code.	0
DEV_023	Le paramétrage technique de la solution est réalisé au travers de fichiers de configurations qui sont stockés de manière indépendante du code applicatif.	0
DEV_024	Afin de lutter contre les risques d'injection de code, les requêtes SQL adressées à la base de données sont faites au moyen de requêtes préparées fortement typées ou par l'intermédiaire d'une couche d'abstraction assurant le contrôle des paramètres.	0
DEV_025	Les tests unitaires sont automatisés, avec un taux de couverture minimum défini d'un commun accord entre tous les acteurs du projet. Ces tests s'exécutent sans erreur dans la forge du CNRS (les cas d'erreurs résiduels seront justifiés par le titulaire).	0
DEV_026	Des frameworks sont utilisés pour développer les tests unitaires, dans les versions mentionnées dans le document CCT_Versions-cibles (ce document est mis à jour régulièrement). Les tests unitaires livrés en même temps que les fonctionnalités couvertes servent aux tests de non régression et peuvent fournir à travers des outils de couverture de tests un indicateur de qualité.	1
DEV_027	Les codes sont documentés et lisibles. Les composants (modules, classes, méthodes) reposent sur une nomenclature de nommage normalisée et cohérente.	0
DEV_028	Pour les langages supportant les packages ou modules, les éléments de code source doivent être organisés avec le préfixe « fr.cnrs »	0
DEV_029	Au niveau OS, le jeu de caractères pour la solution est UTF-8.	1
DEV_030	Les solutions sont compatibles avec la liste des navigateurs/OS et versions associées dans le document CCT-Versions-cibles (ce document est mis à jour régulièrement). La notion de support d'une plate-forme cliente impose que l'ensemble des fonctionnalités attendues soit disponible dans des conditions de complétude, d'ergonomie et de performance tout à fait normales. Les niveaux de prises en charge possibles sont les suivants : ▪ Maximal : Les navigateurs dans cette catégorie offrent aux visiteurs toutes les performances techniques, visuelles et fonctionnelles définies par le cahier des charges et la maquette graphique, ▪ Dégradé : Les navigateurs permettent une expérience utilisateur équivalente au niveau précédent mais qui peut toutefois présenter des différences considérées comme négligeables (décalages minimes, arrondis, ombrages...), ▪ Minimal : L'intégration HTML/CSS est accessible et agencée convenablement, mais aucun effort n'est porté sur la compatibilité visuelle avec les niveaux précédents.	0
DEV_031	L'utilisation de Javascript est autorisée notamment pour fluidifier les échanges avec la solution, *par exemple en effectuant des contrôles côté client.* Cependant, ces contrôles côté client ne se substituent pas aux contrôles côté serveur qu'il faut impérativement réaliser.	0
DEV_032	Il est interdit de construire un framework Javascript.	0
DEV_033	L'architecture de services web recommandée est l'architecture de type REST.	1

Référence	Libellé exigence	Priorité
DEV_034	Le CNRS n'impose pas d'outil de génération de PDF particulier dans la mesure où l'outil choisi est ouvert, éprouvé, avec une large communauté active, et maîtrisé par le titulaire.	0
DEV_035	Les outils de requêtage mis à disposition sont paramétrés de manière à limiter les risques de dégradation des performances de la plate-forme en cas d'utilisation malavisée par certains utilisateurs. Les outils de requêtage garantissent le respect des droits d'accès de l'utilisateur.	0
DEV_036	Les éléments d'architecture critiques, complexes ou difficiles à appréhender font l'objet de paragraphes spécifiques dans la documentation permettant leur bonne compréhension.	0
DEV_037	Les dossiers d'architecture technique, spécifications techniques détaillées (STD) ainsi que les manuels d'exploitation (MEX) et d'installation (MINS) sont actualisés par le titulaire autant que de besoin. Ils sont réputés être à jour à tout moment.	0
DEV_038	La gestion des types d'environnements (développement, recette, production, ...) est prise en charge dans la solution pour adapter automatiquement le niveau de fonctionnalité de la solution (*exemple : activation du debug, paramétrages d'envoi de mails, etc.*). Les propriétés de l'environnement sont renseignées sur l'instance déployée et facilement modifiables (*exemple : fichier unique à modifier au moment du déploiement*)	2
DEV_039	L'ensemble des éléments du bandeau, l'ensemble des couleurs, des polices de caractères, des espaces, filets, comportements au passage de la souris, aplats couleurs, paramétrages de tableaux, gestion des menus et onglets, sont gérés par une feuille de style CSS (pas de code couleur ni de mise en page en dur dans le code de la page).	1
DEV_040	Éviter au maximum l'utilisation de tables pour gérer la mise en forme dans le code HTML.	2
DEV_041	Les configurations des systèmes et des logiciels utilisés par la solution (notamment Java, PHP) sont obligatoirement durcies à l'état de l'art (cf. https://cyber.gouv.fr/publications/securiser-un-site-web), afin de limiter la surface d'attaque et la fuite d'informations par trop grande verbosité. On citera en particulier et sans exhaustivité : ▪ la suppression des balises « meta » dans l'entête HTML lorsque celles-ci indiquent le logiciel ayant généré la page ; ▪ la suppression des éléments visibles sur la page indiquant les outils (CMS, éditeur, etc.) utilisés ; ▪ la limitation en production des informations de débogage dans les messages d'erreur (en évitant par exemple de fournir la requête SQL qui a généré une erreur) ; ▪ l'utilisation de pages d'erreurs personnalisées pour ne pas reposer sur les pages par défaut facilement reconnaissables ; ▪ dans certains cas, l'utilisation de l'erreur 404 générique plutôt que d'une erreur 401, 403, 405, etc. pour éviter de révéler trop d'informations sur le fonctionnement ou le contenu en accès limité du site ; ▪ la banalisation des entêtes HTTP qui peuvent fournir des informations de version trop précises sur le serveur ou le système d'exploitation employés ; ▪ le rejet, en production, des requêtes HTTP TRACE qui n'ont d'intérêt qu'en phase de débogage.	0

4.2.3.4 *Outillage de développement*

Le CNRS opère une forge logicielle afin de favoriser la qualité logicielle, la réduction de la dette technique et l'intégration continue.

Cette forge est composée des éléments suivants :

- un service de gestion de configuration et de dépôt interne : Gitlab
- un service d'intégration continue : Gitlab CI et Gitlab runners
- un analyseur de code : Sonar
- un gestionnaire d'artéfacts : Artifactory

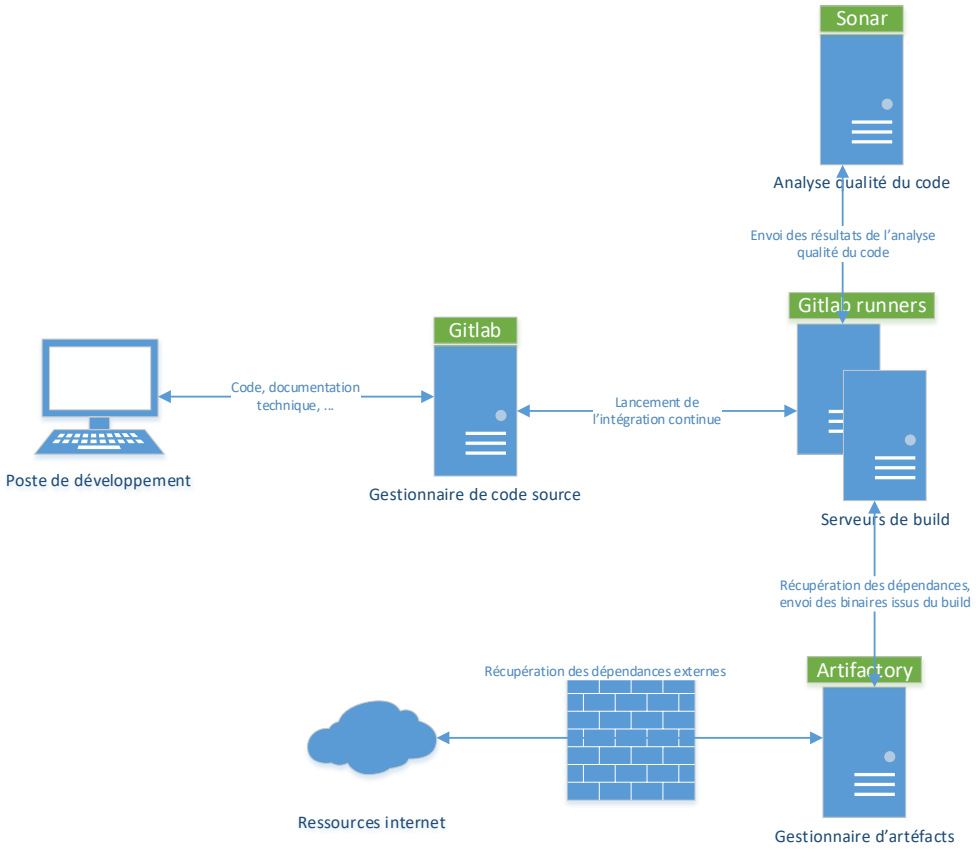


Figure 7 : Présentation de la forge logicielle

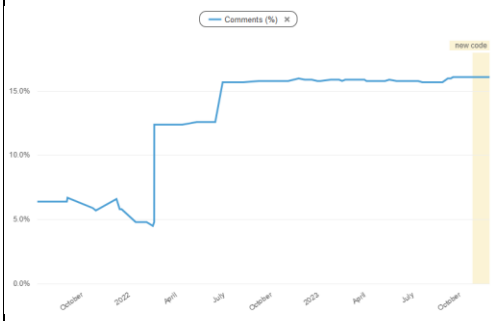
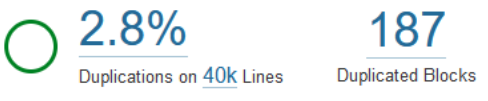
Le titulaire peut utiliser la forge de développement de la DSI du CNRS dans l'objectif d'améliorer la qualité.

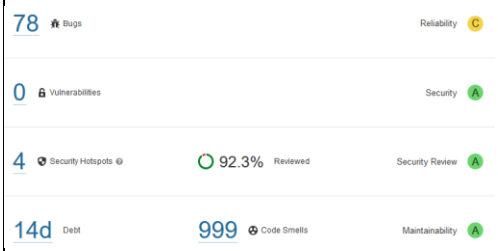
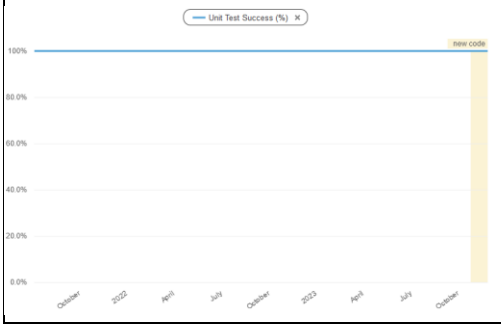
Le CNRS utilise les outils Ansible et Tower pour automatiser autant que possible le déploiement de ses applications.

L'outil de vérification de la qualité du code utilisé à la DSI est SonarQube (https://www.sonarsource.com/products/sonarqube/).

Au démarrage de l'accord-cadre, les équipes CNRS et titulaire se mettent d'accord sur le profil SonarQube à utiliser afin d'évaluer la qualité du code source.

Les métriques particulièrement suivies par le CNRS sont les suivantes :

Métrique SonarQube	Description métrique	Cible CNRS
	Taux de commentaires	*N/A*
	Duplication de code	*N/A*

Métrique SonarQube	Description métrique	Cible CNRS
	Respect des règles de codage, problèmes potentiels de sécurité	Pas d'anomalies de niveau « blocker et « critical ». Analyser les majeures. Pas de vulnérabilités.
	La couverture de tests unitaires (pourcentage de lignes de code du projet qui est appelé pendant la phase de test)	Supérieur à 50%
	Le taux de succès des tests unitaires	égal à 100%

Le niveau de conformité à atteindre fait l'objet d'une concertation entre le titulaire et le CNRS.

Plus que l'atteinte de seuils définis, le CNRS est attentif à l'évolution des métriques au cours du temps (lors de chaque livraison majeure de l'application).

