



**CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE**

DELEGATION CENTRE EST  
17 rue Notre Dame des Pauvres  
B.P. 10075  
54 519 VANDOEUVRE-LÈS-NANCY CEDEX

**PROCEDURE MAPA  
N°26.06.002**

**CREATION D'UNE APPLICATION D'ATTRIBUTION  
D'IDENTIFIANT UNIQUE D'ECHANTILLON (IGSN)  
POUR LA COMMUNAUTE INSU DU CNRS**

**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)**

---

# Table des matières

CAHIER DES CHARGES FONCTIONNEL DE L'OUTIL D'ATTRIBUTION D'IDENTIFIANT UNIQUE ECHANTILLON IGSN (DITE « APPLICATION IGSN »).  
POUR LA COMMUNAUTE INSU..... **Erreur ! Signet non défini.**

I.	CONTEXTE.....	4
1.1	Situation actuelle .....	4
1.2	Émergence du besoin.....	4
1.3	Outil existant.....	5
1.3.1	Système d'allocation d'IGSN du CNRS (www.igsn.cnrs.fr) .....	5
1.4	Acteurs concernés.....	5
II.	EXPRESSION DES BESOINS.....	6
2.1	Objectifs .....	6
2.2	Cadre d'utilisation du produit.....	6
2.3	Utilisateurs concernés.....	6
2.4	Caractéristiques du produit demandé .....	8
2.5	Périmètre du produit demandé .....	8
2.6	Échanges de flux entre le produit demandé et son environnement .....	9
2.7	Cycle de vie et état d'une déclaration d'identifiant échantillon.....	9
2.8	Ergonomie et respect des règles d'accessibilité .....	9
III.	DESCRIPTION FONCTIONNELLE DU BESOIN.....	11
3.1	Acteurs du système.....	11
3.1.1	Rédacteur .....	11
3.1.2	Contributeurs .....	11
3.1.3	Administrateurs .....	11
3.2	Fonctionnalités attendues .....	11
3.2.1	Gestion des droits d'accès des utilisateurs.....	11
3.2.2	Déclaration/modification/suppression d'identifiant échantillons .....	11
3.2.4	Gestion des étapes du cycle de vie d'un identifiant échantillon .....	12
3.2.5	Export des métadonnées d'un identifiant .....	12
3.2.6	Visualisation graphique (lecteurs, contributeurs) .....	12
3.3	Charte graphique .....	12
IV.	Exigences Non Fonctionnelles.....	13
4.1	Interfaces.....	13
4.1.1	Interface avec la CyberCarothèque nationale.....	13
4.1.2	Interface avec les plateformes de gestion physique d'échantillons .....	13

---

4.1.3 Interface avec le service d'authentification et SSO des établissements et organisme de l'enseignement supérieur et de la recherche. ....	13
4.2 Sécurité.....	13
4.3 Performances .....	15
4.4 Garantie apportée en termes de réutilisabilité du code et du logiciel .....	15
V. Développement, Déploiement, transfert de compétence.....	15
5.1 Développement.....	15
5.2 Déploiement.....	16
5.3 Transfert de compétences.....	16
5.3.1 Nature de la prestation .....	16
5.3.2 Livrables.....	16
VI. ARCHITECTURE.....	17
VII. Description de l'infrastructure hôte.....	18
VIII. CONTRAINTES .....	18
ANNEXE .....	19

---

# I. CONTEXTE

## 1.1 Situation actuelle

Missionnée par l'INSU en 2018, la DT INSU est devenue un nœud français (« *allocating agent* ») de l'International Generic Sample Number (IGSN), avec une vocation de service pour toute la communauté scientifique des sciences de la terre et de l'environnement. L'arrivée de l'IR RÉGEF dans le paysage national a conduit l'INSU en 2022 à transférer ces compétences à l'OSU OTELO et l'a missionné pour la création d'un service national d'attribution d'échantillon (IGSN) et opérer le nœud Français IGSN INSU à terme.

Les missions de base d'un nœud national de l'IGSN sont : (1) de permettre la déclaration d'échantillons pour l'obtention d'un numéro IGSN unique (*minting*) ; (2) de sauvegarder les métadonnées associées aux échantillons et mettre en place une page descriptive générale pérenne de l'échantillon dite : « *landing page* » où sont décrites les métadonnées associées à l'échantillon ; (3) de construire un portail interrogeable pour rendre les échantillons visibles et accessibles à la communauté. Chaque numéro d'identification IGSN débute par un préfixe (e.g., CNRS ou TOAE pour les déclarations actuelles).

