|  |  |
| --- | --- |
| |  | | --- | | Clear Space  Spécifications Interfaces | |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | **Nom** | **Fonction** | **Date** | **Signature** | | **Rédaction** | Tripartite | Equipe de réalisation |  |  | | **Vérification** |  | Responsable Qualité |  |  | | **Approbation** |  | Chef de Projet |  |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference :** | **CDSICYBER-DD-25007** | **Classification :** | **Non Protégé** |
| **Edition :** | **00** | **Statut :** | **En cours** |
| **Révision :** | **01** | **Date :** | **11/03/2025** |

Table des matières

[1 Introduction 6](#_Toc199952150)

[1.1 Objet du document 6](#_Toc199952151)

[1.2 Présentation du projet 6](#_Toc199952152)

[1.3 Organisation du document 6](#_Toc199952153)

[2 Référentiel documentaire 7](#_Toc199952154)

[2.1 Documents applicables 7](#_Toc199952155)

[2.2 Documents de référence 7](#_Toc199952156)

[2.3 Abréviations 7](#_Toc199952157)

[3 Interface entre un poste de travail et le système de détections radar embarqué 8](#_Toc199952158)

[3.1 Objet du chapitre/Principe 8](#_Toc199952159)

[3.2 Accès au web serveur de plots radar 8](#_Toc199952160)

[3.2.1 Initialisation du VPN 8](#_Toc199952161)

[3.2.2 Utilisation du VPN 10](#_Toc199952162)

[3.3 Accès à la cartographie nécessaire via internet 10](#_Toc199952163)

[4 Interface entre un poste de travail et le système de visualisation de preuves 11](#_Toc199952164)

[4.1 Objet du chapitre/Principe 11](#_Toc199952165)

[4.2 Interface entre un poste de travail et le système de visualisation de preuves 11](#_Toc199952166)

[5 Interface entre un poste de travail et un ou des systèmes LAD fixes distants 12](#_Toc199952167)

[5.1 Objet du chapitre/Principe 12](#_Toc199952168)

[5.2 Interface entre un poste de travail et un ou des systèmes lad fixes 12](#_Toc199952169)

[5.3 Accès à la cartographie nécessaire via internet 12](#_Toc199952170)

[6 Interface entre un poste de travail et un ou des système LAD embarqués 13](#_Toc199952171)

[6.1 Objet du chapitre/Principe 13](#_Toc199952172)

[6.2 Interface entre un poste de travail et un ou des systèmes lad embarqués 13](#_Toc199952173)

[6.2.1 Initialisation du VPN 13](#_Toc199952174)

[6.2.2 Utilisation du VPN 13](#_Toc199952175)

[6.3 Accès à la cartographie nécessaire via internet 14](#_Toc199952176)

[7 Interface entre les différents outils de détections et le système d’ancrage de preuves dans la blockhain 15](#_Toc199952177)

[7.1 Objet du chapitre/Principe 15](#_Toc199952178)

[7.2 Interface entre le logiciel SMDR2 et le système d’ancrage blockchain 15](#_Toc199952179)

[7.2.1 Documentation de l’API 17](#_Toc199952180)

[7.3 Interface entre le système lad embarqué et le système de blockchain 17](#_Toc199952181)

[7.4 Interface entre le ou les systèmes lad fixes et le système de blockchain 18](#_Toc199952182)

Liste des Tables

**Aucune entrée de table d'illustration n'a été trouvée.**

Historique du document

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Paragraphes modifiés** | **Observations** |
| 0.1 | 11/03/2025 |  | Draft initial |
|  |  |  |  |

# Introduction

## Objet du document

Le présent document contient les spécifications des interfaces système du projet Clear Space.

Il décrit principalement les paramétrages, configurations et échanges de données nécessaires et autorisées pour le bon fonctionnement en réseau entre les différents constituants du système pour les accès, les échanges de données, les affichages déportés … mais aussi des éventuels besoins d’accès à des sites internet spécifiques (récupération de la cartographie numérique par exemple).

Ce document ne décrit pas la sécurisation du système, en d’autres termes simplistes ce qui n’est pas strictement nécessaire donc « verrouillé ».

Le système est constitué du véhicule de surveillance SMDR2 et ses composants fonctionnels principaux incluant un sous-système de LAD embarqué, du ou des systèmes de LAD fixes, du système d’ancrage blockchain, d’un accès à internet pour chacun de ces systèmes via des réseaux filaires ou sans fil.

