Plan d’Assurance Sécurité

de la société Authôt SAS

Version 1.2 de mars 2026

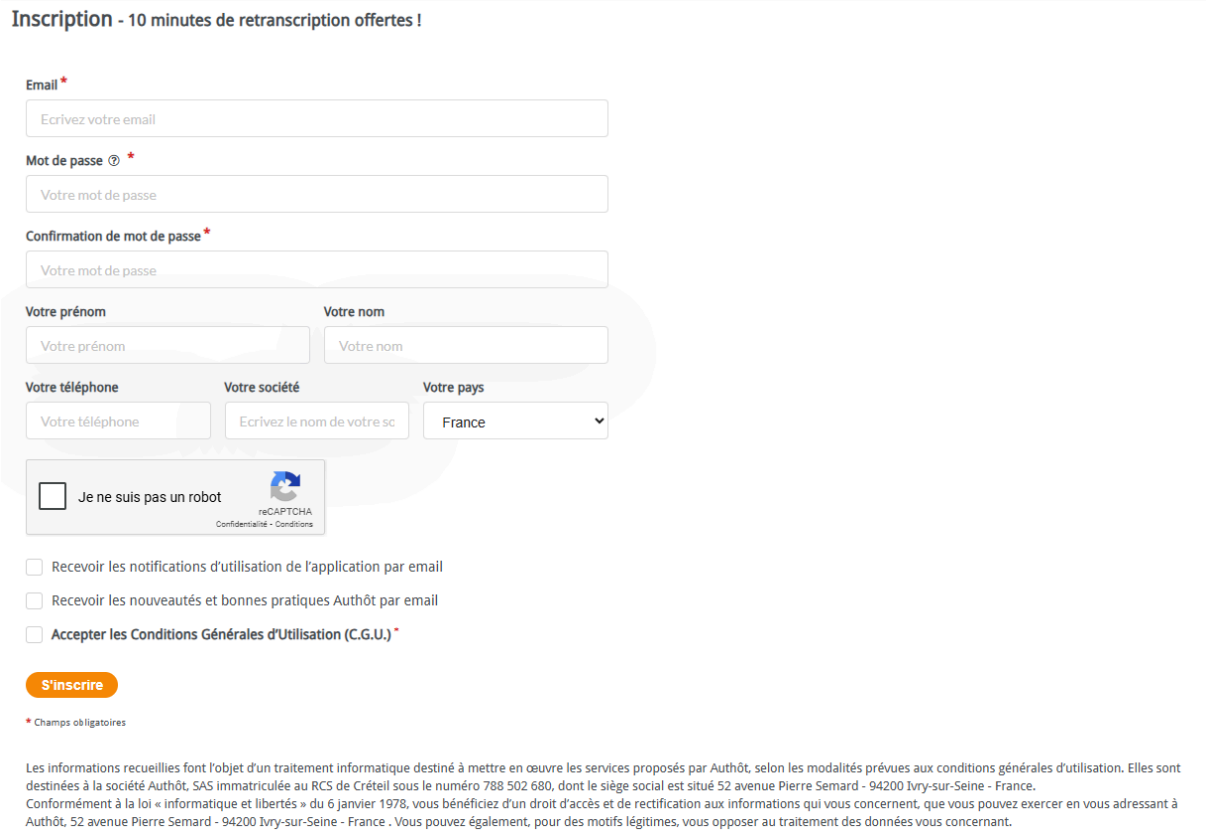
Table des matières

Authentifications des utilisateurs..... 3
Méthode de sécurisation des jetons de session d'authentification.....3
Assistance, gestion des problèmes et communication..... 4
Moyens informatiques et techniques.....7
Moyens immatériels..... 7
Cybersécurité..... 8
Confidentialité & protection des données..... 9
Hébergement, stockage et sécurisation des données des applications Authôt..... 9
Finalités attachées au Traitement des Données personnelles.....10
Base légale du traitement des Données Personnelles.....10
Les données à caractère personnel traitées sont :..... 10
Supports de traitement des Données personnelles.....11
Durée de conservation des Données..... 11
Moyens d'accès..... 11
Mesures de sécurité..... 11
L'interface de programmation applicative..... 12
Architecture Générale.....12
Représentation de l'Architecture..... 13
Mesures de Sécurité par Composant.....14
Protection des communications utilisateurs..... 16
Protection contre les attaques et protection sur les produits.....18
Sécurité de l'environnement de travail..... 20
Surveillance.....20
Mises à jour.....21
Sauvegardes..... 21
Sécurité dans le développement de l'application..... 21
Politique de gestion des incidents vis-à-vis de l'Utilisateur..... 21
Gestion de la réversibilité..... 22

Authentifications des utilisateurs

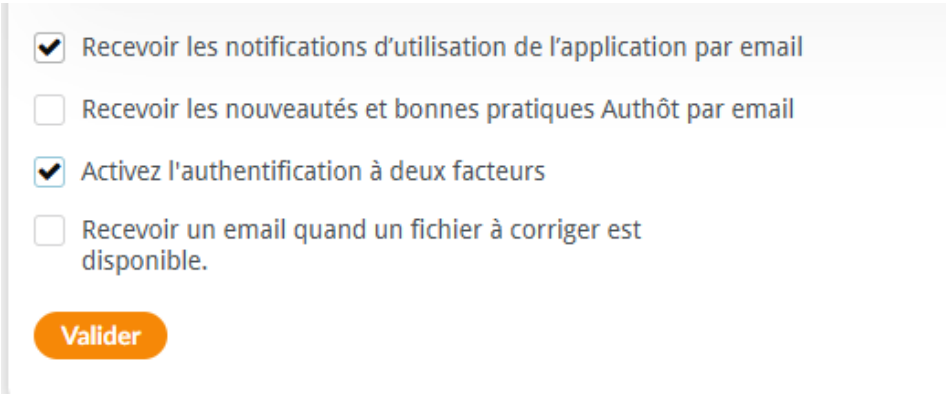
Chaque utilisateur des plateformes Authôt crée un compte avec un email d'identifiant et un mot de passe.