La mise en place par la DT INSU de l'outil de déclaration d'échantillons du CNRS est le fruit d'un travail initié au début des années 2010. En 2018, sous le préfixe CNRS, des déclarations IGSN d'échantillons ont été initiées à travers l'outil SESAR (<https://www.geosample.org>) nœud américain de l'IGSN, alors que dans un second temps la DT INSU devenait nœud français de l'IGSN. Le préfixe TOAE (pour « Terre Océan Atmosphère Environnement ») a été créé en 2020 et est alors utilisé par la DT-INSU. L'outil de déclaration [igsn.cnrs.fr](https://www.igsn.cnrs.fr), mis en place en 2021 délivre des numéros d'identification IGSN uniques et opère avec les préfixes CNRS et TOAE. Les déclarations IGSN actuelles sont accessibles en ligne<sup>1</sup>.

## 1.2 Émergence du besoin

Face à l'enjeu central de la gestion des échantillons, qui touche l'ensemble de la communauté scientifique et a fortiori celle des géosciences et sciences de l'environnement, il est nécessaire de proposer à la communauté un service adapté d'attribution d'identifiant pérenne unique numérique aux échantillons et de gestion de leurs métadonnées. Aujourd'hui, la déclaration des échantillons sur [igsn.cnrs.fr](https://www.igsn.cnrs.fr) se fait par une interface homme-machine (IHM) pour un enregistrement isolé et est partiellement automatisée pour l'import en masse. L'import en masse peut être réalisé par l'utilisation de l'API REST avec un fichier XML, complété avec les métadonnées de chacun des échantillons faisant l'objet de la déclaration, par un utilisateur enregistré au préalable. Les échantillons ainsi déclarés sont consultables sur la page <https://www.igsn.cnrs.fr>, avec les métadonnées associées visibles sur des pages individuelles (« *landing pages* »). Les métadonnées des échantillons peuvent être complétées, corrigées et mises à jour par la même procédure. Cet outil est déjà très utilisé par certaines équipes de recherche environ 15000 déclarations à ce jour). Cependant, les métadonnées associées actuellement ne couvrent pas l'entièreté des besoins des communautés INSU. De plus, pour une utilisation à grande échelle par les communautés INSU il est nécessaire de penser un outil numérique

---

<sup>1</sup> <https://www.igsn.cnrs.fr>

---

plus optimisé et évolutif. L'outil devra donc s'appuyer sur le cadre de déclaration échantillons existant proposé par IGSN et l'enrichir de métadonnées disciplinaires.

### **1.3 Outil existant**

#### **1.3.1 Système d'allocation d'IGSN du CNRS ([www.igs.n.cnrs.fr](http://www.igs.n.cnrs.fr))**

La DT INSU mis en place et assure le fonctionnement de l'instance d'attribution des IGSN du CNRS dont voici les fonctionnalités actuellement opérationnelles :

- Authentification locale
- Comptes individuels
- Création des comptes réalisée par l'administrateur
- Possibilité de modifier les métadonnées d'un échantillon par la personne qui l'a créé
- Enregistrement d'un identifiant échantillon en ligne via une interface web
- Enregistrement « en masse » via API REST (fournir un fichier XML) et via fichier XLS avec possibilité de mettre à jour ou en deprecated (statut d'un échantillon non mis à jour ou détruit)
- Possibilité de télécharger un fichier XLS avec la liste des échantillons recherchés/trouvés
- Validation en ligne pour le fichier XLS
- Possibilité de lister ses fichiers XLS transmis avec le fichier résultat XLS
- Possibilité de lister ses échantillons avec possibilité de recherche / export XLS dans les résultats
- Recherche de codes par carte / texte. (ex : La recherche textuelle (croisée) concerne les champs : code IGSN, nom de l'échantillon, type d'échantillon, commentaire, lieu de stockage, contact du lieu de stockage...)
- Implémentation du Protocole OAI-PMH
- Possibilité de forcer un code IGSN (utilisation d'un autre préfixe que CNRS ou TOAE).