## Présentation du projet

Le projet Clear Space consiste à être capable de constituer des preuves informatiques, infalsifiables de détections de drone ou de mouvements d’intrus dans des zones où ces présences sont interdites.

## Organisation du document

Le document est structuré comme indiqué ci-après :

* Chapitre 1 : Introduction
* Chapitre 2 : Référentiel documentaire
* Chapitre 3 : Interface entre un « poste de travail » et le système de détections radar embarqué
* Chapitre 4 : Interface entre un « poste de travail » et le système de visualisation de preuves
* Chapitre 5 : Interface entre un « poste de travail » et un ou des systèmes LAD fixes distants
* Chapitre 6 : Interface entre un « poste de travail » et un ou des systèmes LAD embarqués
* Chapitre 7 : Interface entre les différents outils de détections et le système d’ancrage de preuves dans la blockchain

NB : On sous-entend ci-dessus dans la dénomination « poste de travail » le fait qu’il soit indifférencié entre le poste de travail embarqué dans un véhicule et un poste de travail fixe.

# Référentiel documentaire

## Documents applicables

|  |  |  |
| --- | --- | --- |
|  | Cahier des charges CDSICYBER-DD-25006 1.0 |  |

## Documents de référence

|  |  |  |
| --- | --- | --- |
|  |  |  |

## Abréviations

|  |  |
| --- | --- |
| **Abréviation** | **Signification** |
| **ACU** | A Confirmer Ultérieurement |
| **ADU** | A Définir Ultérieurement |
| **AIS** | Automatic Identification System |
| **COM** | COMmunications |
| **CD SIC** | Cegelec Défense Systèmes d’Information et Cybersécurité |
| **FAI** | Fournisseur d’Accès Internet |
| **IVV** | Intégration Vérification et Validation |
| **KVM** | Keyboard Video Mouse |
| **LAD** | Lutte Anti-Drone |
| **LITIS** | Laboratoire d'informatique, de traitement de l'information et des systèmes |
| **OS** | Operating System |
| **PC** | Personal Computer |
| **RF** | Radio Fréquence |
| **SMDR2** | Système Mobile de Détection et de Renseignement de 2nd génération |
| **SSI** | Sécurité des systèmes informatiques |
| **TAM** | Terre Air Mer |
| **UC** | Unité Centrale |
| **URL** | Uniform Resource Locator |
| **VPN** | Virtual Private Network |

# Interface entre un poste de travail et le système de détections radar embarqué

## Objet du chapitre/Principe

Ce chapitre décrit ce qui est nécessaire pour afficher via un navigateur internet un fond cartographique et l’affichage géolocalisé des plots radar correspondant aux détections effectuées à bord du véhicule sur ce fond.

Ce navigateur peut être lancé à bord du véhicule ou sur un poste de travail distant connecté au VPN via internet.

Avant de tester cette interface, le véhicule n’étant pas toujours connecté, contacter le 02 32 63 59 47.

## Accès au web serveur de plots radar

Le web server SMDR2 (PC Windows) est localisé à bord du véhicule, et est compris dans le réseau local du modem 4G/5G à bord du SMDR2. Il est donc nécessaire, afin d’y accéder, d’être connecté au réseau VPN associé au véhicule, d’avoir l’adresse IP associée au Serveur Web, ainsi que le port utilisé (51911). La redirection de ports dans le réseau du véhicule s’occupera du reste (NAT).

Dans le cadre du projet Clearspace, utilisez :

**192.168.32.61:51911**

Le mot de passe à utiliser est :

**Radar2025CSP!**

La connexion est valable 4 heures.

Afin d’être homogène avec les autres pages web, testé avec le navigateur Microsoft « Edge ».

Les accès peuvent avoir lieu en parallèle depuis plusieurs postes de travail.

### Initialisation du VPN

Une entité représente un acteur de ce projet.

La liste des entités actuelles est :

* Drone XTR
* LITIS
* Cegelec Défense

Afin d’assurer l’intégrité et la confidentialité des données transmises, il est également nécessaire au préalable de se connecter par VPN (Wireguard) avec le véhicule (si à l’extérieur du réseau local du véhicule).