Les exigences concernant les outils de développement du titulaire sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_042	Le CNRS n'impose pas de contrainte sur l'outil de développement intégré (IDE) dans la mesure où l'outil choisi est maîtrisé par le titulaire.	2
DEV_043	Pour les cas qui nécessitent des interactions avec des éléments externes (tests, environnement d'intégration ou de recette, ...), des mocks/bouchons sont utilisés. L'usage de librairies de mocks est possible. Le CNRS n'impose pas d'outil particulier dans la mesure où celui choisi est ouvert, éprouvé, avec une large communauté active, et maîtrisé par le titulaire.	0
DEV_044	JMeter est l'outil préconisé pour les tests de charge, si un autre outil est proposé il est ouvert, éprouvé, avec une large communauté active, et maîtrisé par l'équipe en charge de son utilisation.	1
DEV_045	Un moteur de production est utilisé afin de gérer les dépendances de la solution, le lancement des tests automatisés, sa construction, la publication des artéfacts sur un gestionnaire d'artéfacts, … Pour les projets Java, Maven est utilisé. Pour les projets PHP sous Symfony, Composer est utilisé.	1
DEV_046	Le nommage des artéfacts générés par la phase de construction de la solution suit les normes de nommage standard (*par exemple Maven pour les projets Java, Composer pour les projets PHP*).	1
DEV_047	Le gestionnaire de source Git est utilisé pour la gestion des codes sources. Le CNRS dispose d'un outil de gestion de code source Gitlab dans lequel se trouve le code source de la solution (soit en posant les commits directement dans le Gitlab du CNRS, soit avec un mécanisme de synchronisation - à la charge du titulaire - dans le cas où le titulaire souhaite utiliser des dépôts Git qui ne sont pas ceux du CNRS).	0
DEV_048	La notion de tag (au sens Git) est utilisée pour faire le lien entre les modifications de code source et la version de la livraison.	0
DEV_049	Un modèle de gestion des branches Git est utilisé (*par exemple Gitflow*) en accord avec le CNRS.	1

Référence	Libellé exigence	Priorité
DEV_050	Le CNRS dispose d'un outil d'analyse statique de code source, SonarQube, utilisé pour analyser le code de la solution. Le titulaire a la possibilité d'utiliser également un outil d'analyse de qualité du code, qui peut ne pas être SonarQube. Des indicateurs et des métriques de qualité logicielle reposant sur ces outils sont proposés par le titulaire. Les éléments de qualité remontés par l'outil SonarQube du CNRS et analysés ensuite, sont définis au démarrage du projet.	1
DEV_051	Le CNRS dispose d'un outil d'intégration continue, Gitlab CI, utilisé à minima pour lancer l'analyse Sonar. De manière générale, la solution est construite par cet outil. Le code source contient un fichier " .gitlab-ci.yml " indiquant la marche à suivre pour construire le projet (ce qui inclut au minimum la récupération des dépendances, le lancement des tests automatisés, la construction de la solution et la publication des artefacts). Tout autre mode de construction est à discuter au démarrage du projet.	1
DEV_052	Le titulaire exécute une tâche de construction automatique avant toute livraison au CNRS afin de valider la bonne réalisation des opérations de compilation, de réussite des tests unitaires ainsi que de vérifications des éventuelles licences.	1
DEV_053	La livraison et l'installation de la solution est réalisée de façon outillée et automatisée en évitant toute opération manuelle (sauvegarde système, rollback, …). Il n'y a pas de recommandation particulière pour le choix de l'outil d'installation, mais l'outillage écrit pour réaliser cette tâche est également géré dans l'outil de gestion de code Gitlab du CNRS.	1
DEV_054	Le titulaire se synchronise avec le gestionnaire de version (Git) du CNRS à chaque livraison pour le code spécifique développé pour le CNRS afin que le CNRS ait une visibilité sur le code, les tests unitaires et les tests d'intégration associés.	0
DEV_055	La réussite de l'ensemble des tests unitaires est une condition nécessaire à l'acceptation d'une livraison majeure. Le niveau de réussite des tests unitaires à atteindre peut cependant faire l'objet d'une concertation en cas de forte contrainte au cas par cas.	1
DEV_056	Les modifications de schémas de base de données sont automatisées par l'application soit par le lancement de commandes de migration fournies par le framework, soit lors du démarrage de l'application.	1
SSI_DEV_101	L'administration fonctionnelle de la solution est réalisée par une IHM spécifique, si possible dédiée. Elle ne nécessite pas de connexions en SSH ou d'actions nécessitant une console (ex : récupération de logs récurrente, édition de fichiers de paramétrage pour lancer une campagne, etc.).	0
SSI_DEV_102	Les configurations des middlewares et des logiciels embarqués dans la solution sont durcies. Précision : les guides de durcissement des éditeurs et constructeurs et les guides de durcissement de l'ANSSI sont à appliquer.	0
SSI_DEV_103	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, le téléversement est effectué dans une zone disque tampon puis le fichier est déplacé hors de l'arborescence d'hébergement web.	0
SSI_DEV_104	Lorsque la solution propose une fonction de téléversement de fichier (upload), le contrôle du type MIME du fichier téléversé est effectué (sans faire confiance ni à l'extension du fichier ni aux entêtes HTTP reçues). Le fichier est refusé s'il n'est pas conforme à des attendus de type MIME prédéfinis. Les moyens techniques utilisés sont décrits dans la documentation.	0
SSI_DEV_105	Lorsque la solution propose une fonction de téléversement de fichier (upload), le contrôle de la taille du fichier téléversé est effectuée. Le fichier est refusé s'il n'est pas conforme à des attendus de taille prédéfinis. Les moyens techniques utilisés sont décrits dans la documentation.	0
SSI_DEV_106	Lorsque la solution propose une fonction de téléversement de fichier (upload), la vérification de la présence de logiciels malveillants est réalisée. La présence d'un code malveillant implique la suppression du fichier concerné. Les moyens techniques utilisés sont décrits dans la documentation.	0
SSI_DEV_107	Lorsque la solution propose une fonction de téléversement de fichier (upload), le nom du fichier téléversé ne comporte pas de données à caractère personnel et n'est pas prédictible.	0
SSI_DEV_108	La solution intègre des mécanismes de sensibilisation (encarts, popups ou bandeaux sur les interfaces utilisateur) dès lors que les services fournis par la solution ou les données traitées par la solution font état d'une sensibilité particulière.	1

Référence	Libellé exigence	Priorité
SSI_DEV_109	Le cycle de développement inclut des phases régulières d'audit statique de code, par l'utilisation d'outils d'aide à l'analyse et/ou par revue de code par un pair. Les constats issus de ces audits sont tous traités de manière proportionnée au risque induit et font l'objet d'un plan d'action formalisé.	1
SSI_DEV_110	Le cycle de développement inclut des phases régulières de revues des vulnérabilités liées aux dépendances logicielles. Les constats issus de ces revues sont tous traités de manière proportionnée au risque induit et font l'objet d'un plan d'action formalisé.	1
SSI_DEV_111	Le processus de développement inclut des dispositions bloquant les mises en production d'un code présentant des vulnérabilités ayant un impact significatif sur la sécurité des données.	0
SSI_DEV_112	Le processus de développement inclut des dispositions permettant de prendre en compte les vulnérabilités résiduelles du code mis en production (dette sécurité).	1
SSI_DEV_113	Toute saisie utilisateur est vérifiée côté serveur en conformité avec le format, la taille, la sémantique et le type de données attendu.	0
SSI_DEV_114	L'utilisateur de la solution est déconnecté de sa session après un temps paramétrable dans la solution. Cette durée est implémentée de manière cohérente dans l'ensemble des modules techniques nécessaires à la solution.	0
SSI_DEV_115	Les identifiants de session utilisateur sont aléatoires.	0
SSI_DEV_116	Les informations liées à l'authentification, l'autorisation, l'habilitation des utilisateurs ne sont jamais passées en paramètres des URL.	0
SSI_DEV_117	Les bannières de connexion et les messages d'erreur applicatifs sont présentés à l'utilisateur en masquant toute information technique divulguant les composants de la solution et leurs versions.	0
SSI_DEV_118	La solution ne récupère pas de code externe (en dehors de sa phase de construction), sauf si la dépendance a été définie explicitement, intégralement et statiquement dans son code.	1
SSI_DEV_119	La solution met en œuvre des mécanismes de protection contre les différents types d'injection de données ou formats non attendus dans la solution (ex: injections SQL, modification de requêtes LDAP, modification d'arguments ou paramètres d'exécution d'un exécutable etc.)	0
SSI_DEV_120	Les composants logiciels utilisés pour le développement (inclus les bibliothèques de développement, l'environnement de développement, les outils de compilation et d'interprétation, etc.) disposent d'un historique clair et vérifiable de leurs vulnérabilités et ne présentent pas de faille non corrigée à la date de l'implémentation.	0

4.2.4 Base de données

Les exigences et recommandations techniques concernant les bases de données sont les suivantes :

Référence	Libellé exigence	Priorité
BDD_001	Une base de données (relationnelle ou non relationnelle si c'est pertinent) est utilisée pour gérer la persistance des données.	0
BDD_002	Les solutions de SGBD de référence sont PostGreSQL et MongoDB.	1
BDD_003	La non adhérence au SGBD est assurée, les requêtes ne sont pas implémentées directement dans le code applicatif (batchs compris), ni au travers de procédures stockées. Dans le cas des langages orientés objet, un ORM (mapping entre le modèle relationnel et le modèle objet) est utilisé. Dans les autres cas, une couche d'abstraction de la base de données est utilisée. Lorsque des requêtes SQL sont implémentées, elles le sont en respectant le standard SQL ANSI.	1
BDD_004	Au niveau SGBD, le jeu de caractères utilisé est UTF-8	1
BDD_005	Tous les objets de la base de données sont documentés.	1

4.2.5 Engagements de qualité de service pour l'application

4.2.5.1 *Disponibilité*

Dans le cas d'une phase de migration en production (portage), une interruption de service de 2 jours maximum est envisageable.

Dans le cas d'un déploiement d'une nouvelle version (mise en production), l'interruption de service acceptable est de 4h en continu une fois par mois ; que ce soit en cas de panne de l'application, ou en cas de maintenance programmée.

Les périodes de maintenance programmée se font à des périodes décidées en commun accord entre le CNRS et le titulaire.

Il est à noter qu'étant donné le caractère particulier d'une application fonctionnant selon un calendrier de campagne, l'application doit rester disponible et performante, en particulier pendant les pics d'utilisation de fin de période.

4.2.5.2 *Intégrité*

La solution doit permettre un contrôle de l'intégrité des données (intégrité structurelle et intégrité du contenu).

En cas de corruption de données, la perte de données acceptable est de 24h. Si nécessaire, l'application doit avoir la possibilité de reprendre les flux ou les batch qui auront été générés lors de la période de perte de données.

Le CNRS doit parfaitement maîtriser la nature des données utilisées par l'application et les mécanismes permettant de restaurer un jeu de données cohérent et exhaustif en cas de nécessité.

Le titulaire est tenu de fournir un descriptif exhaustif des données utilisées et des contraintes techniques associées à une restauration. L'usage des contraintes référentielles est fortement conseillé.

4.2.5.3 *Performances*

Le CNRS définit comme suit les caractéristiques de performances attendues de l'application :

- Connexion au serveur (contrôle des accès compris) et affichage de la page d'accueil en moins de 5 secondes.
- Temps d'affichage d'une IHM de saisie / consultation inférieur à 3s dans 80% des cas.
- Temps d'exécution d'une requête de recherche inférieur à 10 secondes,
- Temps de génération d'un état inférieur à 20 secondes.

Ces chiffres correspondent à des transactions simples et largement utilisées dont le temps de réponse est mesuré sur le poste client hébergé sur le même réseau.

Certaines fonctionnalités peuvent déroger à ces règles. Toutefois elles doivent :

- faire l'objet d'un accord explicite du chef de projet DSI,
- afficher à l'utilisateur des éléments permettant de juger de leur avancement.

Le titulaire fournit au CNRS :

- des éléments de dimensionnement de la plate-forme de production pour garantir un niveau de performance conforme au besoin en regard des éléments de volumétrie disponibles, tout en respectant les principes d'écoresponsabilité (pas de surdimensionnement)
- des éléments de tuning de la plate-forme permettant d'optimiser les performances (système, base de données, …).

Le titulaire fournit au CNRS en même temps que chaque version stable de l'application le rapport des tests de performances qui auront été menés.

Ce rapport met particulièrement en avant les éléments chiffrés concrets qui permettent de valider les temps de réponses exigés par le CNRS en condition de forte charge applicative. Il met aussi en évidence les composantes techniques de l'application nécessitant le plus de ressources techniques et induisant des temps de réponses significatifs.

4.3 EXIGENCES D'ERGONOMIE-GRAPHISME

Les applications Web du CNRS doivent répondre à des impératifs d'identité et d'ergonomie. Elles doivent également suivre des recommandations techniques pour leur intégration (cf. § 4.2.3.3) afin de satisfaire au mieux les exigences d'accessibilité auxquelles tous les services Web d'un établissement public doivent se conformer.

Elles doivent appliquer les règles décrites ci-dessous afin de respecter une cohésion intra et inter-applicative au sein du CNRS.

Les éléments concernant l'ergonomie et le graphisme pourront être ajustés en cours de réalisation, de manière concertée entre le titulaire et l'équipe projet CNRS.

4.3.1 Charte graphique

Référence	Libellé exigence	Priorité
ERG_002	L'interface de la solution respecte la charte du CNRS. Les éléments de base sont décrits dans le guide numérique du CNRS (couleurs, comportements, titrailles, boutons, navigation...).	1
ERG_003	L'ensemble de la solution utilise les mêmes éléments de la feuille de style de manière logique et uniforme : police de caractère, liens de navigation, intitulés de champ, titres de différents niveaux, messages informatifs et d'aides à la saisie, messages d'alerte, etc. Il en est de même pour la sémiologie des pictogrammes.	0
ERG_005	Dans le cas d'une solution responsive, l'organisation des écrans peut s'appuyer sur des grilles (grid). Toutes les fonctionnalités essentielles de la solution sont accessibles quel que soit le média. L'apparence du bandeau et la disposition des liens utiles sont optimisées pour apparaître sur une interface de smartphone.	1

4.3.2 UX/UI et Règles d'ergonomie

L'application est ergonomique c'est-à-dire qu'elle est facilement utilisable, fonctionnelle et compréhensible par l'ensemble des utilisateurs, ce de manière aisée, déductible et conviviale.

L'application accompagne l'utilisateur qui sait ce qu'il doit faire sur la page active. Il doit également pouvoir naviguer et se repérer dans l'ensemble de l'application. Pour cela, l'application doit utiliser les systèmes de navigation les plus adaptés, *par exemple : menus, onglets, enchaînements d'étapes, etc*.

Les éléments fonctionnels du cœur de page doivent être disposés de manière à permettre une lecture facile, avec des éléments regroupés et structurés et des titres explicites et clairement hiérarchisés.