Ci-dessous l'interface d'inscription.



Le mot de passe doit contenir au moins 12 caractères, incluant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

Depuis l'onglet Mon compte, l'utilisateur peut activer ou désactiver à tout moment, la double authentification, ou l'authentification à deux facteurs, de son compte.



Méthode de sécurisation des jetons de session d'authentification

Stockage des Sessions : Par défaut, Rails utilise un magasin de cookies chiffrés et signés (cookie_store). Les informations de session ne sont pas stockées côté serveur dans une base de données, mais directement dans un cookie envoyé au navigateur de l'utilisateur.

Chiffrement (Confidentialité) : Le contenu du cookie de session est chiffré à l'aide d'une clé secrète forte propre à notre application (secret_key_base gérée via les Rails Credentials). Cela empêche quiconque (y compris l'utilisateur ou un attaquant interceptant le cookie) de lire les informations contenues dans la session (comme l'ID de l'utilisateur connecté).

Signature (Intégrité) : En plus d'être chiffré, le cookie de session est également signé numériquement à l'aide de la même clé secrète. Cela garantit que le cookie n'a pas été modifié ou altéré par le client ou un tiers. Si la signature ne correspond pas lorsque le cookie revient au serveur, Rails rejette la session comme invalide.

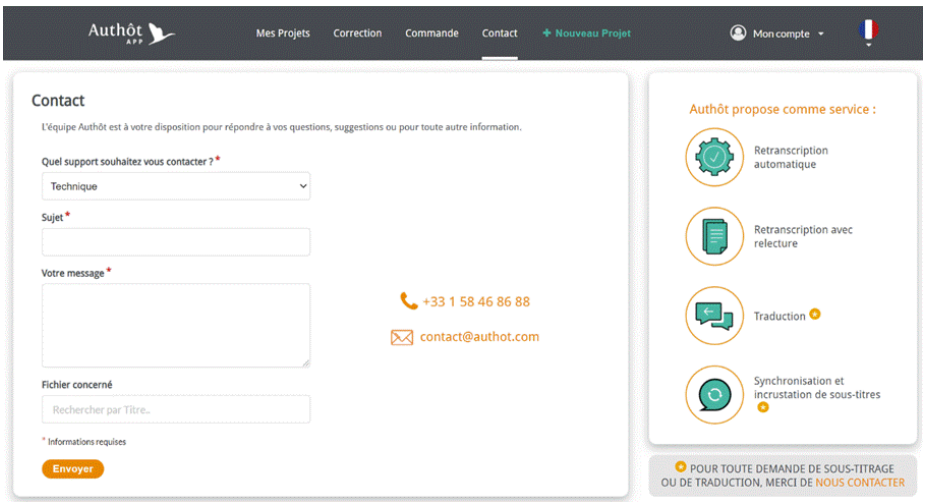
Flag HttpOnly : Rails configure systématiquement le cookie de session avec le flag HttpOnly. Ce flag ordonne au navigateur de ne pas autoriser l'accès au cookie via des scripts côté client (JavaScript). C'est une défense essentielle contre les attaques de type Cross-Site Scripting (XSS) qui tenteraient de voler le jeton de session.

Flag Secure : Suite à une mise à jour récente le flag secure ne semble plus être présent. Nous allons analyser cela pour le remettre.

Dans notre configuration de production, nous avons activé le paramètre config.force_ssl = true dans Ruby on Rails. Ce paramètre force toutes les connexions à passer en HTTPS et, de manière cruciale, ajoute automatiquement le flag Secure à tous les cookies, y compris le cookie de session.

Assistance, gestion des problèmes et communication

Depuis l'application Authôt, la rubrique **Contact** est à l'entière disposition de l'utilisateur pour contacter le service technique, opérationnel ou commercial.



Un accusé de réception accompagné d’une proposition de qualification du fait technique ou opérationnel sera retourné sous 4 heures, quel que soit le moyen de communication utilisé.

Nous proposons de distinguer trois types de faits techniques :

- ➔ Bloquant - Désigne un comportement mettant en péril le processus de transcription, de sous-titrage ou de traduction.
- ➔ Majeur – Désigne un comportement qui, sans mettre en péril le processus de transcription, de sous-titrage ou de traduction, entraîne une surcharge d'activité pour l'Utilisateur.
- ➔ Mineur – Autre cas.

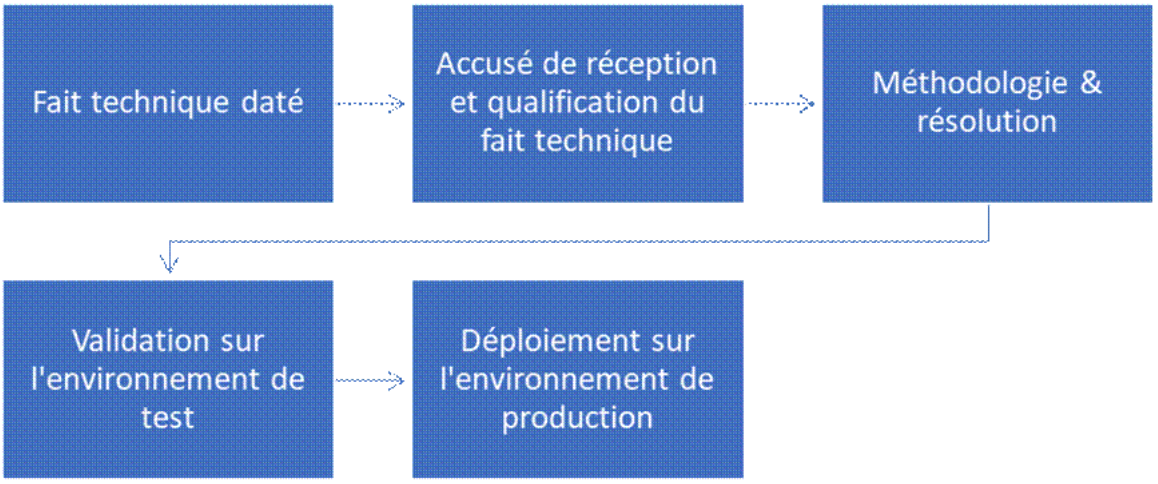


Figure 1. Diagramme du traitement de la maintenance technique

Figure 2. Diagramme du traitement de la qualité opérationnelle

Une fois la proposition de qualification du fait technique ou opérationnel acceptée, nous garantissons un rétablissement du service sous :

- ➔ 1 jour pour un fait technique bloquant.
- ➔ 3 jours pour un fait technique majeur.
- ➔ 5 jours pour un fait technique mineur.