Le VPN fonctionne en peer to peer, c’est-à-dire sans intermédiaire. Chaque entité dans ce réseau VPN aura une paire de clé privée (permettant de déchiffrer) et publique (permettant de chiffrer), définie selon une configuration fournie par Cegelec Défense. Cette configuration nommée « ClearSpace-[*nom\_entité*]-[version\_véhicule]-[identifiant\_véhicule].conf » sera contenue dans un fichier zip nommé « ClearSpace-[*nom\_entité*]-[*version\_véhicule*]-[*identifiant\_véhicule*].zip » (exemple : Clearspace-LITIS-SMDR2-01.zip). Le fichier de configuration sera sous cette forme :

[Interface]

PrivateKey = XXXXXXX

Address = Y.Y.Y.Y/24

DNS = 8.8.8.8

[Peer]

PublicKey = ZZZZZZZ

AllowedIPs = 0.0.0.0/0

Endpoint = clearspace.ddns.net:51820

Les valeurs XXXXXX, ZZZZZZ et l’adresse Y.Y.Y.Y seront fournis directement dans le fichier, et à ne pas modifier.

Afin de le mettre en place, il faut sur un PC Windows connecté sur un compte administrateur :

* Télécharger Wireguard
* Installer Wireguard
* Exécuter Wireguard
* Cliquer sur « Ajouter le tunnel »
* Sélectionner dans la fenêtre de l’explorateur de fichier le fichier zip fourni par Cegelec Défense (ClearSpace-[*nom\_entité*]-[*version\_véhicule*]-[*identifiant\_véhicule*].zip).

Chaque entité peut utiliser ce fichier de configuration sur autant de machine qu’elle le souhaite.

**Attention : Chaque entité ne peut connecter simultanément qu’une seule machine.**

### Utilisation du VPN

Afin de démarrer le VPN, il faut être connecté sur un compte administrateur sur la machine windows et :

* Lancer l’application Wireguard
* Sélectionner le bon tunnel (celui dont le nom correspond au véhicule désiré)
* Cliquer sur le bouton activer

A partir d’ici, les serveurs à bord du véhicule sont accessibles.

## Accès à la cartographie nécessaire via internet

Afin d’afficher correctement le fond cartographique, le client a besoin d’avoir accès au domaine de OpenStreetMap (**https:/ /tile-openstreetmap.org**) car la page internet vient y récupérer des ressources nécessaires. Il ne faut pas configurer une interdiction sur cette URL.

# Interface entre un poste de travail et le système de visualisation de preuves

## Objet du chapitre/Principe

Ce chapitre décrit ce qui est nécessaire pour afficher via un navigateur internet la plateforme de visualisation des preuves juridiques issues des détections SOL ou LAD (fonctionnement identique pour un système de LAD fixe ou embarqué mobile).

Ce navigateur peut être lancé à bord du véhicule ou sur un poste de travail distant connecté à internet.

## Interface entre un poste de travail et le système de visualisation de preuves

Afin d’accéder au système de visualisation de preuves des ancrages sur la Blockchain, il faut avoir accès à internet et taper sur le navigateur internet l’URL du serveur d’interrogation des preuves juridiques (adresse Web du serveur à préciser) et s’identifier (login et mot de passe).