La conception de l'IHM peut faire appel à des composants d'IHM innovants, *par exemple : effets de transition, de transparence, auto complétion, etc*. en restant vigilant toutefois à ne pas alourdir exagérément le poids des pages. Entre plusieurs composants rendant le même service, le choix sera guidé par des critères d'écoresponsabilité (poids du composant, consommation en ressources, pérennité et maintenabilité).

L'application est conçue de manière globale et homogène.

Référence	Libellé exigence	Priorité
ERG_006	La taille des fenêtres est adaptable à différentes tailles et résolutions d'écrans. Aucune fenêtre de la solution ne comporte d'ascenseur horizontal.	1
ERG_007	Les tableaux sont conçus de manière optimisée (utilisation de formules synthétiques, de pictogrammes, interlignages valorisés par des couleurs de fond, mise en valeur des entêtes, des liens, ordre des colonnes pertinent, système de navigation pour les tableaux longs).	1
ERG_008	Les titrailles et entêtes sont explicites et clairement structurées et hiérarchisées (utilisation de la feuille de style CSS et des balises h1, h2, etc.).	0
ERG_009	Les éléments de navigation sont clairs et explicites. Dans le cas d'arborescences complexes, un chemin de navigation apparaît.	1
ERG_010	Dans le cas de solution responsive, l'interface est adaptée au pilotage de l'IHM via un doigt (zone cliquable agrandie, survol impossible, navigation par balayage de l'écran, etc.).	1

4.4 EXIGENCES DE SÉCURITÉ

Le référentiel des exigences sécurité est présenté dans le tableau ci-dessous. Lorsque nécessaire, il est complété par des éléments détaillés dans les paragraphes suivants.

Référence	Libellé exigence	Priorité
SSI_101	Un dossier de sécurité pour la solution détaillant les mesures de sécurité opérationnelle mises en application, ainsi que tous les éléments de preuve de la réelle application de ces mesures (captures d'écran, fichiers de configuration, comptes rendus...) est créé et maintenu. Il indique également comment ces mesures sont régulièrement vérifiées et le dossier comprend le CR des vérifications, le compte-rendu des audits. Ce même dossier constitue une preuve de mise en œuvre des mesures de sécurité conformément au RGPD.	0

Référence	Libellé exigence	Priorité
SSI_102	Lorsque des fonctions de visa ou de signature électronique sont mises en œuvre, elles respectent les dispositions du règlement eIDAS (https://cyber.gouv.fr/le-reglement-eidas-n9102014) et du RGS (https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs). La mise en œuvre est obligatoirement discutée avec le département Cybersécurité de la DSI.	0
SSI_103	Les environnements hors production (développement, intégration, essai, recette, école, pré-production, formation, etc.) n'utilisent pas les données et accès de production.	0
SSI_CRYPT_101	Seuls des protocoles de transport de données chiffrés sont utilisés. Précisions : se référer au RGS 2.0 annexes B1, B2 et B3 pour les versions des protocoles et algorithmes de chiffrement autorisés https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents	0
SSI_PDI_101	Un inventaire des ressources matérielles et logicielles composant la solution et de leurs versions est maintenu à jour.	0

4.4.1 Auditabilité

Niveau de traçabilité

La solution met en œuvre obligatoirement la politique de traçabilité de l'ensemble des accès (autorisés et refusés) et des opérations réalisées. Ces traces doivent contenir à minima les informations suivantes :

- Date et heure de l'accès (avec une information d'horodatage fiable) : connexion et déconnexion ;
- Compte d'accès ;
- Etat de l'accès : autorisé ou refusé (et la raison en cas d'échec) ;
- Opérations réalisées ;
- Adresse IP source et protocole d'accès.

De plus, la solution doit implémenter ces fonctions autours de la gestion des traces :

- Durée de rétention des traces (mécanisme de rotation des traces, capacité de rétention maximale) ;
- Centralisation des traces ;
- Sauvegarde des traces ;
- Archivage des traces ;
- Protection des traces (pour assurer leur disponibilité, intégrité et confidentialité) ;
- Supervision des traces.

Gestion des traces

La solution doit permettre un reporting sur les :

- Opérations en général ;
- Accès et les opérations qualifiées comme sensibles réalisées ;
- Sortie d'information (ou exports de données);
- Données non intègres.

L'accès à ces rapports doit être réservé aux personnes clairement identifiées et habilitées.

4.4.2 Protection des applications web

L'application se doit de réduire au maximum les risques d'intrusion et de prévenir les stratégies d'attaques potentielles venant du web.

L'application ne doit pas être sensible à ce type de risques connus (liste non-exhaustive) :

- les injections de codes (de tous types : SQL, XML, Null Byte, LDAP, Mail Command, OS Command, XQuery…) ;
- les attaques par XSS (Cross Site Scripting) ;

- les attaques par des faiblesses dans la gestion des droits et des sessions ;
- les attaques par références directes aux objets ;
- les attaques par « Cross-Site Request Forgery » ;
- les attaques basées sur des erreurs de configuration ;
- les attaques sur des failles de restriction d'URL ;
- les attaques sur des URL d'accès aux objets prévisibles ;
- les attaques sur des redirections abusives.

Pour cela, l'application intègre, au moins, les dispositifs suivants :

- en cas d'utilisation d'espace privé (identifiant de session, etc.) dans les cookies, privilégier les cookies SSL (attribut secure), associer obligatoirement l'attribut HTTPOnly et associer systématiquement les attributs « Path, Domain et Expire » ;
- prévoir une déconnexion au bout de 20 minutes sans saisie ;
- prévoir une possibilité de déconnexion explicite pour l'utilisateur ;
- l'identifiant de session est à initier par le serveur ;
- l'identifiant de session doit être de type aléatoire et non-prédictible et d'une entropie d'au moins 128 bits ;
- l'identifiant de session doit être forgé après l'authentification ;
- lier l'identifiant de session à l'ID utilisateur, mais aussi à son adresse physique (adresse IP) ;
- interdire le passage d'informations sur les habilitations en paramètre ;
- interdire le passage de commandes (SQL, interpréteur..) directement dans les paramètres ;
- contrôler systématiquement les paramètres (formulaires et requêtes), au niveau du serveur ;
- préférer les POST au GET ;
- interdire les références directes aux objets dans les paramètres ;
- systématiser les contrôles d'accès aux objets et aux ressources ;
- gérer les accès multiples aux ressources ;
- durcir les paramètres et possibilités de redirections et de forward ;
- restreindre les accès aux URL d'administration ;
- gérer les erreurs applicatives pour les masquer à l'utilisateur ;
- un système de token par action serait un plus.

5 CADRE D'ORGANISATION DES PRESTATIONS

5.1 SYSTÈME QUALITÉ

En ce qui concerne la qualité, le CNRS préconise de s'appuyer sur la norme ISO 9001 (Systèmes de management de la qualité) et sur des référentiels de bonnes pratiques tels que :

- ITIL® : Bibliothèque pour l'infrastructure des technologies de l'information (Information Technology Infrastructure Library)
- Agile : Manifeste pour le développement agile de logiciels.

Le CNRS est particulièrement attentif à la forte orientation utilisateur, l'approche processus et l'amélioration continue.

Le plan assurance qualité (PAQ) explicite les dispositions qualité (organisation, méthodes, outillage…) nécessaires à la bonne exécution du projet pour toutes les prestations définies dans l'accord-cadre. Il définit les procédures applicables à l'ensemble du périmètre de l'accord-cadre.

Le CNRS peut effectuer des audits de l'application du PAQ. Dans ce cas, le CNRS prévient le titulaire dans les formes mentionnées au CCAP en précisant la nature, le déroulement et le calendrier souhaité.

Côté CNRS, le chef de projet informatique est garant de l'application des dispositions qualité pour le périmètre de son projet. Il est accompagné dans cette activité par la cellule qualité de la DSI, en particulier lors du démarrage de l'accord-cadre. La cellule qualité DSI s'assure du partage des dispositions qualité entre les différents projets et veille à l'homogénéisation des pratiques.

Référence	Libellé exigence	Priorité
QUA_001	Le titulaire fournit au CNRS un plan assurance qualité. Le PAQ est ajusté d'un commun accord avec le CNRS lors du démarrage de l'accord-cadre. Il est mis à jour tant que de besoin tout au long de l'accord-cadre avec l'accord des deux parties.	0
QUA_002	Le titulaire respecte les normes, méthodes et standards qualité du plan assurance qualité. Chaque non-respect d'une exigence du plan qualité est justifié par le titulaire et approuvé par le CNRS avant d'être mis en œuvre.	0
QUA_003	Le titulaire identifie dans son équipe projet les rôles de rédaction et mise à jour du plan assurance qualité, de mise en œuvre opérationnelle des dispositions d'assurance et contrôle qualité.	1
QUA_062	Le titulaire définit dans le PAQ et met en œuvre les contrôles, revues ou audits qualité qu'il juge nécessaires et suffisants dans le contexte du projet, afin de garantir au CNRS la qualité de la prestation et du produit fourni.	1
QUA_004	Le titulaire définit une démarche d'amélioration continue décrivant les dispositions générales mises en œuvre pour faire progresser la qualité de la prestation et du produit fourni (chapitre du PAQ ou document à part). Il met en œuvre cette démarche tout au long de l'accord cadre. Il livre et présente au CNRS un bilan et un plan de progrès à la fin de chaque version majeure mise en production. En phase de maintenance, il livre et présente annuellement au CNRS un bilan de l'année passée et un plan de progrès pour l'année à venir.	1

5.2 ORGANISATION DES ÉQUIPES PROJET

5.2.1 Organisation de l'équipe projet CNRS

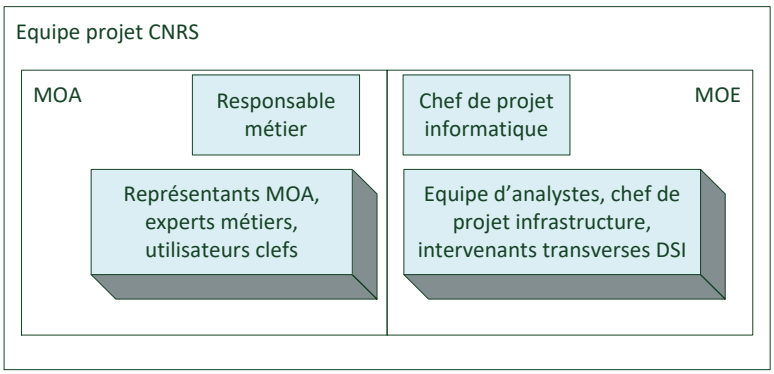


Figure 8 : Organisation du projet au CNRS

La composition de l'équipe projet CNRS est la suivante :

- un **chef de projet informatique** appartenant à la DSI ;
- un **responsable métier** appartenant à la DCIF ;
- une **équipe projet maîtrise d'ouvrage (MOA)** de la DCIF ;
- une **équipe projet maîtrise d'œuvre (MOE)** : équipe projet DMF de la DSI, dont un **chef de projet infrastructure**.

Côté maîtrise d'ouvrage, le responsable métier s'appuie sur des représentants des différentes MOA, des experts métier et des utilisateurs, pour définir les besoins métier, les prioriser, valider la solution fonctionnellement et mettre en œuvre la conduite du changement.

Côté maîtrise d'œuvre, le chef de projet informatique est garant de l'intégration dans le SI CNRS. Il s'appuie sur une équipe d'analystes dédiée au projet et sur des équipes transverses à la DSI (urbanisation, EAI, sécurité, qualité-méthodes, graphisme…). Il est accompagné par un chef de projet infrastructure en charge de coordonner et suivre les actions des équipes techniques de la DSI : infrastructure (gestion de parc, système, réseau), web, bases de données, exploitation.

L'interlocuteur CNRS privilégié du titulaire pour les relations contractuelles est le chef de projet informatique.

Un **comité de pilotage** (interne CNRS) assure le pilotage stratégique du projet. Il est composé des directions assurant la maîtrise d'ouvrage du projet et de la maîtrise d'œuvre (DSI)

5.2.2 Organisation et gestion des compétences de l'équipe projet du titulaire

Le titulaire met en œuvre une organisation et une gouvernance pour piloter l'accord-cadre. Il identifie les compétences nécessaires (y compris éco-responsabilité, accessibilité…) et s'assure du maintien de ces compétences tout au long de l'accord-cadre.