Moyens informatiques et techniques

Moyens immatériels

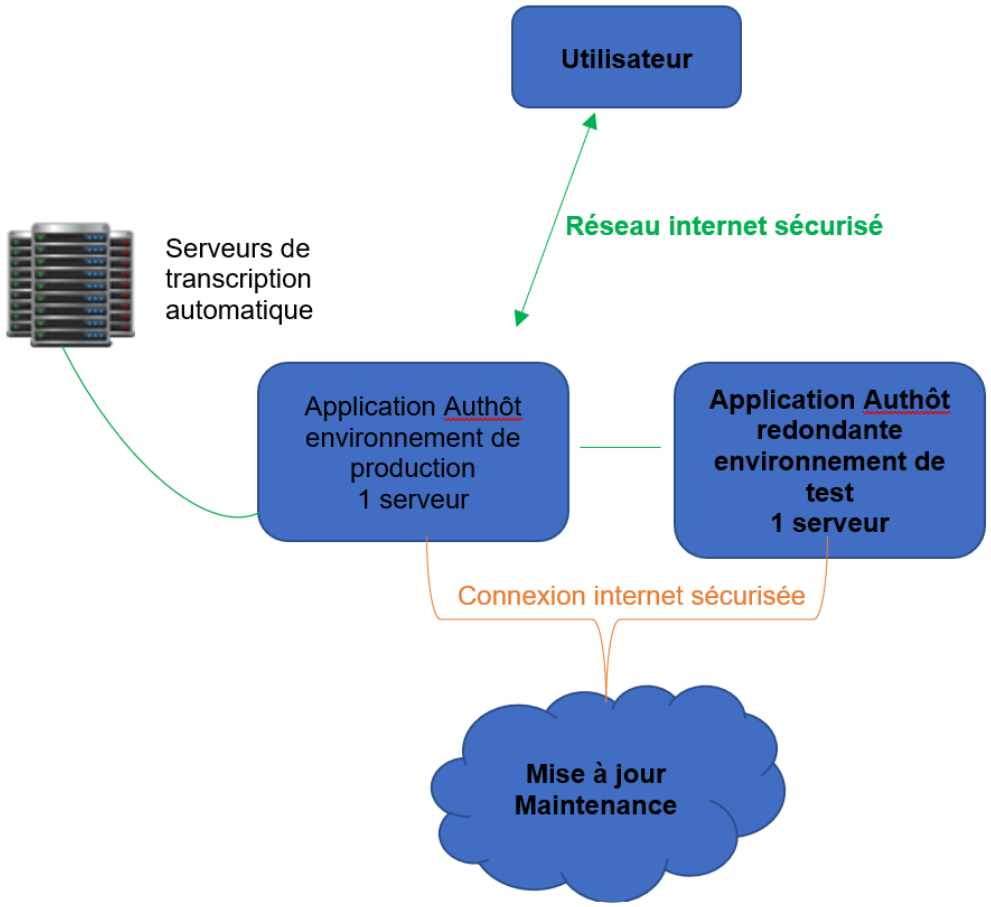


Figure 3. Architecture technique de l'accès à l'application Authôt

L'infrastructure informatique et web installée permettent de partager :

- Une plateforme dédiée et sécurisée pour tous vos livrables (texte, enregistrements, sous-titres,…).
- Une connexion SDSL très haut débit (upload et download).
- Disponibilité : 99.982%, 1.6 heure d'interruption/an, Redondance N+1.

Les serveurs sont hébergés en France par la société OVH et Scaleway.

Le standard de la technologie Authôt accepte les flux audio et vidéo de la collection FFmpeg (licence LGPL version 2.1). Les codecs WAV, MP3, WMA, MP4, AVI, MOV, FLV sont notamment supportés.

Niveaux de services contractuels :

Le service Support technique d'Authôt est disponible du lundi au vendredi de 9h à 18h :
Par téléphone au 01 58 46 86 88.
Par email à l'adresse support@authot.com
Également via un système de ticket sur les plateformes en ligne APP, STUDIO et LIVE depuis l'onglet Contact/ service Technique.
On retrouve l'ensemble des messages échangés sur la plateforme depuis Mon compte / Ma messagerie.

Cybersécurité

Notre équipe technique s'efforce de sécuriser un maximum notre architecture informatique avec des moyens limités à la taille de notre entreprise.

Les accès à nos outils sont sécurisés par le protocole https, et mot de passe. L'accès aux serveurs de transcription et de stockage est restreint aux utilisateurs accrédités.
Lors de l'envoi d'un fichier vidéo, il est converti et stocké sous trois formats : .mp4, .mp3 et .ogg. Les deux derniers sont des formats audios.
Seulement le personnel d'Authôt a accès via une plateforme d'administration grâce à un login et mot de passe aux données utilisateurs.

L'utilisateur possédant les accès à son compte peut aussi accéder à ces données grâce à son email et son mot de passe.

Certaines données personnelles à caractère sensible (adresse IP, timezone, mot de passe encryptés) sont accessibles uniquement via une connexion ssh sur les serveurs des applications protégées par double authentification et restriction par clé ssh.

Nous nous engageons à supprimer toutes les données relatives à un utilisateur dans un délai d'un mois maximum après la demande de celui-ci.
Et un délai de 10 ans pour la conservation des données de facturation (contrats, factures…)
Aucune des données personnelles n'est communiquée à d'autres personnes ou services si l'utilisateur n'a pas clairement indiqué son envie que cela soit fait.