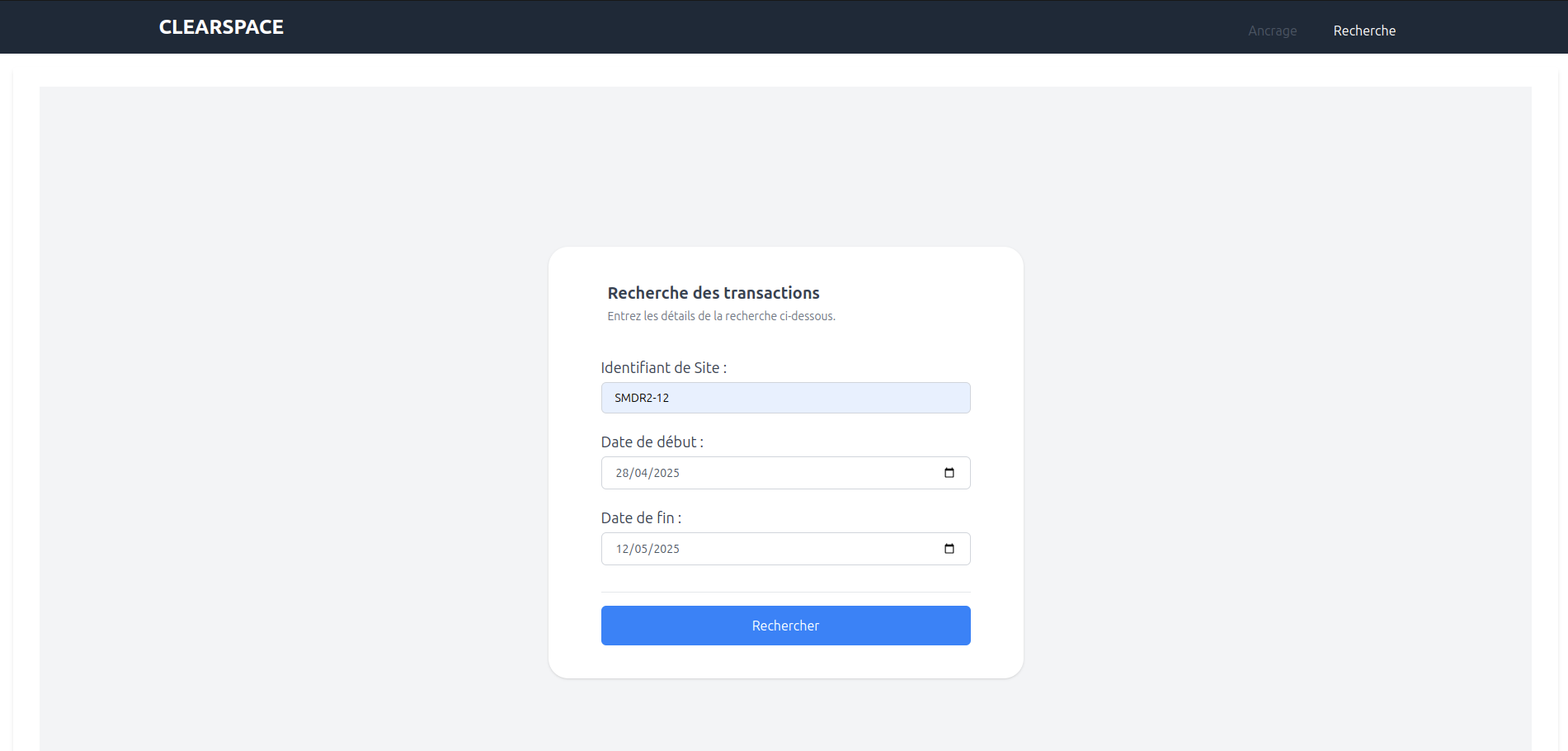


Figure 1 - Formulaire à titre d’exemple de recherche des preuves.

Un formulaire de recherche (exemple simplifié en Figure 1) permettra d’effectuer une recherche dans les différents ancrages à partir de l’identifiant de site, de la date ou encore du type de détection. Une comparaison entre le hash du fichier zippé (comprenant les photos) et le hash stocké dans la Blockchain grâce à l’utilisation d’Smart Contract permettra de certifier la non-altération des preuves.

Il s’agit là d’une application décentralisée (DApps) utilisant un Smart Contract pour l’interrogation du registre de la Blockchain.

# Interface entre un poste de travail et un ou des systèmes LAD fixes distants

## Objet du chapitre/Principe

Ce chapitre décrit ce qui est nécessaire pour afficher sur un poste de travail via un navigateur internet l’interface avec les systèmes de LAD DroneXTR distants.

Ce navigateur peut être lancé à bord du véhicule ou sur un poste de travail distant connecté à internet.

## Interface entre un poste de travail et un ou des systèmes lad fixes

Afin d’accéder à l’interface DroneXTR, il faut avoir accès à internet et taper sur le navigateur internet l’URL du service LAD fixe (**www.infodrone.fr**) et s’identifier (login et mot de passe).

Login à utiliser à partir du véhicule SMDR2 de démonstration dans le cadre du projet Clearspace :

[cegelec@dronextr.fr](mailto:cegelec@dronextr.fr)

Mot de passe temporaire : cegelec

(NB : le mot de passe a été changé à la première connexion : il peut être demandé au 02 32 63 59 47).