Référence	Libellé exigence	Priorité
QUA_005	Le titulaire définit dans le PAQ et met en œuvre une organisation et une gouvernance pour piloter l'accord-cadre, en regard de celle du CNRS. Il identifie les profils types (a minima : chef de projet - interlocuteur privilégié du CNRS, responsable technique - architecte, responsable sécurité, responsable qualité et développeur). Il précise pour chaque profil les compétences associées et le taux de disponibilité minimal.	1
QUA_006	Le titulaire propose dans le PAQ et met en œuvre une organisation des équipes adaptée aux différentes prestations de l'accord-cadre et aux phases de la méthode de développement du projet.	1
QUA_008	Le titulaire communique au CNRS une matrice de couverture des profils types et compétences par l'équipe projet ainsi que l'identité et le CV de chaque membre de l'équipe dès la notification de l'accord-cadre et à chaque changement d'un membre de l'équipe projet.	1
QUA_009	Le titulaire s'engage sur une équipe ferme pour le démarrage de l'accord-cadre, a minima pour les profils types de chef de projet et responsable technique.	1

Référence	Libellé exigence	Priorité
QUA_010	Le titulaire assure tout au long de la durée de l'accord-cadre : ▪ le maintien de la qualité : respect des profils types déposés dans l'offre du titulaire pour chacun des intervenants ; ▪ le maintien de la continuité : pas plus d'un changement au cours d'une période de six (6) mois glissants parmi les profils clés du titulaire, sauf en cas de force majeure.	1
QUA_011	En cas de nécessité de remplacement d'un membre de l'équipe, la période de recouvrement est comprise à minima entre deux (2) semaines et un (1) mois en fonction du profil. Ce délai de transfert de compétences et de connaissances du contexte du CNRS et du projet est défini en accord avec le CNRS et strictement respecté.	1
QUA_012	Le titulaire informe le CNRS par écrit de tout changement concernant l'équipe projet avec un préavis de trois (3) mois pour les profils clefs ou un (1) mois sinon.	1
QUA_013	Le titulaire met en œuvre des dispositions pour gérer la variation de charges de son équipe afin de garantir sa flexibilité et sa réactivité en fonction de l'activité du projet.	1

5.3 DISPOSITIFS DE CONDUITE DE PROJET

5.3.1 Structures de pilotage projet

Les principales structures à mettre en place entre le CNRS et le titulaire pour assurer le bon déroulement du projet sont décrites ci-dessous :

- **Comité de projet (MOA/MOE/titulaire) :**
  - il a pour objet le pilotage global des activités du titulaire (y compris qualité et sécurité), ainsi que le suivi de l'avancement des activités sur les différentes applications du périmètre (risques, indicateurs, planning global, ressources, suivi financier). Il décide du lancement d'une nouvelle prestation et dans ce cadre, valide la commande ;
  - il est composé pour le CNRS du responsable global de l'accord-cadre, des chefs de projet informatiques des différentes applications du périmètre, de membres des équipes projet en fonction de l'ordre du jour, d'un éventuel représentant des départements qualité et sécurité, et de la direction de la DSI, et pour le titulaire, a minima, du chef de projet ;
  - pour chaque réunion de comité, un ordre du jour systématique et un document support sont diffusés au préalable, aux participants et un compte-rendu est rédigé et envoyé à son issue. Le CNRS valide le compte-rendu dans les cinq jours. A défaut de réponse, le compte-rendu est réputé approuvé par le CNRS.

- **Comité de suivi (MOE/titulaire) :**
  - il a pour objet le pilotage régulier des activités du titulaire, ainsi que le suivi opérationnel du projet (suivi des actions, des versions, des livraisons…) ;
  - il est composé pour le CNRS du chef de projet informatique et de membres de l'équipe projet en fonction de l'ordre du jour et pour le titulaire, a minima, du chef de projet ;
  - pour chaque réunion de comité, l'ordre du jour est systématique ainsi qu'un compte-rendu diffusé aux participants. Le CNRS valide le compte-rendu dans les cinq jours. A défaut de réponse, le compte-rendu est réputé approuvé par le CNRS.

Référence	Libellé exigence	Priorité
QUA_014	Le titulaire met en œuvre et participe aux comités de suivi selon une fréquence mensuelle ou définie en accord avec le CNRS.	1
QUA_015	Le titulaire met en œuvre et participe aux comités de projet selon une fréquence hebdomadaire au départ, puis bimensuelle en fonction de l'activité en cours, ou définie en accord avec le CNRS.	1
QUA_016	Le titulaire fournit aux participants des comités un document support dans les deux jours ouvrés précédant la réunion.	1
QUA_017	Le titulaire rédige et adresse le compte-rendu des comités aux participants dans les deux jours ouvrés consécutifs au comité.	1
QUA_018	Le titulaire propose dans le PAQ et met en œuvre toute autre structure de pilotage adaptée aux différentes prestations de l'accord-cadre.	1

5.3.2 Pratiques de gestion de projet

Le CNRS souhaite qu'a minima le titulaire mette en œuvre les pratiques de gestion de projet suivantes :

Référence	Libellé exigence	Priorité
QUA_020	Chaque réunion ou point téléphonique entre le titulaire et le CNRS fait l'objet d'une trace écrite (courriel, compte-rendu de réunion) rédigée par le titulaire et à valider par l'ensemble des participants dans un délai fixé par les 2 parties.	1
QUA_021	Chaque courriel envoyé suit les préconisations suivantes : ▪ préfixer l'objet du message avec le nom du projet : « [Nom projet] sujet » ; ▪ si nécessaire, indiquer l'urgence attendue pour la réponse en précisant URGENT dans l'objet du message « [nom-projet] URGENT sujet » ; ▪ dans le corps du message, préciser ce qui est attendu du destinataire : simple information, avis, décision, action… Si nécessaire, indiquer la date d'échéance attendue pour la réponse ; ▪ éviter les pièces jointes, les remplacer par des liens vers l'outil collaboratif du CNRS.	1
QUA_022	Le titulaire suit et informe le CNRS des actions identifiées lors des comités ou réunions diverses avec le CNRS.	1
QUA_023	Le titulaire tient à jour et diffuse au CNRS un planning du projet, global pour l'ensemble du projet et détaillé pour la phase à venir.	1
QUA_024	Le titulaire gère les risques du projet qui ont été formalisés dans son offre et ajustés lors du démarrage et tout au long de l'accord-cadre.	1
QUA_025	Le titulaire définit les procédures d'alertes et d'arbitrage.	1
QUA_026	Le titulaire met en œuvre une procédure de gestion de crise en cas d'alerte avérée. Il précise le processus d'escalade suivi pour le traitement et la résolution de ces problèmes.	1

La gestion de crise s'impose dans le cas d'incident persistant (délai de résolution indéterminable, correction impossible ou inefficace), d'incident de sécurité de grande envergure (attaque virale), d'incidents multiples, de risque d'altération de données (perte de sauvegarde, …), de risque avéré sur le fonctionnement et les missions du CNRS (atteinte à l'image de marque), et de l'occurrence de tout événement à caractère improbable ou de criticité catastrophique (atteinte à la sauvegarde des personnes ou des biens).

5.3.3 Indicateurs de pilotage et qualité du projet

Des indicateurs pertinents sont définis pour permettre de suivre l'avancement du projet et d'anticiper la survenance des difficultés. Ces indicateurs sont mesurés régulièrement et présentés par le titulaire lors des différents comités.

Les indicateurs que le CNRS souhaite suivre sont notamment les suivants :

- indicateurs de pilotage :
  - état d'avancement des prestations en cours (livrées, recettées, facturées)
  - coûts et ressources prévues, affectées, consommées
  - turnover de l'équipe projet
  - respect des délais de diffusion des documents pour les comités
  - taux de satisfaction client
- indicateurs de qualité du code :
  - taux de couverture des tests unitaires automatisés
  - taux de commentaires
  - convention de nommage
  - complexité du code, couplage
  - mesures de performance
  - mesures d'éco-responsabilité si disponibles
- indicateurs de qualité des livraisons :
  - respect des délais de livraison

- nombre d'anomalies[4] (bloquantes, majeures, mineures) en recette et en production, ratio nombre anomalies/charge commandée, nombre d'anomalies imputables à des régressions
- nombre de livraisons nécessaires au prononcé de la validation (documents et logiciels)

Le titulaire peut proposer de nouveaux indicateurs, dans la mesure où ils permettent de piloter efficacement le projet.

Le plan de mesure explicite les indicateurs, leurs modalités de calculs (formule, période retenue, outillage), leurs objectifs à atteindre et leurs modalités de suivi.

Référence	Libellé exigence	Priorité
QUA_027	Le titulaire fournit au CNRS un plan de mesure (chapitre du plan assurance qualité ou document à part) adapté à la méthode de développement du projet. Le plan de mesure est ajusté d'un commun accord avec le CNRS lors du démarrage de l'accord-cadre. Il est mis à jour tant que de besoin tout au long de l'accord-cadre avec l'accord des deux parties.	1
QUA_028	Le titulaire élabore, maintient et livre lors des différents comités les tableaux de bord conformes au plan de mesure comprenant les indicateurs adaptés au niveau du comité concerné.	1

5.4 MÉTHODE DE DÉVELOPPEMENT

5.4.1 Cycle de vie

Les activités à mener tout au long du projet se répartissent de la manière suivante :

- expression des besoins (à la charge du CNRS) ;
- réalisation (à la charge du titulaire) : spécifications fonctionnelles et techniques détaillées, conception, paramétrage ou développements spécifiques, tests unitaires, d'intégration, de validation, de non-régression, de performance et de sécurité ;
- recette (à la charge du CNRS, avec assistance éventuelle du titulaire) : validation des développements en environnement de recette ;
- mise en production (à la charge du CNRS, avec assistance éventuelle du titulaire) : initialisation du système, mise en production ;
- en parallèle, conduite du changement (à la charge du CNRS, avec assistance éventuelle du titulaire) : communication, formation des utilisateurs, documentations utilisateurs, organisation de l'assistance.

Pour l'enchaînement de ces activités, le CNRS préconise un cycle de vie itératif et incrémental[5], découpé en plusieurs versions mises en production sur décision du CNRS. Chaque version suit globalement un cycle en cascade.

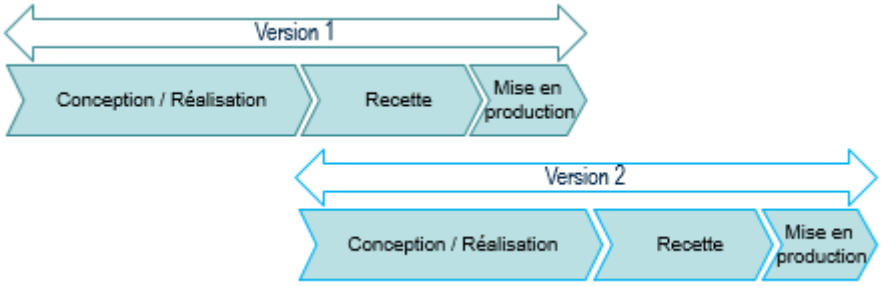


Figure 9 : Cycle de vie en cascade itératif et incrémental

Toutes les dispositions mises en œuvre par le titulaire pour donner visibilité au CNRS sur la réalisation d'une version en cours sont appréciées par le CNRS.

Afin de vérifier l'avancement régulier des travaux et de détecter en amont les problèmes, le titulaire peut planifier, en accord avec le CNRS, une ou plusieurs mises à disposition intermédiaires des produits de la commande. Elles donnent lieu, le cas échéant et selon le livrable, à des remarques pour les documents ou des déclarations d'anomalies (pour l'application). Elles ne donnent pas lieu à des opérations de réception au sens du CCAP.

[4] La définition et la typologie des anomalies sont décrites dans le glossaire du Livret 2 du CCTP.
[5] La notion d'incrémental sous-entend ici qu'une première itération de la mise en œuvre d'une fonctionnalité peut être suivie d'une deuxième itération visant à la compléter ou la modifier au vu de ce qu'a matérialisé la première itération mais également au vu de ce que l'ajout d'autres fonctionnalités a pu mettre en évidence pour l'utilisateur.

Référence	Libellé exigence	Priorité
QUA_029	Le titulaire définit dans le PAQ et met en œuvre une méthode de développement itérative-incrémentale, adaptée au contexte du projet ou de l'évolution. Il identifie les phases, entrées attendues, activités, rôles et livrables fournis.	1
QUA_031	Le titulaire, en accord avec le CNRS, définit le périmètre des versions et des itérations en fonction des exigences fonctionnelles (priorités des utilisateurs), ergonomiques, techniques et dans un objectif de réduction des risques.	1
QUA_030	Dans le cas où le CNRS demande une méthode de développement orientée agile, Scrum est préconisé (cf. https://www.scrum.org). Le titulaire définit dans le PAQ les modalités de sa mise en œuvre opérationnelle. Le cycle de développement de l'application est découpé en versions mises en production, elles-mêmes composées d'itérations (sprints de durée fixe) permettant de disposer rapidement de nouvelles fonctionnalités. Les activités à réaliser, les livrables attendus et l'outillage de suivi et pilotage du projet demeurent les mêmes qu'en mode non orienté agile. L'ensemble de la documentation est créée, mise à jour et livrée de façon itérative et incrémentale.	1
QUA_007	Dans le cas où le CNRS demande une méthode de développement orientée agile, le titulaire définit dans le PAQ les rôles spécifiques liés au mode agile (*par exemple :* product owner, proxy product owner, scrum master, équipe de développement). L'attribution des rôles aux membres des équipes CNRS et titulaire se fait en concertation avec le CNRS.	1
QUA_019	Dans le cas où le CNRS demande une méthode de développement orientée agile, le titulaire définit dans le PAQ les objectifs, la fréquence ainsi que les participants du titulaire et du CNRS pour chaque rituel mis en place (*par exemple : sprint planning, daily scrum, sprint review, sprint retrospective*).	1

5.4.2 Activités de réalisation (à la charge du Titulaire)

Le titulaire conduit les travaux de réalisation en respectant les exigences applicables.

Afin de minimiser les phases de recette du CNRS (nombre d'anomalies[6] minimal et période réduite de tests de recette), le titulaire maximise la qualité des documents de conception et du code produit et propose une organisation pertinente quant à ses propres tests (organisation, outillage…).