Confidentialité & protection des données

Hébergement, stockage et sécurisation des données des applications Authôt

Société : OVH

SIREN : RCS Lille Métropole 424 761 419 00045
N° de TVA : FR 22 424 761 419
Siège social : 2 rue Kellermann - 59100 Roubaix - France
Site : https://www.ovh.com/

Localisation physique des serveurs OVH : Gravelines (France).

Usage : Stockage Object des vidéos + audio + XML de transcription automatique. Le MP4 est conservé trois mois.

Pour les fichiers audios + json, ils sont conservés jusqu'à la date de fin de contrat. Authôt s'engage à mettre tout en œuvre pour détruire l'intégralité des enregistrements qui concernent l'utilisateur y compris auprès de ses sous-traitants et à faire un retour écrit si besoin

Société : Scaleway

SIREN : 433 115 904 RCS Paris
Siège social : 8 rue de la Ville l'Evêque - 75008 Paris - France
N° de TVA : FR 35 433115904

Courrier : SCALEWAY SAS BP 438 75366 PARIS CEDEX 08 FRANCE

Site : https://www.scaleway.com/
Téléphone : +33 (0)1 84 13 00 00

Localisation physique des serveurs Scaleway : Paris (France).

Usage : Applications en ligne + Service de Base de données (DBaaS) qui contient toutes les informations liées à l'utilisateur ainsi que les transcriptions de ses fichiers.

Société : Ikoula

SIREN : 417 680 618 RCS Paris
Siège social : 2 Cité Paradis - 75010 Paris - France
N° de TVA : FR 37417680618

Site : https://www.ikoula.com/fr
Téléphone : +33 (0)1 78 76 35 51

Localisation physique des serveurs Ikoula : Reims (France).

Usage : Technologies de transcription automatique de la parole, solution d'Intelligence Artificielle neuronale hébergée en local basée sur la technologie open source Whisper avec des surcouches propriétaires Authôt.
Contient les fichiers audios plus les transcriptions automatiques. Les données sont conservées deux mois pour les fichiers json de transcription automatique et un mois pour les fichiers audios, sauf si l'utilisateur fait une demande de suppression de son fichier.

Finalités attachées au Traitement des Données personnelles

Utilisation des données pour :

- Gestion de la relation technique avec les interlocuteurs concernés.
- Gestion de la relation Clients avec les interlocuteurs concernés.
- Gestion financière avec les interlocuteurs concernés.
- Les documents audios et vidéos envoyés sur les applications et API Authôt afin d'effectuer les transcriptions et sous-titres.

Base légale du traitement des Données Personnelles

La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

Les données à caractère personnel traitées sont :

- L'adresse électronique et le mot de passe qui est encrypté chez Authôt qui sont obligatoires pour accéder aux plateformes.
- Les documents déposés sur les plateformes qui sont obligatoires pour être retranscrit.
- Nom prénom, numéro de téléphone, adresse, ville, code postal, pays, nom de société, numéro de tva intracommunautaire sont facultatifs.
- L'adresse IP de la dernière connexion de l'utilisateur, Timezone , type de navigateur et version, version du système d'opération, taille d'affichage.

Supports de traitement des Données personnelles

Applications en ligne et API permettant le dépôt et la transcription des documents audios ou vidéos souhaités par l'utilisateur.

Chaque utilisateur dispose d'un espace personnel propre et privé.

Durée de conservation des Données

Les Données personnelles sont conservées jusqu'à la date de fin de contrat.

Dans le cas d'une demande de suppression de ces données, les informations personnelles seront détruites dans un délai maximum d'un mois.

Et un délai de 10 ans pour la conservation des données de facturation (contrats, factures…). Cette durée est spécifiée dans nos Conditions Générales d'Utilisations et s'applique à l'ensemble de nos utilisateurs. À votre demande, nous pouvons y apporter un avenant.

Moyens d'accès

Les données personnelles relatives à l'utilisateur sont accessibles via une plateforme d'administration en mode SAAS sécurisée et accessible uniquement par certains utilisateurs ayant les droits.

Certaines données personnelles (adresse IP, timezone, mots de passe encryptés, version de navigateur, système opérationnel et taille d'écran) sont accessibles uniquement via une connexion ssh sur les serveurs des applications protégées par une double authentification et restriction par clé ssh.

Mesures de sécurité

Seulement le personnel d'Authôt a accès via une plateforme d'administration grâce à un login et mot de passe aux données utilisateurs.

L'utilisateur possédant les accès à son compte peut aussi accéder à ces données grâce à son email et son mot de passe.

Certaines données personnelles (adresse IP, timezone, mot de passe encryptés) sont accessibles uniquement via une connexion ssh sur les serveurs des applications protégées par double authentification et restriction par clé ssh.

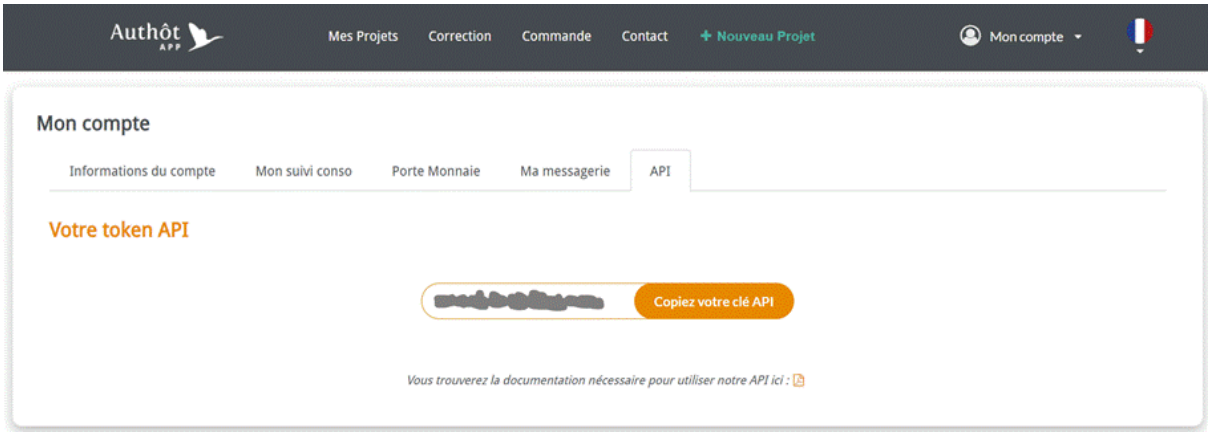
Nous nous engageons à supprimer toutes les données relatives à un utilisateur dans un délai d'un mois maximum après la demande de celui-ci.