Les accès peuvent avoir lieu en parallèle depuis plusieurs postes de travail.

Afin d’être homogène avec les autres pages web, testé avec le navigateur Microsoft « Edge ».

## Accès à la cartographie nécessaire via internet

Afin d’afficher correctement le fond cartographique, le client a besoin d’avoir accès au domaine de OpenStreetMap (https:/ /tile-openstreetmap.org) car la page internet vient y récupérer des ressources nécessaires. Il ne faut pas configurer une interdiction sur cette URL.

**A VALIDER PAR DXTR, ne fonctionne pas chez nous. A tester lors de la mise en place sur le serveur embarqué**

# Interface entre un poste de travail et un ou des système LAD embarqués

## Objet du chapitre/Principe

Ce chapitre décrit ce qui est nécessaire pour afficher via un navigateur internet l’interface DroneXTR embarquée.

Ce navigateur peut être lancé à bord du véhicule ou sur un poste de travail distant connecté au VPN via internet.

## Interface entre un poste de travail et un ou des systèmes lad embarqués

Le web server de DroneXTR (PC Linux) est localisé à bord du véhicule, et est compris dans le réseau local du modem 4G/5G à bord du SMDR2. Il est donc nécessaire, afin d’y accéder, d’être connecté au réseau VPN associé au véhicule, d’avoir l’adresse IP associée au Serveur Web, ainsi que le port utilisé (61911). La redirection de ports dans le réseau du véhicule s’occupera du reste (NAT).

Dans le cadre du projet Clearspace, utilisez :

**192.168.32.62:61911**

Il faudra ensuite s’identifier (login et mot de passe) de manière équivalente au chapitre 5.2. **(login et mot de passe à indiquer par DXTR ou à configurer par CD SIC sur indication de DXTR)**

***En attente de livraison du Web Server DXTR et de sa documentation pour configurer finaliser ce chapitre et tester***

Les accès peuvent avoir lieu en parallèle depuis plusieurs postes de travail embarqués ou distants.

Afin d’être homogène avec les autres pages web, testé avec le navigateur Microsoft « Edge ».

### Initialisation du VPN

Il faudra initialiser le VPN si ce n’est pas déjà fait de manière équivalente au chapitre 3.2.1.

**Attention : Chaque entité ne peut connecter simultanément qu’une seule machine.**

### Utilisation du VPN

Il faudra utiliser le VPN de manière équivalente au chapitre 3.2.2

## Accès à la cartographie nécessaire via internet

Afin d’afficher correctement le fond cartographique, le client a besoin d’avoir accès au domaine de OpenStreetMap (https:/ /tile-openstreetmap.org) car la page internet vient y récupérer des ressources nécessaires.

**A VALIDER PAR DXTR**

# Interface entre les différents outils de détections et le système d’ancrage de preuves dans la blockhain

## Objet du chapitre/Principe

Ce chapitre décrit ce qui est nécessaire pour l’envoie de preuves des détections radars vers la blockchain depuis le poste de travail embarqué, des détections du ou des systèmes LAD embarqués vers la blockchain, et des détections du ou des systèmes LAD fixes vers la blockchain.

## Interface entre le logiciel SMDR2 et le système d’ancrage blockchain

Le firewall et le réseau interne du véhicule SMDR2 sont configurés pour autoriser l’information (le JSON et le dossier zippé à transiter vers l’adresse IP fixe ou une URL, ainsi que le potentiel port du service de blockchain à travers internet.

Format du fichier JSON :

**{**

**"time" : "11:44:32 10/01/2024",**

**"positionCible" : {**

**"latitude" : "49.324556",**

**"longitude" : "32.115154",**

**"altitude" : "12"**

**},**

**"positionVehicule" : {**

**"latitude" : "49.324556",**

**"longitude" : "32.115154",**

**"altitude" : "12"**

**},**

**"hash" : "321215561f56dsf16dsf11fsg13g15ds1fdsfz1g56z1gz1g15zf6df13dsg1fd5h13fd1g561f56ez1f56z15f1dz6f1dz1gdz",**

**"type" : "RADAR-PERSONNE",**

**"idsite" : "SMDR2-01",**

**"zipName" : "example.zip"**

**"comment" : "mission Octeville interception cigarette"**

**}**

Ainsi que le dossier zippé contenant 3 images .png (l’interface de l’IHM, la vue caméra jour associée et la vue caméra nuit associée).