### **1.4 Acteurs concernés**

- Le Groupe de Travail Échantillon de RéGEF
  - Les communautés scientifiques en sciences de la terre et de l'environnement, via les Commissions Spécialisées de l'INSU (CS-INSU, qui sont pluriorganismes)
  - Le Groupe de Travail Géothèques et, plus largement la communauté des responsables/gestionnaires (ITA, ITRF, etc.) de matériels d'étude et de collections.
-

## II. EXPRESSION DES BESOINS

### 2.1 Objectifs

Le projet a pour but de proposer à la communauté scientifique une **application** de deuxième génération qui permettra de :

- Déclarer des identifiants échantillons pour toutes les communautés INSU potentiellement concernées (IGSN, avec déclarations individuelles ou groupées)
- Corriger et mettre à jour les métadonnées des échantillons déclarés
- Héberger les landing pages des échantillons
- Être interopérable avec les dispositifs existants ou à venir (Cyber Carothèque Nationale, Recolnat ...)
- Cartographier les échantillons déclarés
- Rechercher des échantillons et les filtrer (type, lieu, ...)
- Implémenter et utiliser des listes de vocabulaire contrôlées pour la déclaration d'échantillon ;
- Implémenter et utiliser des thésaurus validés par la communauté scientifique pour les métadonnées spécifiques à chaque typologie d'échantillon
- Extraire des contenus sous format JSON afin de faciliter la constitution de différents types de documents (publication, bibliographie ...)
- Être accessible à l'ensemble de la communauté, y compris chercheurs individuels ou autres acteurs (projets, campagne, repositories, laboratoires, etc.)
- Être flexible et évolutif.

### 2.2 Cadre d'utilisation du produit

L'utilisation de l'application doit être simple et accessible à l'ensemble de la communauté des sciences de la terre et de l'environnement. La déclaration d'identifiant unique échantillons avec les métadonnées associées favorisant leur trouvabilité, accessibilité, interopérabilité, réutilisation (selon les principes FAIR<sup>2</sup>) et utiliser les standards internationaux.

L'application permettra de suivre les déclarations d'identifiant échantillons à des fins de suivi des activités par la gouvernance de l'INSU.

Elle devra assurer un lien avec la gestion physique de collections d'échantillons.

### 2.3 Utilisateurs concernés

Les utilisateurs concernés seront :

- Les personnes impliquées dans la collecte et le traitement d'échantillons
- Les chercheurs et équipes scientifiques souhaitant rechercher un échantillon existant via l'application

---

<sup>2</sup> <https://www.go-fair.org/fair-principles/>

---

- Les organismes, universités et les autres institutions, groupements de chercheurs, responsable d'entrepôt de données (e.g., chercheur individuel, lithothèques, laboratoires, projets, campagnes, etc.)
- Les membres du GT Échantillons IGSN et l'INSU pour le pilotage.

## 2.4 Caractéristiques du produit demandé

L'application permettra les actions suivantes :

- 1 Une authentification simplifiée par Fédération d'identité, ProConnect, ORCID basée sur le SSO de Gaia Data
- 2 La gestion des accès, rôles et droits des utilisateurs
- 3 La gestion de groupes d'utilisateurs
- 4 La gestion de déclaration « brouillon » par profil utilisateur
- 5 L'accès aux déclarations d'échantillons en cours d'élaboration aux seules personnes accréditées et authentifiées
- 6 La pré-réservation de plages de code IGSN (e.g., campagnes océanographiques ou missions terrain sans accès internet et besoins de gestion d'échantillons sur le terrain)
- 7 La déclaration, modification, suppression (deprecated) d'identifiant échantillons par saisie manuelle ou assistée (masque de saisie, listes de choix), contrôlée et autorisée
- 8 La déclaration, modification, suppression (deprecated) d'identifiant échantillons par utilisation d'API, contrôlée et autorisée
- 9 La déclaration, modification, suppression (deprecated) d'identifiant de sous-échantillons.
- 10 La recherche d'échantillon avec filtrage (type, lieu, responsable technique, scientifique...)
- 11 L'extraction des contenus afin de faciliter la constitution de différents types de documents (par exemple : fiche de suivi de déclaration échantillons) par API
- 12 Permettre le moissonnage des données échantillons via API (Protocole standardisé, OAI-PMH ...)
- 13 Une interface multilingue, avec support a minima du français et de l'anglais et possibilité d'ajouts ultérieurs d'autres langues
- 14 L'export des données au format JSON dans le respect du maintien de l'authentification (respectant des schémas de métadonnées Internationaux comme Datacite, ...);
- 15 La conformité aux normes d'accessibilité définies par le World Wide Web Consortium.
- 16 Possible point à ajouter : possibilité de prendre la main (par l'administrateur du service ?) sur des déclarations/métadonnées (cas de retraites, personnes non plus dans le système etc -> afin d'assurer le management à long terme des métadonnées
- 17 La possibilité d'attacher des documents annexes (plus complets) pour la description d'une série d'échantillons (conditions de terrain, etc .. ).