Et un délai de 10 ans pour la conservation des données de facturation (contrats, factures…) Aucune des données personnelles n'est communiquée à d'autres personnes ou services si l'utilisateur n'a pas clairement indiqué son envie que cela soit fait.

Nous ne collectons pas de données personnelles sensibles ou protégées.

L'interface de programmation applicative

L'interface de programmation applicative Authôt est accessible directement depuis votre espace utilisateur.



Accès à l'API depuis Mon Compte

Voici la documentation en ligne :
https://documenter.getpostman.com/view/6136336/2sAYk8thJv

Une clé d'accès sécurisée est dédiée à chaque compte utilisateur.

Architecture Générale

Notre système est conçu pour la haute disponibilité et la sécurité, en s'appuyant sur des services hébergés chez des fournisseurs français reconnus :

Point d'Entrée (Load Balancer Scaleway) : Le trafic entrant des utilisateurs (HTTPS) est d'abord reçu par un Load Balancer managé par Scaleway. Celui-ci répartit la charge et assure la continuité de service. Il gère également la terminaison SSL/TLS.

Application Web Principale (Ruby on Rails - Scaleway) : L'application tourne sur deux serveurs privés virtuels (VPS) redondants chez Scaleway, placés derrière le Load Balancer. Cette configuration améliore la disponibilité et les performances. Ces VPS communiquent

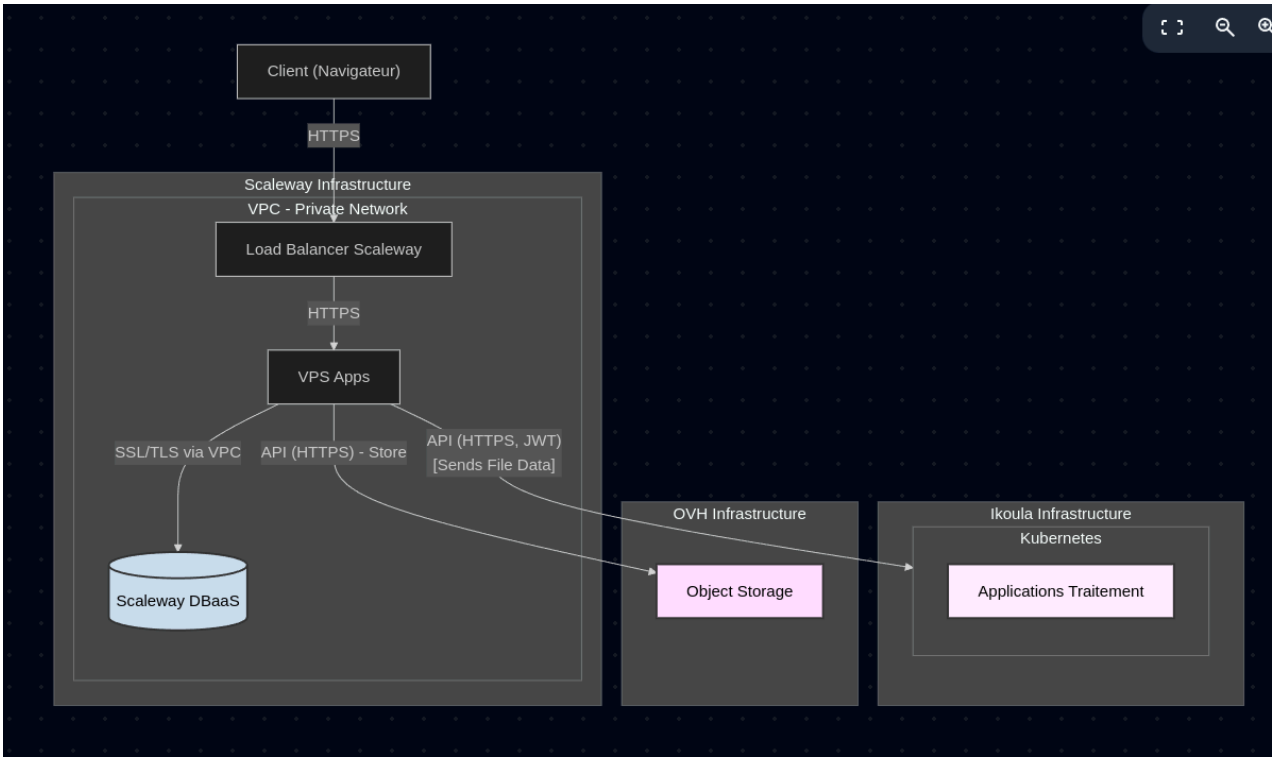
entre eux et avec la base de données via un réseau privé sécurisé (VPC/Private Network Scaleway).

Base de Données (DBaaS - Scaleway) : Les données structurées sont stockées dans une base de données managée (DBaaS) fournie par Scaleway. Point essentiel : cette base de données est isolée dans le même réseau privé (VPC) que les VPS applicatifs, la rendant inaccessible depuis l'internet public.

Stockage Fichiers Multimédia (Object Storage - OVHcloud) : Les fichiers que vous nous confiez sont stockés de manière sécurisée sur le service Object Storage d'OVHcloud.

Service de Traitement Multimédia (Application Rails dédiée - Ikoula) : Les opérations spécifiques sur vos fichiers sont effectuées par une application Rails distincte sur un serveur dédié chez Ikoula, contactée via une API REST sécurisée depuis l'application principale. Les données n'y sont présentes que temporairement.

Représentation de l'Architecture



Le Client se connecte en HTTPS au Load Balancer Scaleway.

Le Load Balancer transmet la requête (en HTTP ou HTTPS) à l'un des VPS Applicatifs Rails (Scaleway) via le réseau interne.