Le champ « idsite » correspond à [modèle\_véhicule]-[identifiant\_véhicule], actuellement en développement, le modèle du véhicule est SMDR2, l’identifiant est 01.

Le champ « type » peut contenir comme différentes valeurs :

En cas de détections terrestres :

* RADAR-PERSONNE
* RADAR-INCONNU
* RADAR-VEHICULE

En cas de détections maritimes :

* RADAR-BATEAU
* AIS

Commentaire libre « comment » permet l’entrée d’un texte libre limité à 250 caractères.

NB : L’idée est de permettre à postériori un filtrage sur mot(s) clé(s) lors de la requête de récupération des preuves ancrées.

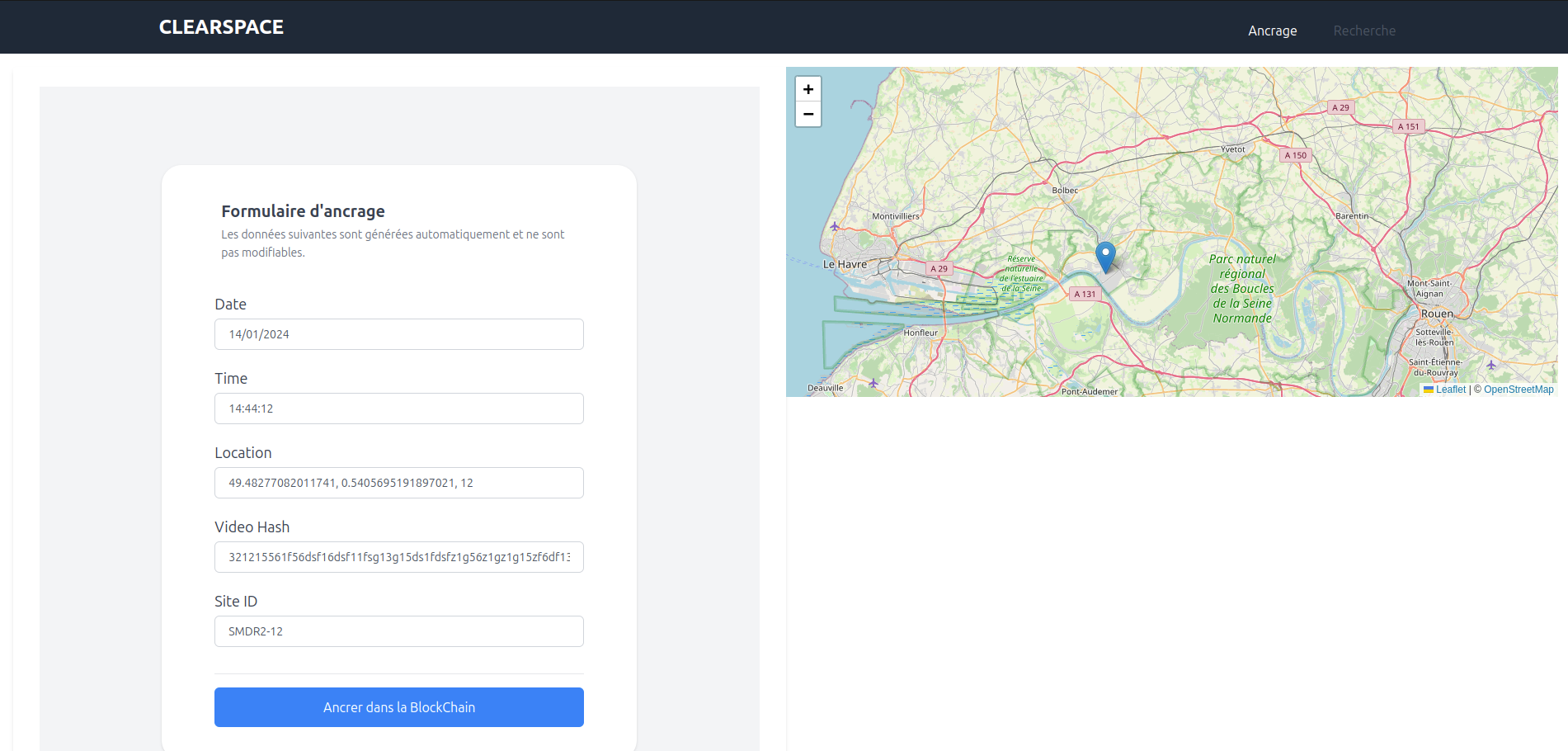


Figure 2 - Formulaire d'ancrage des preuves dans la Blockchain.