Référence	Libellé exigence	Priorité
QUA_032	Le titulaire décrit dans le PAQ le déroulement des ateliers de travail avec le CNRS : leur déclenchement en lien avec le cycle de vie du projet, leurs modalités de déroulement, les supports produits (avant, après et dans quels délais).	1
QUA_033	Le titulaire intègre dans sa démarche de conception de la solution une méthode d'analyse de l'expérience utilisateur (UX) afin de prendre en compte les critères de satisfaction de l'utilisateur.	2
QUA_034	Le titulaire s'appuie sur une maquette pour faire valider au CNRS, avant codage, les règles d'ergonomie, de présentation des écrans et de navigation dans l'application.	1
QUA_035	Les spécifications fonctionnelles détaillées sont formalisées sous forme de cas d'utilisation et de diagrammes UML.	1
QUA_036	Le titulaire définit dans le PAQ la stratégie de tests qu'il met en place pour le projet, en couverture des exigences fonctionnelles, techniques et d'interface. Il en précise également les différents niveaux (unitaire automatisé ou manuel, d'intégration, de validation, de non-régression, de performance unitaire et/ou plus global, de sécurité) et l'outillage associé.	1
QUA_037	Le titulaire adapte l'activité de test à la méthode de développement du projet.	1

[6] La définition d'une anomalie est décrite dans le glossaire du Livret 2 du CCTP.

Référence	Libellé exigence	Priorité
QUA_038	Dans le cas où le CNRS demande une méthode de développement orientée agile, le titulaire définit dans le PAQ et met en œuvre : ▪ l'utilisation de user stories permettant de spécifier le contenu du backlog de chaque itération (tout en assurant la rédaction finale des spécifications fonctionnelles détaillées sous forme de cas d'utilisation), ▪ des techniques de tests adaptées (tels que Test Driven Development, Acceptance Test-Driven Development…).	1

5.4.3 Activités de recette (à la charge du CNRS)

Le CNRS rédige son cahier de recette pour ses propres tests. Ce cahier de test est partagé par la DSI dès que possible et réutilisé par le titulaire pour ses tests d'intégration ou de validation.

La recette CNRS est composée de différents types de tests :

- fonctionnels, techniques, intégration dans le SI, sécurité (par la maîtrise d'œuvre DSI) ,
- métier (par les maîtrises d'ouvrage).

Une analyse de la qualité du code et de l'architecture logicielle peut également être réalisée par la DSI (en plus des comptes rendus et indicateurs fournis par le titulaire).

Le CNRS passe des scénarios de tests en environnement de recette à chaque livraison logicielle ou évolution du paramétrage.

Les résultats des tests du CNRS sont consignés dans des dossiers de tests ou dans l'outil de gestion des tests de recette du CNRS.

Les anomalies détectées par le CNRS sont formalisées et classifiées selon 3 niveaux de gravité (cf. glossaire du Livret 2 du CCTP) dans l'outil de gestion des anomalies et évolutions du CNRS.

Référence	Libellé exigence	Priorité
QUA_039	Le titulaire s'engage à corriger la totalité des anomalies issues de la recette avant mise en production, sauf dérogation explicite du CNRS.	0

5.5 GESTION DES ENVIRONNEMENTS

5.5.1 Postes de travail du titulaire

Le titulaire respecte les contraintes suivantes pour les postes de travail de tous les membres de son équipe :

Référence	Libellé exigence	Priorité
ENV_001	Le titulaire fournit pour ses équipes, les postes de travail, imprimantes, scanner… et les logiciels, ainsi que les fournitures bureautiques, y compris lorsque la réalisation s'effectue dans les locaux du CNRS.	0
ENV_002	Le titulaire respecte les contraintes du cadre de cohérence technique (CCT) au niveau de la connectivité SSL, et regroupe dans un réseau dédié tous les postes de travail non hébergés dans les locaux du CNRS et devant accéder aux ressources serveurs et bureautiques du CNRS.	0

5.5.2 Environnement de développement

La plate-forme de développement et de tests unitaires mise en œuvre par le titulaire doit respecter les contraintes suivantes :

Référence	Libellé exigence	Priorité
ENV_003	Le titulaire met en œuvre une plate-forme de développement et tests pour son besoin propre, compatible avec l'environnement cible de production qui fait référence.	0

Référence	Libellé exigence	Priorité
ENV_004	Le titulaire implémente sur la plate-forme de développement des « bouchons » afin de simuler des connexions aux services d'infrastructures qui seront utilisés sur les autres environnements (en particulier l'EAI/ESB et le service d'authentification).	0

5.5.3 Environnements CNRS

Le CNRS fournit et administre l'ensemble des plates-formes serveurs du projet à l'exception de la plate-forme de développement et de tests du titulaire :

- Un environnement d'Intégration : cet environnement permet au titulaire de tester le déploiement et l'intégration de l'application dans le SI du point de vue technique uniquement (authentification et EAI/ESB compris).
- Un environnement de Recette : cet environnement permet au CNRS de réaliser les tests de recette (Vérification d'Aptitude) de l'application avant mise en production.
- Un environnement de Production : cet environnement héberge l'application accessible aux utilisateurs et permet au CNRS de réaliser la Vérification de Service Régulier.
- Un environnement de Formation : cet environnement est dédié aux formations des utilisateurs à l'application.

Le CNRS est responsable des briques mutualisées comme les frontaux web, le SSO (Single Sign-On) et les serveurs de base de données.

Le CNRS est responsable (installation et exploitation) des composants d'infrastructures, OS, stockage, réseau, sur tous les environnements (intégration, recette, formation et production). La configuration logicielle des environnements de recette et de formation est la même que celle de production, alors que la configuration de l'infrastructure sous-jacente (CPU, RAM, …) est équivalente ou proportionnelle (selon les projets) à celle de l'environnement de production.

Le CNRS assure l'exploitation applicative des environnements de recette, formation et production.

Le CNRS utilise l'outil Ansible Tower pour automatiser les déploiements des applications lorsque cela est possible.

Les exigences suivantes s'appliquent au paysage applicatif précité :

Référence	Libellé exigence	Priorité
ENV_005	Un environnement d'Intégration est préparé par le CNRS. Il est ensuite à la charge du titulaire de procéder aux installations applicatives sur cet environnement. Le titulaire est autonome sur cet environnement.	0
ENV_006	Les environnements de recette, de formation et de production ne sont pas accessibles au titulaire. Cependant, en cas de besoin, le CNRS demande au titulaire d'y accéder, sur site CNRS uniquement.	0

5.6 GESTION DES LIVRAISONS

La réalisation d'une commande par le titulaire donne lieu par celui-ci à la mise à disposition des livrables mentionnés dans chaque prestation (cf. Livret 2). La procédure de livraison s'effectue selon les modalités suivantes :

Référence	Libellé exigence	Priorité
QUA_040	Chaque livraison d'un produit fini effectuée par le titulaire est accompagnée d'un bon de livraison, précisant la version des composants livrés (application ou document), la liste des exigences et des modifications implémentées, en particulier la liste des fiches de relecture prises en comptes ou la liste des anomalies corrigées dans la version. Ce bon de livraison est déposé par le titulaire dans l'outil collaboratif du CNRS : cet espace est défini par le MOE et est susceptible d'évoluer au cours du projet.	1
QUA_041	Un courriel est adressé à l'équipe projet CNRS l'informant de la mise à disposition de la livraison et contenant un lien vers le bon de livraison.	1
QUA_042	Pour les livraisons documentaires, le titulaire utilise l'outil collaboratif du CNRS : cet espace est défini par le MOE et est susceptible d'évoluer au cours du projet.	1

Référence	Libellé exigence	Priorité
QUA_044	Tous les éléments fournis lors d'une livraison applicative (y compris le code source) permettent d'identifier l'application concernée et sa version livrée. Toute version de l'application est identifiée par un numéro de version unique : version. sous-version.état technique[-rcN] : ▪ le numéro de version est incrémenté à chaque évolution fonctionnelle importante, ▪ le numéro de sous-version : lors d'une évolution fonctionnelle minime, ▪ l'état technique : lors d'une correction logicielle (par rapport à la version en production), ▪ [-rcN] : (optionnel) numéro de Release Candidate pour les livraisons en recette ; ce numéro de Release Candidate n'est pas présent dans la version finale (pour la production)	1
QUA_045	En cas de livraison d'un delta, le titulaire procède à une relivraison totale une fois la version stabilisée.	1
QUA_046	En accord avec le CNRS, les livraisons applicatives peuvent être accompagnées d'une démonstration de l'application par le titulaire, en présence du titulaire et de l'équipe CNRS.	2

5.7 GESTION DE LA DOCUMENTATION

La documentation produite par le titulaire doit être de qualité et permettre une bonne compréhension des mécanismes développés à des fins d'exploitation et de maintenabilité.

Référence	Libellé exigence	Priorité
QUA_047	Tous les documents produits dans le cadre du présent accord-cadre sont livrés sous format électronique modifiable (donc pas uniquement en PDF).	1
QUA_048	Les documents du projet sont déposés et partagés par le CNRS et le titulaire dans l'outil collaboratif du CNRS.	1
QUA_049	Le titulaire remet à l'issue de l'accord-cadre l'ensemble de la documentation fonctionnelle et technique de l'application à jour (créée et modifiée tout au long de l'accord-cadre).	0

L'objectif du CNRS est de tendre vers l'application de dispositions communes pour la documentation des différentes applications. Dans le cas de l'application DMF où il existe des principes de gestion de la documentation spécifiques, ils sont appliqués tels quels ou évoluent sur demande du CNRS.

Les principes de gestion de la documentation préconisés au CNRS sont les suivants :

Référence	Libellé exigence	Priorité
QUA_050	Tout document produit contient : le nom du document, une référence, la date de dernière mise à jour, la version, l'historique des versions (si besoin), le sommaire, les pages numérotées, les marques de révision apparentes d'une version à l'autre (si besoin).	1
QUA_051	Chaque document reçoit une référence unique au sein du projet (nom du fichier) : **Nom-du-projet_Identification-du-document_[Confidentialité_]Vx.y** **ou** **Nom-du-projet_Identification-du-document_[Confidentialité_]Date-evenement** avec **:** ▪ Identification-du-document = nom représentatif du contenu, de la forme : Type-document_[Code-domaine]_Libelle-libre ▪ Confidentialité : code indiquant le niveau de confidentialité du document, DL, DC ou DR ▪ Vx.y : version du document pour les documents de référence ▪ Date-evenement au format AAAAMMJJ pour les documents événementiels (CR de réunion…). La référence du document ne contient aucun caractère accentué ni espace (à remplacer par « - »).	1

Référence	Libellé exigence	Priorité
QUA_052	Chaque document mentionne dans sa référence le code de confidentialité. Seuls les documents de niveau classification PUBLIC (cible de diffusion non contrôlée : la publication de l'information présente un impact nul pour l'organisme) n'ont pas de code de classification. Les différents codes et niveaux de classification sont les suivants : ▪ **DL** :DIFFUSION LIMITEE + Mention pour une information dont la cible n'est pas nominative mais dont la mention précise les structures ou entités destinataires de l'information ou des personnes es-qualité. La mention spécifique associée au niveau de classification peut être suffisante pour définir la liste de diffusion. Une divulgation non autorisée de l'information aurait un impact modéré ; ▪ **DC** : DIFFUSION CONFIDENTIELLE pour une information dont la cible n'est pas nominative mais précise les structures ou entités destinataires de l'information, des personnes es-qualité et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact important ; ▪ **DR** :DIFFUSION RESTREINTE conformément à l'II901 pour une information dont la cible est nominative ou précise les structures ou entités destinataires de l'information, des personnes es-qualité ayant besoin d'en connaître et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact catastrophique.	1
QUA_053	Pour chaque document, un marquage est apposé afin de signifier le niveau de protection et les mesures règlementaires à appliquer en ce qui concerne la communication, la diffusion, la reproduction, la conservation et la destruction de ceux-ci : le niveau de classification (DIFFUSION LIMITEE, DIFFUSION CONFIDENTIELLE ou DIFFUSION RESTREINTE) est apposé en haut de chaque page en caractères gras, rouge et en capitales.	1
QUA_054	Le numéro de version du document est incrémenté à chaque modification du contenu du document devant faire l'objet d'une diffusion (il n'est pas incrémenté pour des corrections portant sur la forme du document - fautes de frappe, d'orthographe, ...). Le numéro de version est de la forme : x.y, avec : ▪ **x** : incrémenté à chaque évolution majeure du document (*par exemple*, ajout de chapitres, changement de version de l'application, refonte du document…) ▪ **y** : incrémenté à chaque évolution mineure (*par exemple, prise en compte de remarques de relecture, ajout de précisions*…).	1
QUA_055	Les documents du projet sont initiés à partir de modèles. Ces modèles sont définis au démarrage de l'accord-cadre et référencés dans le plan assurance qualité. Ils peuvent être issus soit du fonds documentaire du CNRS soit de celui du titulaire.	1

Le CNRS formalise ses remarques au travers d'une fiche de relecture pour les documents qui ont fait l'objet d'une livraison, par marques de révision dans le document pour les comptes rendus et les mises à dispositions intermédiaires.

Une partie de la documentation peut éventuellement être gérée dans le Wiki du CNRS.

Les règles et pratiques à mettre en œuvre autour de la gestion documentaire sont ajustées d'un commun accord au démarrage de l'accord-cadre.

5.8 CAPITALISATION DES CONNAISSANCES

Ce paragraphe peut être intégré sur des marchés d'ampleur conséquente compte tenu des contraintes supplémentaires introduites.