## 2.5 Périmètre du produit demandé

- L'application ne permettra pas de gérer les collections d'échantillons, toutefois elle implémentera des protocoles standardisés d'échange pour garantir l'interopérabilité avec des applications de gestion de collection.
-



## 2.6 Échanges de flux entre le produit demandé et son environnement

L'application sera accessible via des API pour permettre l'attribution d'identifiants pour le compte de dispositifs existants, tels que la [Cyber Carothèque Nationale](#). Il est toutefois souhaité que des fonctionnalités d'export pour intégration dans des outils tiers dépourvus d'API puissent être proposés.

## 2.7 Cycle de vie et état d'une déclaration d'identifiant échantillon

Déclaration/modification/suppression d'un identifiant échantillon :

### 1- Déclaration d'un identifiant échantillon

- Réalisée par le rédacteur : création de la fiche, de son profil et de la liste des contributeurs/lecteurs

### 2- Modification d'un identifiant échantillon

- [Etat « en cours de déclaration »] tant que le rédacteur et les contributeurs n'ont pas achevé la saisie/modification
- [Etat « Finalisé »] quand l'utilisateur et les contributeurs ont fini la saisie et que les champs obligatoires ont été renseignés (contrôle automatique).
- [Etat « déclaration identifiant »] attribution d'un identifiant échantillon, création d'une landing page associée et envoi d'un mail préconfiguré à tous les participants (rédacteur, contributeurs, administrateur)
- [Etat « déclaration identifiant avec embargo »] attribution d'un identifiant échantillon, création d'une landing page associée non publiée (non accessible par tout le monde) et envoi d'un mail préconfiguré à tous les participants (rédacteur, contributeurs, administrateur). Embargo positionné par défaut à 2ans prolongeable.
- Si la déclaration « brouillon » n'est pas finalisée et non modifiée durant 1 mois : le rédacteur et les contributeurs reçoivent un mail de rappel de finalisation.

### 3- Suppression (deprecated) d'un identifiant échantillon

- Possibilité de suppression (deprecated) d'une fiche par un rédacteur ou un administrateur

Un schéma de ce cycle de vie est fourni en annexe.

## 2.8 Ergonomie et respect des règles d'accessibilité

L'ergonomie de l'application devra faciliter sa prise en main :

- Chaque bouton devra indiquer l'action qui lui est associée, soit au travers de son libellé, soit au travers d'une info-bulle
- Les actions ayant un résultat risqué ou irréversible comme la suppression d'un identifiant devront être précédées d'une étape de validation.

Une adaptation de l'ergonomie à la taille de l'écran pour un smartphone ou une tablette (Responsive design) devra être implémentée.

L'application devra également se conformer au minimum au niveau A des règles internationales pour l'accessibilité des contenus Web (WCAG) 2.1.

---

L'application devra proposer une documentation détaillée et des tutoriels accessibles sur son site web.

## III. DESCRIPTION FONCTIONNELLE DU BESOIN

### 3.1 Acteurs du système

Les utilisateurs de l'application se répartissent en 3 catégories :

#### 3.1.1 Rédacteur

Qui : La communauté française impliquée dans la gestion des échantillons en science de la terre et environnement.

Rôles et droits : Les rédacteurs (Individuels et autres) déclarent un ou plusieurs identifiants échantillons. Ils créent et modifient le contenu des métadonnées de chaque échantillon dont ils ont la responsabilité. Ils attribuent pour chaque identifiant les droits à des contributeurs. Ils peuvent supprimer (deprecated) les identifiants qu'ils ont créés.

#### 3.1.2 Contributeurs

Qui : Une ou plusieurs personnes d'un groupe, gérant le ou les identifiant(s) échantillons.

Rôles et droits : Les contributeurs peuvent modifier, ajouter, supprimer (deprecated) des métadonnées liées à la déclaration d'un identifiant échantillon.