Dans un premier temps pour tester l’ancrage des données sur la Blockchain, une interface Web permettra à la fois de fournir le fichier JSON et le fichier zippé contenant les images. Cette interface est en cours de développement (cf. Figure 2).

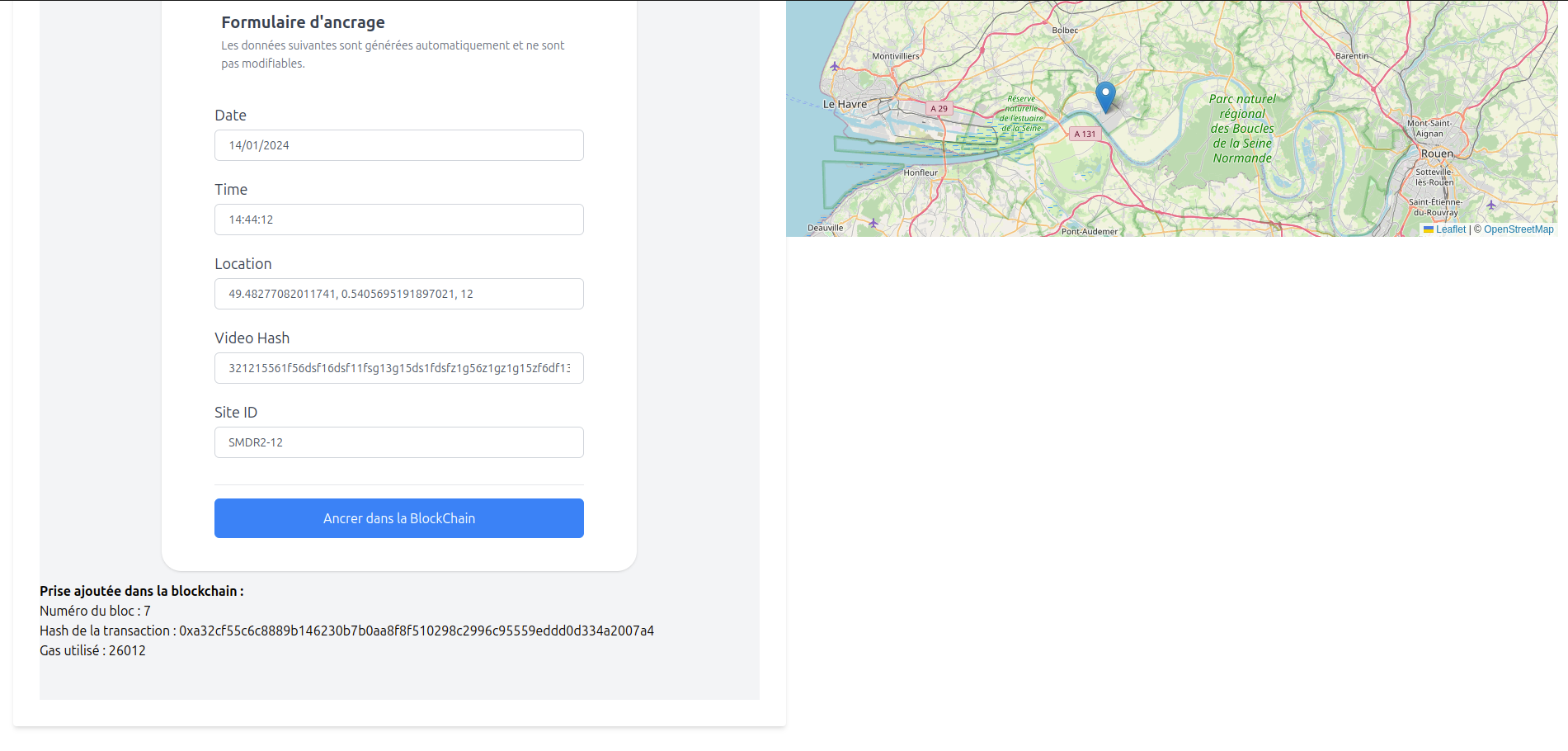


Figure 3 - Résultat de l'ancrage dans la Blockchain.