La capitalisation des connaissances acquises lors de l'exécution des prestations est un facteur clés de succès, tant pendant la durée d'exécution de l'accord-cadre que lors de la phase de réversibilité éventuelle en fin d'accord-cadre. A ce titre, le titulaire met en œuvre les pratiques suivantes :

Référence	Libellé exigence	Priorité
QUA_056	Le titulaire identifie les informations (hors livrables documentaires), nécessaires à ses équipes pour exécuter correctement les prestations objet de l'accord-cadre. Il peut s'agir, sans que la liste ne soit exhaustive, de procédures, de guides opératoires, d'une base de connaissance, … Il s'assure également de leur suivi, de leur mise à jour et de la gestion de leur obsolescence.	1
QUA_057	Le titulaire rend compte de l'avancement de la mise en œuvre du système de capitalisation pendant le comité de suivi du projet.	1

Référence	Libellé exigence	Priorité
QUA_058	Le titulaire livre annuellement ou à la demande les informations relevant de la capitalisation des connaissances dans les formats compatibles avec les outils du CNRS.	1

5.9 OUTILLAGE DE SUIVI ET PILOTAGE DU PROJET

Le CNRS utilise les outils suivants :

- gestion des anomalies et des évolutions : Mantis (https://www.mantisbt.org/)
- assistance : e-dem, basé sur JIRA Service Desk (désormais Jira Service Management https://www.atlassian.com/fr/software/jira/service-management)
- base de connaissance, wiki : Confluence (https://fr.atlassian.com/software/confluence)
- gestion documentaire, collaboratif : CoRe, basé sur Microsoft SharePoint (https://www.microsoft.com/fr-fr/)
- modélisation : PowerAMC
- gestion des tests de recette : TestLink (http://www.testlink.org/)

Référence	Libellé exigence	Priorité
QUA_059	Le titulaire utilise les outils ci-dessous, fournis par le CNRS : ▪ l'outil libre Mantis, pour le suivi des anomalies et du portefeuille de demandes d'évolution, ▪ si demandé par le CNRS, l'outil e-dem, basé sur JIRA Service management, pour le suivi des incidents, problèmes et demandes, associé à une base de connaissance dans le wiki Confluence ▪ l'outil CoRe, basé sur la plate-forme collaborative MS SharePoint, pour le partage des documents, livraisons documentaires, calendriers, annuaires, suivi d'actions...	1
QUA_060	Le CNRS se réserve la possibilité de changer l'un ou l'autre des outils présentés ci-dessus, au cours de la durée de vie de l'accord-cadre. Dans ce cas, le titulaire en est informé suffisamment à l'avance et procède également au changement d'outillage dans ses relations avec le CNRS. Ce changement est réputé n'avoir aucun impact financier quant à l'exécution du présent accord-cadre.	1

Ces outils sont mis en œuvre et paramétrés par le CNRS. Ils sont accessibles par les équipes maîtrise d'œuvre et maîtrise d'ouvrage CNRS, et le sont également par le titulaire (avec des profils différents). Les pratiques mises en place autour de ces outils sont préconisées par la cellule qualité de la DSI du CNRS, elles sont communiquées au titulaire et ajustées d'un commun accord au démarrage de l'accord-cadre.

Référence	Libellé exigence	Priorité
QUA_061	Le titulaire met en œuvre des outils bureautiques et de gestion de projet qui supportent des formats compatibles avec les outils utilisés ou préconisés par le CNRS, mais non fournis au titulaire : ▪ suite bureautique : MS Office, ▪ gestion de projet : MS Project, ▪ modélisation des données : PowerAMC, ▪ dossiers et suivi des tests : TestLink, ▪ wiki : Confluence.	1

Le titulaire peut le cas échéant proposer d'autres outils pour compléter ceux proposés par le CNRS. Toutefois, ceux-ci seront soumis à acceptation par celui-ci.

5.10 MESURES ET CLAUSES DE SÉCURITÉ

5.10.1 Gestion de la Sécurité par le titulaire

Responsabilité

Référence	Libellé exigence	Priorité
SECU_001	L'organisation de la sécurité des systèmes d'information du titulaire pour le projet est décrite dans le PAS. L'équipe comporte à minima : ▪ Une personne de niveau hiérarchique supérieur formé et compétent en SSI capable de prendre des décisions dans la conduite du projet, responsable du respect des dispositions du PAS ▪ Une personne intégrée ou proche des équipes de MOE du titulaire en charge du projet responsable de la mise en œuvre du PAS ▪ La rédaction, la mise à jour et le suivi du PAS sont à la charge du titulaire	0

Dans l'exercice de leurs activités, les intervenants sont liés par un devoir de réserve et astreints au secret professionnel.

Sensibilisation, qualification et formation

Référence	Libellé exigence	Priorité
SECU_002	Le titulaire indique au CNRS la fréquence et le contenu des actions de formation et de sensibilisation de ses personnels aux enjeux et aux méthodes de Sécurité.	0

5.10.2 Protection des biens

Protection des sites

Référence	Libellé exigence	Priorité
SECU_003	Si le titulaire exécute les prestations à partir de ses propres locaux ou en télétravail, il opère en « *site sûr* » dont les caractéristiques sont à évaluer avec le département Sécurité de la DSI. Cette disposition est également valable pour le support ou la maintenance à distance. Le titulaire ne détient à aucun moment de données de production signifiantes sur ses infrastructures. Le cas échéant, le titulaire réalise un dossier de type « *site sûr* » incluant les modalités d'accès aux ressources de la DSI et les mesures de sécurité nécessaires à l'accomplissement des prestations. Si un Plan d'Assurance Sécurité existe, le dossier « *site sûr* » lui sera annexé. En cas de télétravail, aucun accès aux environnements ou aux données de production n'est autorisé.	0
SECU_004	Le titulaire fournit un dossier de site sûr décrivant les mesures de sécurité physique en place dans les locaux qu'il utilise pour l'accomplissement des prestations. Ce dossier traite des thématiques suivantes sous les angles **technique** et **organisationnel** : ▪ Infrastructures informatiques (réseaux et systèmes) ▪ Contrôle d'accès physique aux locaux ▪ Contrôle d'accès logique aux systèmes ▪ Postes de travail ▪ Liaisons réseaux externes (WAN, réseaux privés avec le CNRS) ▪ Plan de reprise/de continuité d'activité ▪ Télétravail ordinaire et télétravail exceptionnel ▪ Gestion de crise	0

Protection du système d'information

Référence	Libellé exigence	Priorité
SECU_005	Le titulaire dispose de dispositifs, de procédures et de moyens qu'il met en œuvre afin protéger les actifs du CNRS. Ces moyens permettent en particulier de : ▪ contrer les virus et codes malveillants ▪ protéger son réseau contre les intrusions. Il décrit les mesures mises en œuvre.	0

Politique de contrôle d'accès

Référence	Libellé exigence	Priorité
SECU_006	Le titulaire dispose d'une politique, de mesures et de dispositifs pour gérer le contrôle d'accès à ses locaux et à ses systèmes d'information. Cette politique concerne notamment : ▪ la politique d'attributions des droits ▪ les méthodes d'accès (authentification et autorisation) ▪ la gestion des identifiants uniques ▪ la politique de mots de passe et de gestion de l'authentification forte ▪ les processus d'autorisation pour l'accès et les privilèges des utilisateurs ▪ les processus de gestion des listes de personnes autorisées à participer aux activités de TMA ▪ les processus de révocation des droits ▪ la politique et les processus de révision des droits d'accès ▪ le contenu de la charte interne utilisateur et/ou de la charte interne administrateur Le titulaire décrit les mesures en place. Il fournit en particulier sa PSSI d'entreprise.	0

Gestion des vulnérabilités

Référence	Libellé exigence	Priorité
SECU_007	Le titulaire dispose de procédures de gestion interne des vulnérabilités sur le système d'information qu'il met en œuvre pour assurer les activités de développement, de maintenance et de support. Il décrit les méthodes et outils en place pour la découverte et le suivi de la correction de ces vulnérabilités.	0

Gestion des incidents

Référence	Libellé exigence	Priorité
SECU_008	Le titulaire dispose de procédures de gestion des incidents internes de sécurité sur le système d'information qu'il met en œuvre pour assurer les activités de développement, de maintenance et de support.	0

Exigences de Sécurité concernant les personnels extérieurs

Référence	Libellé exigence	Priorité
SECU_009	Le titulaire met en œuvre des moyens de contrôle pour s'assurer du respect des exigences de sécurité du CNRS par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre des prestations. Il fournit les éléments contractuels le liant avec ses partenaires prouvant les obligations qui leur incombent dans ce domaine.	0

Travail dans les zones sécurisées

Référence	Libellé exigence	Priorité
SECU_010	Le titulaire ne doit jamais intervenir physiquement sur un site du CNRS ou géré par le CNRS sans être mandaté et surveillé par du personnel du CNRS ou mandaté par le CNRS. Il doit refuser d'assurer sa prestation, si le personnel encadrant du CNRS ou mandaté par le CNRS ne respecte pas son obligation de surveillance. Il notifie l'incident à sa direction et au RSSI de la DSI. Le délai d'exécution de la prestation est suspendu jusqu'à ce que le personnel encadrant du CNRS ait pris les mesures nécessaires à cette surveillance. Le titulaire n'est pas autorisé, sauf autorisation expresse du CNRS, à photographier, faire des enregistrements audio ou vidéo des locaux ou des équipements du CNRS. De même, il est interdit au titulaire d'introduire du matériel photographique, vidéo, audio ou d'autres matériels d'enregistrement dans les locaux du CNRS ou géré par le CNRS, sauf autorisation expresse du CNRS.	0

Stockage et échange d'informations

Référence	Libellé exigence	Priorité
SECU_011	Le titulaire met en œuvre des moyens techniques conformes aux recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) afin de protéger de toutes divulgations indésirables volontaires ou accidentelles, toutes les informations relatives au CNRS : ▪ lors du stockage de celles-ci en dehors des sites physiques du CNRS, pendant et après les prestations. ▪ lors des échanges avec le CNRS, quel qu'en soit le moyen (e-mail, partage de fichier, etc.). De plus le titulaire effacera les informations qu'il aura en sa possession, immédiatement et en fournissant au CNRS un quitus formel : ▪ sur simple demande du CNRS ▪ en fin de prestation	0

Gestion des sauvegardes

Référence	Libellé exigence	Priorité
SECU_012	Le titulaire donne au CNRS l'ensemble des éléments techniques concourant à une sauvegarde intègre et régulière des données du CNRS qui lui sont confiées et des données nécessaires à l'exécution des prestations (plan de sauvegarde, procédures, script d'arrêt/démarrage, objets à sauvegarder, intégrité temporelle des données, etc.). La solution du titulaire doit permettre au CNRS de mettre en place des tests réguliers de restauration des sauvegardes.	0

Rétrocession des informations du CNRS

Référence	Libellé exigence	Priorité
SECU_013	Le titulaire précise les mesures et dispositifs qui garantissent le retour au CNRS et la destruction des informations du CNRS qu'il a en sa possession à l'expiration ou à la résiliation du marché. Le titulaire fournit au CNRS l'ensemble de la documentation nécessaire et une description précise des éléments techniques permettant au CNRS d'extraire les données de la solution dans un format compréhensible (*par exemple fichier csv et schéma relationnel des données*). Ces éléments doivent permettre au CNRS de reprendre ces données dans une autre solution le cas échéant.	0

5.10.3 Obligations du titulaire

Référence	Libellé exigence	Priorité
SECU_014	Le titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier, il s'engage à informer le CNRS des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention. Le titulaire est responsable du maintien en condition de sécurité des systèmes nécessaires à la réalisation des prestations jusqu'à leur échéance. Le titulaire ne peut se dégager de cette responsabilité que si, après qu'il ait informé le CNRS de failles dans la sécurité du système, de manière circonstanciée, précise et détaillée, et qu'il ait proposé une ou des solutions de nature à pallier la faille, le CNRS a choisi de ne pas mettre en œuvre ces préconisations.	0

5.10.4 Localisation des données

Référence	Libellé exigence	Priorité
SECU_015	Les lieux d'hébergement des données du CNRS, dont les journaux, les jeux d'essai pour les environnements de développement (liste non-exhaustive), satisfont aux exigences de sécurité du donneur d'ordres (CNRS) et aux dispositions de la loi informatique et libertés en vigueur. Tout transfert de données en dehors des Etats de l'UE est soumis à avis, et autorisation préalable du CNRS, après avis de son Délégué à la Protection des Données. Le titulaire communique 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 s'avère délicate dans le cadre d'architectures distribuées, il est demandé au titulaire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident. Enfin, le titulaire doit fournir au CNRS tous les éléments attestant qu'il satisfait bien aux exigences règlementaires ci-dessus, quel que soit la localisation.	0