#### 3.1.3 Administrateurs

Qui : Les responsables techniques de l'application.

Rôles et droits : Les administrateurs peuvent accéder et gérer tous les identifiants échantillons. Ils gèrent aussi les préfixes.

Possibilité d'établir des nouveaux préfixes.

### 3.2 Fonctionnalités attendues

#### 3.2.1 Gestion des droits d'accès des utilisateurs

##### *a. Gestion des accès des utilisateurs*

La connexion sera réalisée par login et mot de passe à partir de la page d'accueil.

L'authentification utilisateur sera possible à minima via l'authentification partagée ORCID et la fédération d'identités Renater (basée sur le SSO de Gaia Data ), ProConnect ainsi que par des logins/mdp individuels ou de groupe.

##### *b. Gestion des droits des utilisateurs*

L'application permettra de saisir les données administratives concernant les utilisateurs.

Elle permettra au rédacteur ou l'administrateur de valider les rôles (rédacteur, contributeur) et droits qui sont préalablement sélectionné par l'utilisateur.

#### 3.2.2 Déclaration/modification/suppression d'identifiant échantillons

Le rédacteur pourra déclarer un nouvel identifiant échantillon vierge ou issue de l'import d'un template tabulaire/XML/XLS/JSON (à définir). Le rédacteur et/ou le(s) contributeur(s) pourront modifier cet identifiant.

L'application proposera un module de saisie.

---

La saisie sera manuelle et/ou assistée : par des listes de choix dont les valeurs seront gérées dans les tables de valeur correspondantes ou par l'implémentation de référentiels existants.

Le module de saisie sera dynamique et sera généré en fonction des métadonnées générales et spécifique préalablement sélectionnées par l'utilisateur issues de tables de valeurs et référentiels sélectionnés.

Seuls le rédacteur et les administrateurs pourront supprimer (deprecated) un identifiant échantillon.

### **3.2.3 Déclaration/modification/suppression de valeurs dans les tables de valeurs**

Les tables de valeurs doivent être modifiables par l'administrateur (par exemple : roche, eau, sol, poudre ...).

### **3.2.4 Gestion des étapes du cycle de vie d'un identifiant échantillon**

L'identifiant échantillon suivra le cycle de vie suivant :

- 1- En cours de déclaration
- 2- Modification
- 3- Validation de déclaration d'un identifiant.

### **3.2.5 Export des métadonnées d'un identifiant**

Les métadonnées d'un ou plusieurs identifiants devront pouvoir être exportées dans un format pivot structuré de type JSON ou XML.

### **3.2.6 Visualisation graphique (lecteurs, contributeurs)**

L'application proposera aux lecteurs et contributeurs une visualisation des identifiants permettant une sélection et un filtrage selon plusieurs critères de métadonnées (type, localisation...).

## **3.3 Charte graphique**

L'application devra s'appuyer sur la charte graphique définie et validée par le comex RéGEF.

## IV. Exigences Non Fonctionnelles

### 4.1 Interfaces

#### 4.1.1 Interface avec la CyberCarothèque nationale

L'application devra assurer une interopérabilité avec la plateforme de la Cyber Carothèque Nationale via l'utilisation de l'API REST avec authentification pour automatiser les déclarations IGSN. Les spécificités techniques de la plateforme sont assurées par l'OASU-EPOC de bordeaux qui collaborera étroitement dans le cadre de ce projet sur le périmètre indiqué.

#### 4.1.2 Interface avec les plateformes de gestion physique d'échantillons

L'application devra assurer une interopérabilité avec l'infrastructure de recherche ReCOLNAT qui assure la gestion physique d'une partie des échantillons de l'INSU. Le MNHN fournira les attendus techniques à cet interfaçage.

#### 4.1.3 Interface avec le service d'authentification et SSO des établissements et organisme de l'enseignement supérieur et de la recherche.

Le système d'authentification et de SSO de Gaia Data est construit sur la solution Keycloak (<https://www.keycloak.org/>). Cette solution fournit des protocoles d'authentification standards tels que l'OpenID Connect, OAuth 2.0 ou le SAML. L'application IGSN s'appuiera sur ce service pour l'ensemble des étapes de la gestion d'un compte utilisateur (création, authentification, modération, autorisations, expiration, suppression). L'application devra s'appuyer sur un des standards proposés par Keycloak, préférentiellement OIDC, pour gérer l'authentification des utilisateurs et les autorisations d'accès aux ressources.