Le résultat de l’ancrage est présenté en Figure 3.

Ces interfaces ont été remplacées par une API qui permet d’appeler la fonction d’ancrage à partir du fichier JSON et du fichier zippé.

### Documentation de l’API

L’ensemble des routes sont protégées par une clé d’API. La clé administrateur par défaut est **admin\_api\_key**. La clé administrateur est la seule à pouvoir créer de nouvelles clés API.

La clé d’API est à transmettre dans l’en-tête de la requête HTTP:

**x-api-key: <votre\_clé\_api>**

Vous pouvez importer la documentation réalisé avec Insomnia appelée api-v1.

**Définir les données**

* **URL:** https://clearspace.databeam.eu/data
* **Méthode:** POST

Attends 2 fichiers à envoyer en tant que multipart/form-data: - data: Fichier sous la forme application/octet-stream (flux d’octets) contenant les données à ancrer - file: Fichier sous la forme application/octet-stream (flux d’octets) contenant les preuves à ancrer.

**Obtenir une donnée par identifiant**

* **URL:** https://clearspace.databeam.eu/data/{\_id}
* **Méthode:** GET
* **Paramètres:**
  + \_id: Identifiant de la donnée

**Obtenir toutes les données**

* **URL:** https://clearspace.databeam.eu/data/
* **Méthode:** GET

**Obtenir la preuve d’ancrage de la donnée par identifiant**

* **URL:** https://clearspace.databeam.eu/data/{\_id}/anchor
* **Méthode:** GET
* **Paramètres:**
  + \_id: Identifiant de la donnée

**Clés API****: Définir la clé API**

* **URL:** https://clearspace.databeam.eu/apikeys/
* **Méthode:** GET

## Interface entre le système lad embarqué et le système de blockchain

Le firewall et le réseau interne du véhicule SMDR2 sont configurés pour autoriser l’information (le JSON) à transiter vers l’adresse IP fixe ou une URL, ainsi que le potentiel port du service de blockchain à travers internet.

L’interfaçage se fera de manière similaire à l’interfaçage entre le logiciel SMDR2 et le système d’ancrage sur la Blockchain. Il s’agira donc de l’envoi d’un fichier JSON par le biais d’une API permettant l’ancrage sur la Blockchain. La seule différence pourra venir d’un contenu légèrement adapté du JSON, mais sa structure demeure la même.

Le fichier JSON qui contient l’horodatage, la localisation GPS, le type de drone, son N° de série et le ZIP qui contient le fichier de photos ou vidéos.

Format du fichier JSON :

**{**

**"time" : "11:44:32 10/01/2024",**

**"positionCible" : {**

**"latitude" : "49.324556",**

**"longitude" : "32.115154",**

**"altitude" : "12"**

**},**

**"positionVehicule" : {**

**"latitude" : "49.324556",**

**"longitude" : "32.115154",**

**"altitude" : "12"**

**},**

**"hash" : "321215561f56dsf16dsf11fsg13g15ds1fdsfz1g56z1gz1g15zf6df13dsg1fd5h13fd1g561f56ez1f56z15f1dz6f1dz1gdz",**

**"type" : " ????",**

**"idsite" : " ????",**

**"zipName" : "example.zip"**

**}**

**A CONFIRMER PAR DXTR**

**Le champ « type » utilisé pour les détections Radar et AIS peut être utilisé pour les détections LAD pour le type de drone détecté (genre DJI oun Parrot ????). Non nous indiquons le type : drone. l’horodatage, de la localisation GPS, du type de drone=modèle, son N° de série et un fichier, identifiant de l’antenne = n° de série**

**Le champ « idsite » peut être utilisé pour identifier l’antenne origine de la détection (Serial number ou autre à préciser ainsi que la grammaire/nomenclature). Cf ci dessus**

**Le champ « comment » utile dans le cas Radar peut être ajouté si DXTR le souhaite (voir description chapitre 7.2). oui il est utilisé pour ajouter un commentaire**

## Interface entre le ou les systèmes lad fixes et le système de blockchain

L’interfaçage se fera de manière identique à l’interfaçage entre le logiciel LAD embarqué et le système d’ancrage sur la Blockchain (voir chapitre précèdent 7.3).

**Fin du document**