5.10.5 Audit

Référence	Libellé exigence	Priorité
SECU_016	Le titulaire est informé de la volonté du CNRS de conduire ou organiser des audits réguliers des systèmes d'information. Ces audits techniques et organisationnels ont pour objectifs de vérifier le respect par le titulaire de ses engagements initiaux en termes d'organisation et de moyens mis en œuvre concernant la SSI. Le CNRS peut, à tout moment, à son initiative, par ses propres équipes ou par celles de tiers désignés par lui (sélectionnés sur la liste des prestataires qualifiés en audit SSI publiée sur le site de l'ANSSI à la date de commande de l'audit https://cyber.gouv.fr/produits-services-qualifies?field_type_service_value[passi]=passi), procéder à des audits des prestations confiées au titulaire, afin de : ▪ vérifier les engagements de niveaux de service, de qualité, de sécurité des prestations réalisées ; ▪ vérifier la mise en application des règles d'organisation, des méthodes, des pratiques mises en œuvre pour réaliser les prestations. A cet effet, le CNRS ou son mandataire désigné met en œuvre tous les moyens qu'il juge nécessaire pour s'assurer du parfait achèvement des prestations. Ceci inclut, sans volonté d'exhaustivité : ▪ la communication de documents tenus à jour par le Titulaire (plans, documentations, contrats, certifications, rapports…) ; ▪ l'audition orale d'équipes de maîtrise d'œuvre (techniciens, ingénieurs, responsables techniques, opérationnels, responsables de la sécurité, équipes de direction…) ; ▪ la conduite de tout audit organisationnel ou technique, en boîte blanche, noire ou grise. Le CNRS s'engage à respecter un préavis raisonnable conforme aux dispositions du CCAP avant tout déclenchement d'audit. Le résultat des audits est présenté au titulaire, et conduit à la rédaction d'un plan d'action. Les actions inscrites ne conduisent pas à facturation supplémentaire de la part du titulaire si elles découlent directement d'un constat de non-conformité par rapport : ▪ à ses engagements initiaux ou ▪ à la règlementation en vigueur à la date de notification de l'appel d'offres. Dans tous les autres cas (évolution de la règlementation, évolution de la PSSI du CNRS, évolution d'une application modifiant son profil de risque...), le titulaire peut proposer une cotation pour la réalisation des prestations de mise en conformité. Le résultat des audits de conformité aboutit à un avis formel du CNRS ▪ conforme : l'audit n'a pas révélé de dysfonctionnements majeurs, et les engagements qui ont été audités sont tenus ; ▪ conforme avec réserves : des dysfonctionnements mineurs ont été relevés ou des objectifs ne sont pas remplis au niveau de l'engagement de service attendu. Dans ce cas, le titulaire propose un plan de remédiation aux dysfonctionnements à court terme : le plan est soumis au CNRS dans les huit jours après communication de l'avis formel, et l'engagement de remédiation ne peut dépasser six mois. Le titulaire démontre à ses frais que les engagements sont tenus à l'issue du plan d'action ; ▪ non conforme : tout ou partie des engagements ne sont pas tenus, ou des dysfonctionnements majeurs ont été constatés. Dans ce cas, le titulaire engage des actions selon les modalités décrites supra, sous astreinte journalière de remise en conformité.	0

5.10.6 Application des plans gouvernementaux

Référence	Libellé exigence	Priorité
SECU_017	Dans le cadre de l'application de plans gouvernementaux, les autorités françaises peuvent décider la mise en œuvre d'un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes visant les systèmes d'information de l'État ou les systèmes d'information et réseaux de télécommunications. Il peut également s'agir de mesures d'entraînement à la réaction en cas d'incident. Dans le cadre du marché, le titulaire peut être concerné par ces alertes décidées au niveau gouvernemental, et s'engage à appliquer les consignes de sécurité données par le CNRS. Ces mesures sont susceptibles d'évoluer. Les modifications sont régulièrement transmises durant l'exécution du marché. Le titulaire est tenu de mettre immédiatement en œuvre lesdites dispositions, quand bien même elles auraient un impact significatif sur le coût de la prestation. Dans ce dernier cas, les conséquences financières de ces dispositions sont tirées soit par voie d'avenant, soit, en cas de désaccord persistant entre le CNRS et le titulaire, par les tribunaux compétents. Sans impact significatif sur les coûts, le respect de cette exigence est réputé réalisé pro bono.	0

6 ANNEXES

6.1 DOCUMENTS JOINTS

Les documents suivants sont joints au présent CCTP. Ils sont applicables tout le long de l'accord cadre.

Le CNRS pourra faire évoluer ces documents au cours de l'accord cadre en fonction des évolutions technologiques rendues nécessaires par l'état de l'art. Ces évolutions pourront faire l'objet de commandes au titulaire le cas échéant.

Nom	Description	Type[7]
Annexe 1 : Tableau des exigences	Ce document présente : ▪ les exigences applicables dans le cadre des développements et de la maintenance de la solution (onglet « cadre de cohérence technique ») ▪ les exigences applicables à l'organisation des prestations (onglet « organisation des prestations »)	[A]
Annexe 2 : CCT_Versions-cibles	Ce document présente à un instant t (ce document évolue régulièrement dans le temps et n'est donc pas figé en termes d'engagement) les versions cibles des composants applicatifs et les éléments de compatibilité navigateurs requis dans le cadre des développements et de la maintenance d'applications	[A]

6.2 PRÉSENTATION DÉTAILLÉE DU CNRS

6.2.1 La présidence-direction générale

Les entités suivantes sont rattachées à la présidence-direction générale :

- la direction de la communication (DIRCOM)
- le fonctionnaire de sécurité de défense (FSD)
- la délégation à la protection des données (DPD)
- la direction de l'audit interne (DAI)
- la mission pour la place des femmes (MPDF)

6.2.2 La direction générale déléguée à la science (DGD-S)

La **DGD-S** conduit, aux côtés du président-directeur général, la politique scientifique de l'établissement. Elle coordonne l'action des dix instituts du CNRS, veille à promouvoir l'interdisciplinarité et organise les partenariats avec les divers acteurs de la recherche, à l'échelle régionale, nationale, européenne ou internationale.

Pour remplir ses missions, la DGD-S s'appuie sur :

- les dix instituts et les unités de recherche qui leur sont rattachées,
- trois directions fonctionnelles :
  - la direction Europe et international (DEI),
  - la direction des données ouvertes de la recherche (DDOR),
  - la direction d'appui aux partenariats publics (DAPP),
- la mission pour les initiatives transverses et interdisciplinaires (MITI),
- la mission pour l'expertise scientifique (MPES),
- la mission programmes nationaux (MiPN)
- le Comité Très grandes infrastructures de recherche (TGIR),
- le secrétariat général du Comité national (SGCN).

[7] [A] = document applicable
[R] = document de référence (cf. dans le glossaire au § 6.4.2)

Des informations plus complètes sont disponibles à l'adresse suivante : https://www.cnrs.fr/fr/le-cnrs/organisation.

6.2.2.1 *Les instituts*

Les **instituts** sont les structures de mise en œuvre de la politique scientifique de l'établissement. Les directeurs des instituts participent à l'élaboration de la politique scientifique du CNRS et définissent les modalités de son application.

Chaque institut anime et coordonne l'action d'un ensemble cohérent d'activités de recherche relevant de plusieurs disciplines. Des programmes interdisciplinaires de recherche intéressant plusieurs instituts peuvent être décidés par le président après avis du conseil scientifique et approbation du conseil d'administration.

- CNRS Biologie : il a pour mission de développer et coordonner des recherches en biologie qui visent à décrypter la complexité du vivant, des atomes aux biomolécules, de la cellule à l'organisme entier et aux populations.
- CNRS Chimie : il a pour mission de développer et de coordonner les recherches concernant l'élaboration de nouveaux composés, la compréhension de la réactivité chimique, l'élucidation toujours plus fine et la prédiction des relations entre la structure des composés au niveau atomique et leurs propriétés..
- CNRS Ecologie & Environnement : il a pour mission de développer et de coordonner les recherches poursuivies dans les domaines de l'écologie et de l'environnement, incluant la biodiversité et les relations hommes-milieux.
- CNRS Ingénierie : il a pour mission d'assurer le continuum entre recherche fondamentale, ingénierie et technologie en privilégiant l'approche "système" à partir du développement des disciplines au cœur de l'institut.
- CNRS Mathématiques : il a pour mission de développer et de coordonner les recherches dans les différentes branches des mathématiques, allant des aspects fondamentaux aux applications. Il contribue aussi à la structuration de la communauté mathématique française et à son insertion dans la communauté internationale.
- CNRS Nucléaire & Particules : il a pour mission de promouvoir et fédérer les activités de recherche poursuivies dans les domaines de la physique nucléaire, physique des particules et astroparticules.
- CNRS Physique : il a pour mission de développer et de coordonner les recherches dans le domaine de la physique avec deux motivations principales : le désir de comprendre le monde et la volonté de répondre aux enjeux actuels de notre société.
- CNRS Sciences humaines & sociales : il a pour mission de développer les recherches sur l'homme, aussi bien comme producteur de langages ou de savoirs que comme acteur économique, social ou politique.
- CNRS Sciences informatiques : il a pour mission de développer des recherches dans les domaines des sciences informatiques et du numérique. L'un de ses principaux objectifs est de les positionner, avec les sciences de l'information, au cœur des enjeux pluri et interdisciplinaires en s'appuyant sur un partenariat avec les autres instituts du CNRS et plus particulièrement CNRS Ingénierie.
- CNRS Terre & Univers : il a pour mission d'élaborer, développer et coordonner les recherches d'ampleur nationale et internationale en astronomie, sciences de la Terre, de l'océan et de l'espace.

6.2.3 La direction générale déléguée aux ressources (DGD-R)

La **DGD-R** conduit, aux côtés du président, la politique administrative et financière de l'établissement. Elle a en charge le développement des ressources humaines et des activités de soutien à la recherche. Dans ce cadre, et en relation étroite avec la DGD-S, elle s'appuie sur les compétences des instituts et des dix-sept délégations du CNRS.

Pour remplir ses missions, la DGD-R s'appuie sur :

- dix-sept délégations régionales,
- six directions fonctionnelles :
  - la direction des ressources humaines (DRH)
  - la direction de la stratégie financière, de l'immobilier et de la modernisation (DSFIM)
  - la direction des comptes et de l'information financière (DCIF)
  - la direction des affaires juridiques (DAJ)
  - la direction des systèmes d'information (DSI)
  - la direction de la sûreté (DIRSU)
- une structure transversale : la mission transverse d'appui au pilotage (MTAP)
- un pôle santé et sécurité au travail (PSST) composé de :
  - la coordination nationale de prévention et de sécurité (CNPS)
  - la coordination nationale de médecine de prévention (CNMP)

- la coordination nationale de la sécurité des systèmes d'information (CNSSI).

Des informations plus complètes sont disponibles à l'adresse suivante : https://www.cnrs.fr/fr/le-cnrs/organisation.

6.2.3.1 *La direction des comptes et de l'information financière (DCIF)*

La **DCIF** est garante de la régularité des opérations comptables et de la cohérence de l'ensemble des informations financières et comptables.

Elle assure le suivi et l'enregistrement des actes de gestion liés à la mise en œuvre des crédits et à l'exécution du budget. Elle garantit l'exhaustivité et la qualité des données. Elle restitue l'information financière selon les besoins et les calendriers des services utilisateurs, de la direction de l'établissement ou des tutelles.

Dans son domaine, elle est en charge de la maîtrise d'ouvrage des systèmes d'information ainsi que de l'administration des données.

Des informations plus complètes sont disponibles sur le site Web de la DCIF à l'adresse suivante : https://www.cnrs.fr/fr/dcif

6.2.3.2 *La direction des systèmes d'information (DSI)*

La **DSI** définit et met en œuvre les systèmes d'information de gestion et de pilotage des activités de l'établissement, en adéquation avec les orientations stratégiques et métiers de l'établissement (RH, finance, décisionnel, formation, référentiels, valorisation, missions…).

Elle gère également les outils mis en commun avec les partenaires du CNRS tels que l'Amue et les universités, ainsi que la sécurité des systèmes d'information.

Enfin, la DSI met à disposition des laboratoires une offre de services numériques (ODS) destinée à simplifier, soutenir et sécuriser leur quotidien (travail collaboratif, mobilité, services cloud, sauvegarde des données, exploitation sécurisée de sites internet…).

La DSI comprend :

- **La Direction** : la directrice de la DSI est assistée d'un directeur adjoint et d'une directrice adjointe administrative.
- **Le Secrétariat Général** est chargé des aspects administratifs de la DSI. Il gère les ressources humaines, le budget, le contrôle de gestion, la logistique et les achats.
- **Le département SI Finance** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques de BFC (budget, finance, comptabilité) et de l'Infocentre métier Finance, SI financiers du CNRS.
- **Le département SI Laboratoires et soutien à la recherche** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques des applications à destination des laboratoires et des services centraux notamment pour la gestion des achats, la gestion des missions, le dialogue de gestion, la gestion du patrimoine immobilier, la gestion de la valorisation et les appels à projets. Il assure également la conduite de projets de développement d'applications dans son périmètre d'activité.
- **Le département SI Ressources humaines et paie** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques de Sirhus (Système d'Information Ressources Humaines des Unités et Services du CNRS), de l'infocentre métier RH et des convertisseurs équivalent temps plein travaillé (ETPT).
- **Le département SI Ressources humaines, santé prévention sécurité, décisionnel** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques des applications ressources humaines, santé, prévention, sécurité et décisionnel. Il réalise également la conduite de projets de développement d'applications dans son périmètre d'activité.
- **Le département Cybersécurité** met en œuvre la politique de sécurité des SI du CNRS pour l'ensemble des SI qui sont sous la responsabilité de la DSI. Il pilote et met en œuvre les démarches d'homologation de son périmètre. Il détermine les risques, objectifs et mesures de sécurité à intégrer dans les applications, services, outils, architectures et infrastructures. Il contrôle les mises en œuvre techniques et organisationnelles. Il définit, met en place et maintient les services de confiance numériques du CNRS. Il gère les incidents de sécurité de son périmètre. Il participe et collabore aux travaux de la CNSSI et de son centre de cyberdéfense.
- **Le département Plateforme des référentiels et de dématérialisation** met en œuvre les principaux référentiels structurants du SI. Il est chargé de les maintenir en conditions opérationnelles (plateforme GDR – Gestion des Données de Référence). Il est aussi chargé de la mise en œuvre des plateformes de dématérialisation des documents, de préservation et de conservation de ces derniers (services de GED – Gestion Electronique de Documents et de SAE – Système d'Archivage Electronique).