### 4.2 Sécurité

Il devra être mis en œuvre des mesures de sécurité rigoureuses tout au long du processus de développement et de déploiement de l'application afin d'assurer la protection des données et des utilisateurs contre les menaces potentielles.

#### Principes DevSecOps, Privacy By Design

Le développement de l'application devra suivre les principes de DevSecOps pour intégrer la sécurité dès les premières étapes du cycle de développement logiciel.

- Intégrer des contrôles de sécurité automatisés dans les pipelines CI/CD pour détecter et corriger les vulnérabilités dès qu'elles sont introduites.
  - Mettre en place des pratiques de gestion de la configuration sécurisée pour assurer la conformité aux politiques de sécurité.
  - S'assurer que tous les membres de l'équipe de développement sont sensibilisés aux bonnes
-

pratiques de sécurité et suivent les processus définis.

Le développement de l'application devra également s'inscrire dans le concept fondamental de Privacy By Design (PbD) qui vise à intégrer la protection de la vie privée dès la conception des systèmes, des applications et des processus. L'approche Privacy by Design implique d'anticiper et d'intégrer les principes de protection de la vie privée à chaque étape du cycle de vie du projet, renforçant ainsi la confiance des utilisateurs et assurant leur protection tout au long de leur expérience sur la plateforme.

- Collecte minimale de données personnelles.
- Sécurisation des données sensibles.
- Transparence dans la gestion des informations des utilisateurs.
- Prise en compte des préférences de confidentialité des utilisateurs.
- Évaluation continue des risques liés à la confidentialité.
- Mesures proactives pour atténuer les risques tout au long de la durée de vie du portail web.

### **Sécurisation des échanges de données, chiffrement des données**

Il devra être garanti que toutes les données sont chiffrées en transit et au repos conformément aux normes de sécurité du cadre réglementaire PPST, PSSIE, RGPD, NIS 2.

- Sécuriser les flux d'échange de données en utilisant la dernière version de TLS et en s'assurant de sa bonne configuration et mise en œuvre.
- Rendre l'utilisation de TLS obligatoire sur toutes les pages.
- Utilisation d'algorithmes de chiffrement robustes pour le chiffrement des données.
- Gestion sécurisée des clés de chiffrement pour assurer la confidentialité des données.
- Utilisation de bonnes pratiques de protection des données conformes aux normes de confidentialité et de protection des données en vigueur.

### **Protections contre les attaques**

Il devra être mis en œuvre des mesures de sécurité conformes aux meilleures pratiques reconnues, notamment à minima les principes du Top 10 OWASP (Open Web Application Security Project), afin de garantir la sécurité de l'application contre les attaques potentielles.

### **Tests de sécurité**

Le Titulaire devra effectuer les types suivants de tests de sécurité pour évaluer la robustesse du portail web et identifier les vulnérabilités potentielles :

- **Tests Dynamiques d'Application (DAST)** : Effectuer des analyses automatisées de sécurité des applications web en simulant des attaques externes pour identifier les failles de sécurité.
  - **Tests Statiques d'Application (SAST)** : Analyser statiquement le code source du portail web pour détecter les vulnérabilités de sécurité, les mauvaises pratiques de codage et les erreurs de configuration.
  - **Tests Intégrés d'Application (IAST)** : Utiliser des outils intégrés dans l'application en cours d'exécution pour détecter les vulnérabilités en temps réel et fournir des informations sur les attaques potentielles.
  - **Tests Software Composition Analysis (SCA)** : Analyser les dépendances logicielles pour identifier les composants avec des vulnérabilités connues.
-

Il devra être fourni des rapports détaillés sur les résultats de ces tests de sécurité, y compris le cas échéant les vulnérabilités détectées et les mesures correctives appliquées.

- Exigences du site hébergeur : cf **Erreur ! Source du renvoi introuvable.** (article VII).

#### 4.3 Performances

L'application devra être à l'état de l'art et ne doit pas imposer de latence supérieure à 1 seconde pour les requêtes utilisateurs.

Elle devra donc être scalable sur un environnement de type cloud. Pour cet objectif, les composants logiciels de l'application pourront être containerisés. Les recettes de déploiements devront être fournies pour pouvoir être implémentées sur des environnements virtuels ou sur des orchestrateurs de containers comme Kubernetes.