Le VPS Applicatif :

Communique avec la Base de Données Scaleway via le réseau privé (VPC) en utilisant une connexion SSL/TLS.

Communique avec OVH Object Storage via API HTTPS pour stocker/récupérer des fichiers.

Communique avec l'Application de Traitement (Ikoula) via API REST (HTTPS + JWT) pour déclencher des traitements.

L'Application de Traitement (Ikoula) traite les fichiers nécessaires une fois reçu par l’Application Principale via API HTTPS, puis les supprime localement une fois terminé.

Mesures de Sécurité par Composant

Application Web Principale (Scaleway VPS)

Accès Réseau : Le serveur est protégé par un pare-feu local (ufw) configuré pour n'autoriser que les connexions strictement nécessaires (HTTPS: 443, SSH: [Port non standard recommandé]).

Système d'Exploitation : Nous maintenons le système d'exploitation à jour. Les mises à jour de sécurité critiques sont appliquées automatiquement grâce à unattended-upgrades.

Accès Sécurisé : L'accès administratif (SSH) au serveur est restreint, se fait uniquement via des clés SSH sécurisées et est renforcé par une authentification à deux facteurs (2FA). L'authentification par mot de passe est désactivée.

Sécurité Applicative (Ruby on Rails) :

Utilisation systématique des mécanismes intégrés de Rails pour prévenir les attaques courantes (CSRF, XSS, SQL Injection via ActiveRecord).

HTTPS : Tout le trafic entre le client et l'application est chiffré via HTTPS (SSL/TLS) en utilisant des certificats Let's Encrypt. La redirection de HTTP vers HTTPS est forcée.

Gestion des Secrets : Les clés d'API (OVH, etc.), mots de passe de base de données et autres secrets (secret_key_base) sont gérés de manière sécurisée grâce au système de Credentials chiffrés intégré à Rails (credentials.yml.enc). Ils ne sont jamais stockés en clair dans le code source ou les dépôts de code.

Dépendances : Nous surveillons les dépendances (gems) pour les vulnérabilités connues et nous nous efforçons de les maintenir à jour.

Isolation : L'application tourne avec des permissions utilisateur restreintes.

- **Base de Données (Scaleway DBaaS)**

Service Managé : Scaleway gère la sécurité de l'infrastructure sous-jacente, l'application des patchs et la configuration de base.

Accès Réseau : La base de données n'est accessible que depuis l'adresse IP de notre serveur applicatif VPS (liste blanche IP).

Connexions Chiffrées : Les connexions entre l'application Rails et la base de données sont chiffrées via SSL/TLS.

Authentification : L'accès à la base de données est protégé par des identifiants forts, gérés via les Rails Credentials.

Sauvegardes : Des sauvegardes régulières et automatisées sont effectuées par Scaleway, permettant une restauration rapide en cas d'incident.

- **Stockage Fichiers (OVH Object Storage)**

Transferts Sécurisés : Tous les transferts de fichiers (upload/download) entre nos applications et OVH Object Storage se font via HTTPS.

Accès Contrôlé : L'accès aux fichiers est géré par des clés d'API spécifiques au service Object Storage. Ces clés sont stockées de manière sécurisée via les Rails Credentials et ont des permissions limitées au strict nécessaire.

Redondance et Durabilité : OVH Object Storage est conçu pour une haute disponibilité et durabilité des données (réplication interne).

Chiffrement au Repos : OVH Object Storage propose des options de chiffrement des données au repos (côté serveur). Nous sommes en train de vérifier la configuration actuelle et nous assurerons que cette protection est active pour renforcer la sécurité de vos fichiers stockés. [Action interne : Vérifier et activer si nécessaire]

- **Service de Traitement Multimédia (Ikoula Dédié)**

Accès Réseau : Le serveur est protégé par un pare-feu local (ufw) limitant les connexions entrantes aux flux nécessaires (HTTPS pour l'API depuis le VPS Scaleway, SSH sécurisé).

Système d'Exploitation : Le système est maintenu à jour (avec unattended-upgrades également).

Accès Sécurisé : L'accès administratif est restreint via clés SSH (+ 2FA si appliqué aussi ici).