- **Le département Architecture et assistance applicatives** met en place et maintient les annuaires et outils de gestion d'habilitations, fournit de l'assistance en termes d'expertise développement et architecture applicative. Il met en place et maintient les outils d'intégration des données et assure l'assistance utilisateurs.
- **Le département Infrastructures SI** est chargé de spécifier, mettre en œuvre, opérer et maintenir les infrastructures (notamment réseaux, systèmes, bases de données) du SI du CNRS. Il accompagne toutes les activités portées par la DSI dans le domaine des infrastructures et de l'exploitation technique.
- **Le département Sites web, communication, accompagnement projet** conçoit et met en œuvre les outils pour la communication et le travail collaboratif au sein du CNRS (intranet, portails, espaces collaboratifs, sites web). Il accompagne le déroulement des projets SI au niveau urbanisation (études pour l'intégration de nouveaux besoins), qualité-méthodes et ergonomie des technologiques interface homme machine (IHM). Enfin, il a en charge la communication interne et externe de la DSI.

La DSI est implantée sur deux sites Toulouse-Labège (31) et Meudon (92).

Des informations plus complètes sont disponibles à l'adresse suivante : https://www.cnrs.fr/fr/dsi

6.2.4 La direction générale déléguée à l'innovation (DGD-I)

La **DGD-I** conduit, aux côtés du président-directeur général, la politique de transfert des résultats de la recherche, de leur valorisation et des interactions avec le monde socio-économique.

Elle définit les lignes directrices contractuelles et d'organisation afin d'accélérer les processus de transfert et de valorisation. Elle veille pour cela à construire des relations de confiance efficaces avec les partenaires académiques des unités de recherche et à amplifier les relations avec les acteurs socio-économiques. Elle coordonne la politique de l'établissement en ce qui concerne les relations avec les industriels et la création d'entreprises.

Elle pilote le suivi et le contrôle de l'accomplissement des missions confiées par le CNRS à CNRS-Innovation et aux sociétés d'accélération du transfert de technologies (SATT).

Elle a en charge le suivi et la maîtrise des coûts budgétaires associés à l'exercice des missions de transfert et de valorisation.

Pour remplir ses missions, la DGD-I s'appuie sur :

- la Direction des relations avec les entreprises (DRE),
- CNRS Innovation,
- l'ensemble des entités de la DGD-S et de la DGD-R impliquées dans les actions de valorisation de l'établissement et de la filiale CNRS Innovation.

Des informations plus complètes sont disponibles à l'adresse suivante : https://www.cnrs.fr/fr/le-cnrs/organisation.

6.2.5 Les délégations régionales (DR)

Les dix-sept **DR** du CNRS sont les interlocutrices de premier plan des partenaires de l'organisme sur le terrain. Elles ont un rôle de gestion et d'accompagnement de proximité des laboratoires répartis sur le territoire. Elles apportent notamment leur aide pour le montage de projets industriels et de programmes européens.

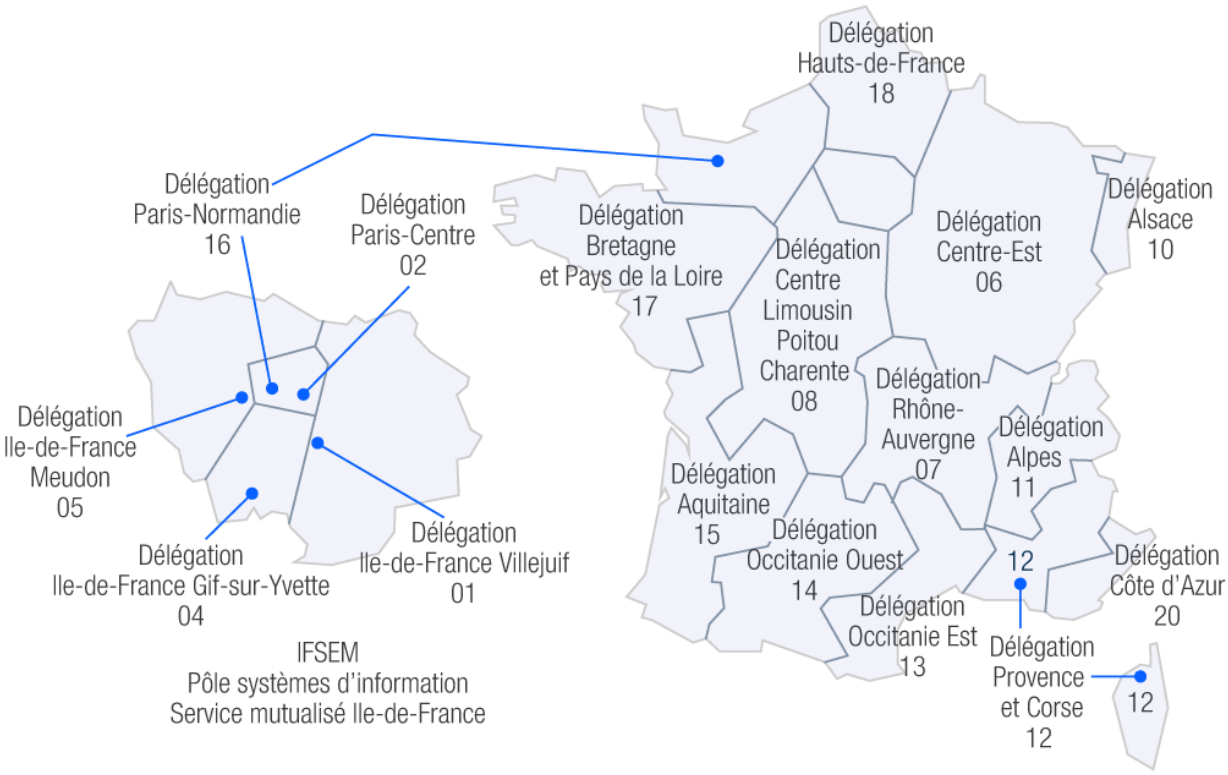


Figure 10 : Le CNRS en région

Des informations plus complètes sont disponibles à l'adresse suivante : https://www.cnrs.fr/fr/delegations-regionales-du-cnrs

6.2.6 Les unités (laboratoires)

Le CNRS compte environ 1100 laboratoires répartis sur l'ensemble du territoire français. Ce sont en très grande majorité des unités mixtes de recherche (UMR) associées à une université, une école supérieure ou un autre organisme de recherche. À ces laboratoires s'ajoutent 80 laboratoires de recherche internationaux, un nombre en progression constante.

Les **laboratoires** du CNRS sont les « briques de base » de l'établissement. Leurs équipes, formées de chercheurs, d'ingénieurs et de techniciens, sont à l'origine de la production et de la transmission des connaissances. Les laboratoires sont pour la plupart des unités mixtes de recherche, associant des partenaires du monde académique (universités, écoles et autres organismes de recherche) et industriel.

6.3 RÉFÉRENCE DES EXIGENCES

Référence	Groupe d'exigence
ACC	Accessibilité
AUTH	Authentification
BDD	Base de données
DEV	Développement
DOC	Stockage des documents
ECH	Echange de données
ENV	Environnements
ERG	Ergonomie, graphisme
HAB	Habilitations
INF	Infrastructure

Référence	Groupe d'exigence
QUA	Qualité
REGL	Conformité règlementaire
SECU	Mesure et clauses de sécurité
SSI	Sécurité des systèmes d'information
SSI_COM	Sécurité des communications
SSI_CRYPT	Cryptographie
SSI_EXP	Exploitabilité
SSI_PCA	Plan de Continuité d'Activité SSI
SSI_PDI	Politique de l'information SSI
URB	Urbanisation

6.4 ABRÉVIATIONS ET GLOSSAIRE

6.4.1 Abréviations

Le tableau suivant présente la liste des abréviations utilisées dans ce document.

Ne garder que les abréviations effectivement utilisées dans le document et compléter le tableau si nécessaire.

Sigle	Description
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface (interface de programmation applicative)
BDD	Base De Données
BFC	
CCAP	Cahier des Clauses Administratives
CCT	Cadre de Cohérence Technique
CCTP	Cahier des Clauses Techniques Particulières
CNMP	Coordination Nationale de Médecine de Prévention
CNPS	Coordination Nationale de Prévention et de Sécurité
CNRS	Centre National de la Recherche Scientifique
CPP	Chorus Pro
CSS	Cascading Style Sheets
CSV	Comma-separated values
DAJ	Direction des Affaires Juridiques
DAPP	Direction d'Appui aux Partenariats Publics
DCIF	Direction des Comptes et de l'Information Financière
DCP	Donnée à caractère personnel
DEI	La Direction Europe et International
DEV	plate-forme de DEVeloppement
DRE	Direction des Relations avec les Entreprises
DGD-I	Direction Générale Déléguée à l'Innovation
DGD-R	Direction Générale Déléguée aux Ressources
DGD-S	Direction Générale Déléguée à la Science
DNS	Domain Name System (système de noms de domaine)

Sigle	Description
DPD	Déléguée à la Protection des Données
DR	Délégation Régionale
DRH	Direction des Ressources Humaines
DSFIM	Direction de la Stratégie Financière, de l'Immobilier et de la Modernisation
DSI	Direction des Systèmes d'Information
EAI/ESB	Enterprise Application Integration (intégration d'applications d'entreprise) / Enterprise Service Bus
ETPT	Equivalent Temps Plein Travaillé
FSD	Fonctionnaire de Sécurité de Défense
FTP	File Transfer Protocol (protocole de transfert de fichiers)
GED	Gestion Electronique de Documents
GDR	Gestion des données de référence. Aussi communément nommé MDM en anglais.
GIP	Groupement d'Intérêt Public
HTML	HyperText Markup Language (langage de balisage d'hypertexte)
HTTP	HyperText Transfer Protocol (protocole de transfert hypertexte)
HTTPS	HyperText Transfer Protocol Secure (protocole de transfert hypertexte sécurisé)
IdP	Identity Provider (fournisseur d'identité)
IHM	Interface Homme Machine
IPv4	Internet Protocol version 4 (protocole internet version 4)
JMS	Java Message Service
JSON	JavaScript Object Notation (format de données textuelles dérivé de la notation des objets du langage JavaScript)
LDAP	Lightweight Directory Access Protocol (protocole d'accès aux annuaires)
MESR	Ministère de l'Enseignement Supérieur et de la Recherche
MDM	Master Data Management (gestion des données de référence)
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
MTAP	Mission Transverse d'Appui au Pilotage
NAT	Network Address Translation (mécanisme de translation d'adresses)
NTP	Network Time Protocol (protocole d'heure réseau)
NIST	National Institute of Standards and Technology (Institut national des normes et de la technologie)
OS	Operating System
P2D2	Projet de Dématérialisation et de Pilotage de la Dépense)
PD	Process Director
PDAP	Process Director Account
PGSI	Politique Générale de Sécurité de l'Information
PAQ	Plan Assurance Qualité
PAS	Plan Assurance Sécurité
PSSI	Politique de Sécurité des Systèmes d'Information
PSST	Pôle Santé et Sécurité au Travail
RENATER	REseau NAtional de télécommunications pour la Technologie, l'Enseignement et la Recherche
REST	REpresentational State Transfer

Sigle	Description
RFC	Requests For Comments (demande de commentaires)
RGAA	Référentiel général d'Accessibilité pour les Administrations
RGI	Référentiel Général d'Interopérabilité
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
RH	Ressources Humaines
SAE	Service d'archivage électronique
SAML	Security Assertion Markup Language (langage de balisage d'informations d'authentification)
SATT	Société d'accélération du transfert de technologies
SCAP	Security Content Automation Protocol (Protocole d'automatisation de contenu de sécurité)
SCD	Service Centralisé de la Dépense
SFC	Services Financier et Comptable
SGBD	Système de Gestion de Base de Données
SGCN	Secrétariat Général du Comité national
SI	Système d'Information
SMTP	Simple Mail Transfer Protocol (protocole simple de transfert de courrier)
SNMP	Simple Network Management Protocol (protocole simple de gestion de réseau)
SP	Service Provider (fournisseur de services)
SQL	Structured Query Language (langage de requête structurée)
SSH	Secure SHell
SSI	Sécurité des Systèmes d'Information
SSI	Service des Systèmes d'Information
SSL	Secure Socket Layer
SSO	Single Sign-On (authentification unique)
TLS	Transport Layer Security
VLAN	Virtual Local Area Network (réseau local virtuel)
VPN	Virtual Private Network (réseau privé virtuel)
W3C	World Wide Web Consortium
WAYF	Where Are You From
WCAG	Web Content Accessibility Guidelines (règles pour l'accessibilité des contenus Web)
XML	eXtensible Markup Language (langage de balisage extensible)
XSS	Cross Site Scripting

6.4.2 Glossaire

Le tableau suivant présente le glossaire des termes utilisés dans ce document.

Terme	Description
Authentification multi-facteurs	Méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN.
Document applicable	Document devant être obligatoirement appliqué par le Titulaire

Terme	Description
Document de référence	Document pouvant être utilement consulté par le Titulaire
EAI/ESB	Plateforme d'intermédiation des flux de données
Flux	Tout échange de données ou d'information entre deux briques applicatives (y compris services d'intermédiation), quelle que soit la modalité et forme de cet échange. Un flux peut être entièrement manuel, ou peut faire appel à des services web, ou peut passer par l'EAI/ESB, ou ……
LDAP	Protocole permettant l'interrogation et la modification des services d'annuaire.
REST	Style d'architecture d'échange de données autour de services web basés sur le protocole HTTP
Shibboleth	Mécanisme de propagation d'identités, développé par le consortium Internet2, qui regroupe 207 universités et centres de recherche. Pour toute information complémentaire se référer au site suivant : https://www.shibboleth.net/
Téléservice	Application destinée à la communication inter administration ou destinée à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public.