#### 4.4 Garantie apportée en termes de réutilisabilité du code et du logiciel

Le Titulaire devra proposer des actions de réversibilité (i.e. permettant une tierce maintenance applicative) à l'issue de la phase de livraison finale

Le logiciel fourni devra être open source sous licence CC-BY-NC-SA ou équivalente.

La réutilisation de composants open source (avec une communauté vaste et active) sera à privilégier par rapport à des développements à façon ou des composants commerciaux.

## V. Développement, Déploiement, transfert de compétence

### 5.1 Développement

Le développement sera réalisé en mode agile.

Un Product Owner sera désigné côté OSU OTELo pour assurer la vision et la stratégie du produit application recherche et attribution IGSN dite 'application IGSN'. Il travaillera avec les clients et autres parties prenantes.

Définition clients et autres parties prenantes : (i.e. qui oriente de haut niveau).

Parties prenantes :

- Equipe 'application IGSN'
- Coordinateur technique
- Les personnes impliquées dans la collecte et le traitement d'échantillons ;
- Les chercheurs et équipes scientifiques souhaitant rechercher un échantillon existant via l'application

Client :

- Le Groupe de Travail Échantillon de REGÉF
  - Les communautés scientifiques des sciences de la terre et de l'environnement
-

## 5.2 Déploiement

La solution devra être régulièrement déployée sur l'infrastructure composée d'environnement de développement, de pré-production et de production. (intégration continue)

## 5.3 Transfert de compétences

### 5.3.1 Nature de la prestation

- une description de l'environnement technique et logiciel de l'application IGSN,
- la fourniture d'une compilation des documentations complètes sur support électronique ainsi que toute information pertinente pour avoir une "photographie" fidèle du système au moment de la livraison.

### 5.3.2 Livrables

#### Phases du projet :

- Prototype initial attendu à M0 + 3 mois. (MVP : Minimum viable product)

Implémentation des caractéristiques 1,2,3,5,7,10

- Première version déployable (V1) à M0 + 6 mois.

Implémentation des caractéristiques 4,6,8,9,12,13

- Version finale avec toutes les fonctionnalités (V2) à M0 + 12 mois.

Implémentation des caractéristiques restantes 11,14,15,16,17

Ce planning est indicatif, le soumissionnaire pourra proposer un ajustement.

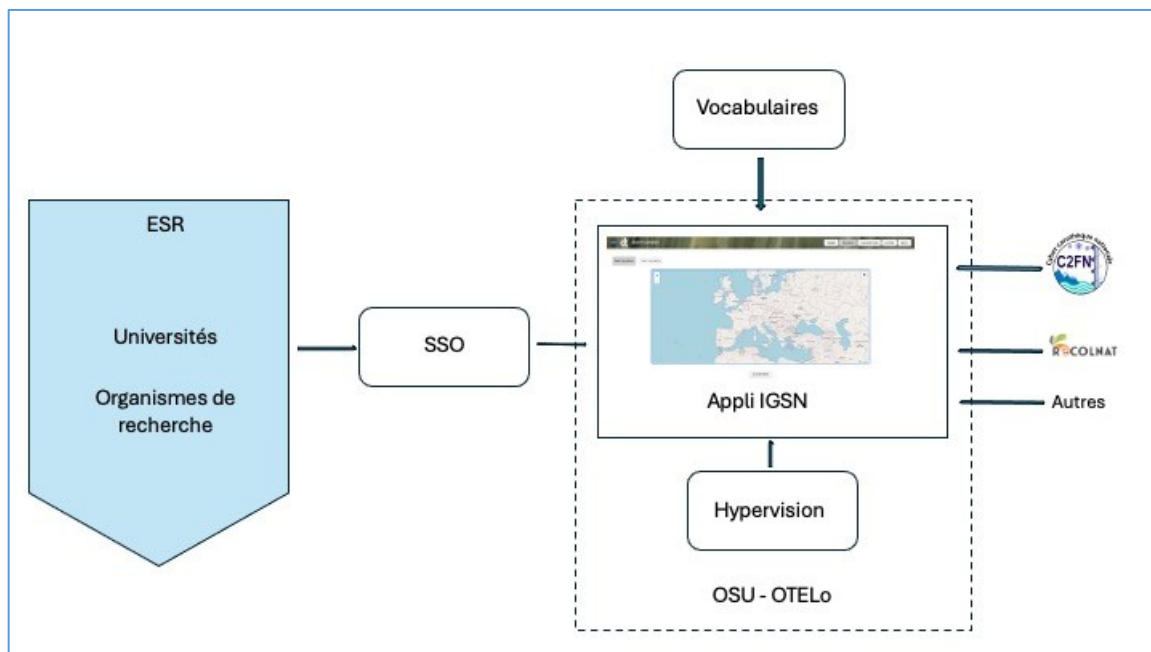
Le soumissionnaire s'engage à fournir :