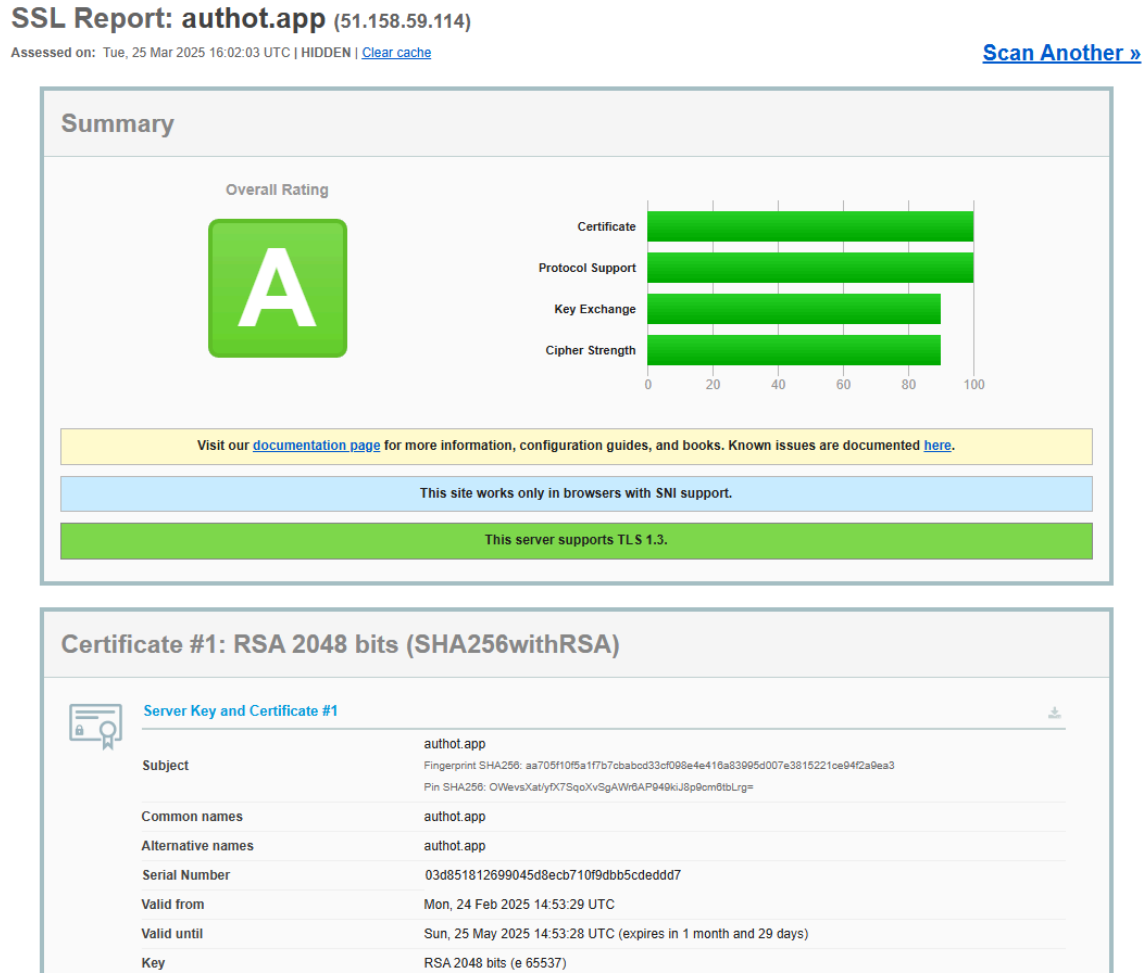
Communication Sécurisée : L'application principale communique avec ce service via une API REST interne sur HTTPS. L'authentification est assurée par des tokens JWT (JSON Web Tokens), garantissant que seules les requêtes légitimes sont acceptées.

Gestion des Données Temporaires :
Point crucial : les fichiers multimédia ne sont présents sur ce serveur que de manière éphémère. L'application de traitement utilise Active Storage pour gérer les fichiers. Une fois le traitement terminé (succès ou échec), la copie locale du fichier gérée par Active Storage est automatiquement et systématiquement supprimée du serveur Ikoula. Aucune donnée client ne persiste sur ce serveur au-delà de cette opération.

Protection des communications utilisateurs

Nos plateformes en ligne sont bien sur les versions actuelles de serveurs protégés.

HTTPS
TLS 1.3
HSTS Preloading (Chrome Edge Firefox IE)



SSL Report: authot.studio (163.172.138.253)

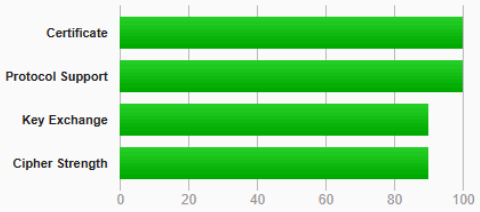
Assessed on: Thu, 27 Mar 2025 13:52:47 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A



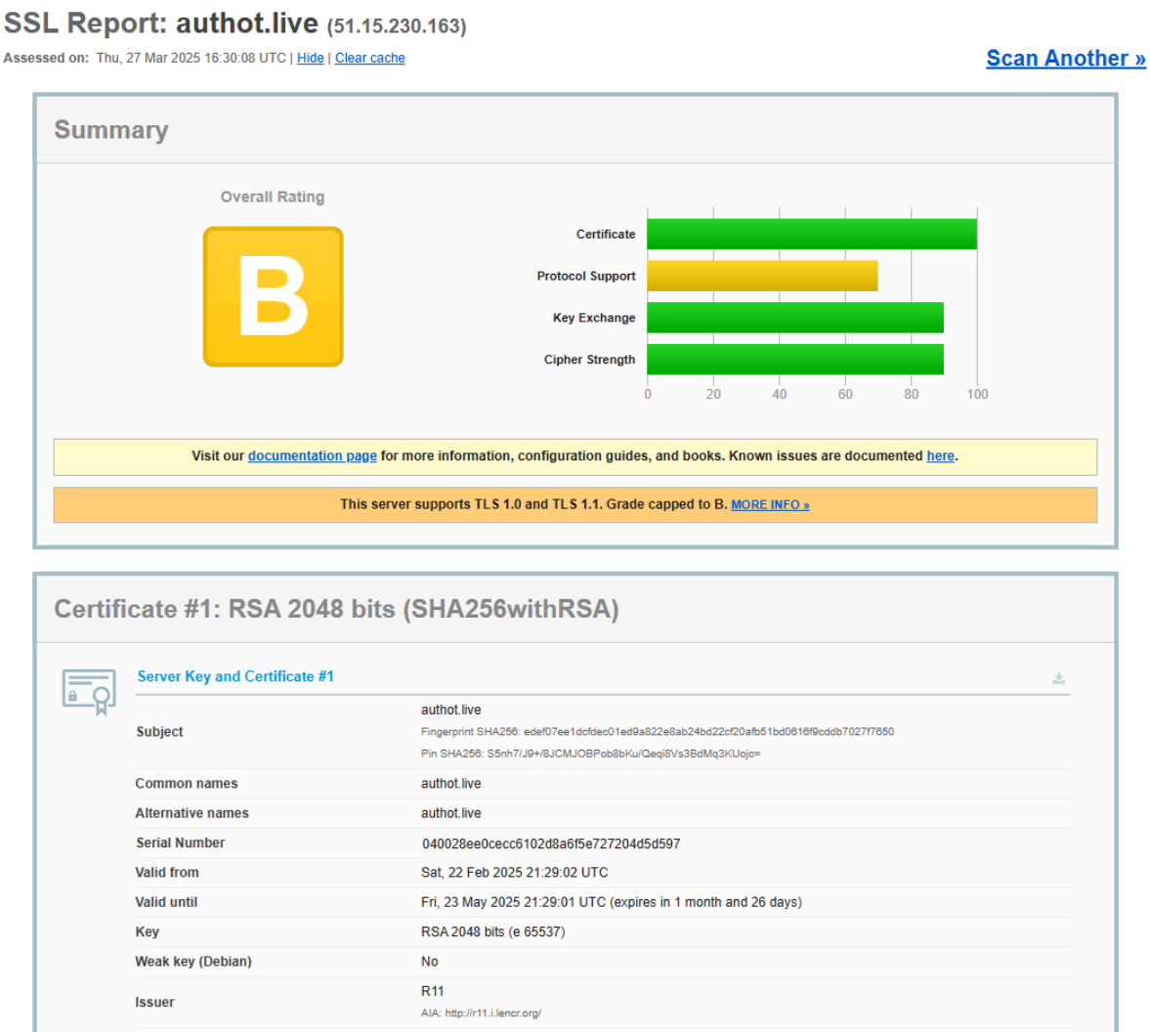
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	authot.studio Fingerprint SHA256: 3bb85e9a52941188cbbe62409df9b01c3da0fee3110103b1691463f60b7da57a Pin SHA256: /BFm/hrMRThmlAtEwd7SzB1pN7D7ehm7p+sJKv+qV0w=
Common names	authot.studio
Alternative names	authot.studio
Serial Number	04ced4a1d9e782a90a70a4618b7ac27a3d9c
Valid from	Mon, 17 Feb 2025 07:22:42 UTC
Valid until	Sun, 18 May 2025 07:22:41 UTC (expires in 1 month and 20 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R10 AIA: http://r10.i.lencr.org/