- transfert des informations fonctionnelles et techniques sur le système (documentations fonctionnelle et technique complètes, composants logiciels sources et exécutables des applicatifs, état des versions des progiciels, outils et utilitaires en exploitation) à jour et cohérents avec la version en exploitation,
  - transfert des compétences fonctionnelles et techniques sur le système. Le prestataire devra prévoir pour cela une journée dans les locaux d'OTELo.
-



## VI. ARCHITECTURE

### 6.1 Architecture générale de l'« applicationIGSN »



#### Sur la gauche :

L'ensemble de la communauté scientifique susceptible d'interroger l'application IGSN via l'IHM ou l'API.

Le SSO est géré par les établissements hébergeur des personnels de la communauté ou via ORCID. L'implémentation d'un WAYF (Where are you from) sera intégrée à l'application ou fournie par Renater.

#### Sur la droite :

Les vocabulaires seront fournis par des serveur de vocabulaire (<https://terra-vocabulary.org/ncl/> et <https://earthportal.eu/>) ou par les pôles de données de DataTerra La communauté scientifique soumettant des listes de vocabulaires qui sont validées par les pôles. (GT Métadonnées RéGEF). Il sera également fait appel à des référentiels internationaux (ROR, SPDX...).

[Le serveur d'Hypervision et l'hébergement de l'application IGSN sera assuré par l'OSU OTELo \(cf détails dans la partie VII\)](#)

[La plateforme de la cyber carothèque nationale ainsi que l'infrastructure ReCOLNAT seront interconnectés à l'application.](#)

Le prestataire devra fournir et détailler dans sa réponse le niveau d'expertise du développeur dans chacune des technologies proposées (Connaissance-Notion / Maîtrise / Expertise), accompagné d'exemples d'expériences attestant des compétences ainsi que des années d'expérience du développeur dans les principales technologies. Des exemples de projets, précédemment réalisés, utilisant les technologies proposées, devront être également fournis.

## VII. Description de l'infrastructure hôte

L'appli IGSN sera hébergé sur l'infrastructure de l'OSU OTELo. Le site fournira une infrastructure informatique d'hébergement permettant :

- d'opérer des services web accessibles depuis internet. Cette infrastructure d'hébergement comprendra :
  - un système de virtualisation compatible avec l'exploitation de services containerisés ou directement un orchestrateur de containers type kubernetes
  - un accès à internet à 10GBps permettant d'exposer les services du portail
  - un système de stockage HDD ou flash pour les bases de données
  - des services de reverse proxy sous Apache
  - des services de bases de données PostGreSQL, MariaDB ou MongoDB. Les configurations permettant la haute disponibilité et la sauvegarde des bases de données pourront être intégrées dans la solution proposée.
- de mettre en place les différents niveaux de sécurité pré-requis et spécifiques à l'application IGSN
- de mettre en œuvre un plan de continuité d'activité et un plan de reprise d'activité en cas de défaillance de l'infrastructure d'hébergement ou d'attaque et corruption du service.
- d'accéder au service d'authentification et de SSO de l'ESR, ProConnect et ORCid
- D'assurer les métriques de contrôle et de supervision de l'application.

## VIII. CONTRAINTES

1- Le code de l'application devra être déposé dans un entrepôt public et disposer d'une licence ouverte de type CC-BY.

2- L'application devra être fournie avec toute la documentation nécessaire à son déploiement dans un centre de données. L'utilisation d'une méthode dite de « conteneurisation » de type Docker sera privilégiée.

3- L'application devra être déclarée et conforme aux règles du RGPD. Elle en affichera les mentions de manière explicite sur le site.

---

## ANNEXE

### Cycle de déclaration/modification d'un identifiant échantillon