SSL Report: authot.live (51.15.230.163)

Assessed on: Thu, 27 Mar 2025 16:30:08 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B

Certificate
Protocol Support
Key Exchange
Cipher Strength
0 20 40 60 80 100

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	authot.live Fingerprint SHA256: edef07ee1dcfdec01ed9a822e8ab24bd22cf20afb51bd0616f9cddb7027f7650 Pin SHA256: S5nh7/J9+/8JCMJOBPob8bKu/Qeqj8Vs3BdMq3KUojc=
Common names	authot.live
Alternative names	authot.live
Serial Number	040028ee0cecc6102d8a6f5e727204d5d597
Valid from	Sat, 22 Feb 2025 21:29:02 UTC
Valid until	Fri, 23 May 2025 21:29:01 UTC (expires in 1 month and 26 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R11 AIA: http://r11.i.lencr.org/

Protection contre les attaques et protection sur les produits

Nous suivons chaque année les vulnérabilités les plus fréquentes identifiées par l'OWASP :

Injection, rupture d'authentification, exposition des données sensibles, référence directe non sécurisée à un objet, mauvaise configuration de sécurité, falsification de requête intersite, scripts intersites, désérialisation non sécurisée, utilisation de composants vulnérables, journaux et suivi insuffisant.

Nous nous engageons à détailler et à mettre en œuvre les mesures de sécurité suivantes :
- la mise en œuvre de moyens et dispositifs anti-intrusions ;
- la gestion et traçabilité des accès physiques des personnes sur site ;
- la mise en œuvre de cloisonnement physique garantissant la protection et la confidentialité des activités réalisées pour l'utilisateur par rapport aux autres activités ;
- la mise en œuvre de moyens et dispositifs de détection et de lutte contre les incendies ;

- la mise en œuvre de moyens de services généraux (énergie, climatisation, réseaux) en cas d'hébergement de systèmes d'informations.

Sécurité, réseaux de nos différents hébergeurs

Les serveurs hébergés chez nos prestataires répondent à toutes les exigences de sécurité physiques.

OVH RGPD lié à nos serveurs utilisés :
https://www.ovhcloud.com/fr/about-us/data-sovereignty/

OVH Cybersécurité liée à nos serveurs utilisés : https://www.ovhcloud.com/fr/compliance/

Mise en œuvre de différentes normes et référentiels (ISO 27001, ISO 27701, SecNumCloud, HDS, SOC, CSA Star, PCI-DSS

OVH Développement durable lié à nos serveurs utilisés :
https://corporate.ovhcloud.com/fr/sustainability/

Scaleway Sécurité et résilisence liées à nos serveurs utilisés :
https://www.scaleway.com/fr/securite-et-resilience/

Scaleway Modèle de responsabilié lié à nos serveurs utilisés :
https://www.scaleway.com/en/docs/elastic-metal/reference-content/shared-responsibility-model/

Scaleway Responsabilité sociale lié à nos serveurs utilisés :
https://www.scaleway.com/fr/responsabilite-sociale/

Ikoula Certifications ISO liés à nos serveurs utilisés :
https://www.ikoula.com/fr/politique-rse/certifications-iso

Ikoula Développement durable lié à nos serveurs utilisés :
https://www.thegreenwebfoundation.org/green-web-check/?url=https%3A%2F%2Fwww.ikoula.com

Dans le cas de détection d'évènements anormaux provenant de nos services ou nos prestataires, nous mettons en oeuvre les mesures de sécurité suivantes :

- la mise en œuvre de moyens et dispositifs anti-intrusions ;

- la gestion et traçabilité des accès physiques des personnes sur site ;

- la mise en œuvre de cloisonnement physique garantissant la protection et la confidentialité des activités réalisées pour l'Utilisateur par rapport aux autres activités ;

- la mise en œuvre de moyens et dispositifs de détection et de lutte contre les incendies ;

- la mise en œuvre de moyens de services généraux (énergie, climatisation, réseaux) en cas d'hébergement de systèmes d'informations.

L'application des correctifs de sécurité d'un niveau de sévérité élevé (Score CVSS v3 supérieur à 7) est au maximum de 24 heures après publication. Les correctifs d'un niveau inférieur sont appliqués sous un délai maximal de 2 jours.

Sécurité de l'environnement de travail

La sécurité de l'environnement du poste de travail de l'équipe Authôt est en conformité avec les normes en vigueur et répond en particulier à la :

- prévention contre les virus ou logiciels malveillants avec un logiciel antivirus et antimalware;

- prévention contre le vol d'information en appliquant une politique de gestion des mots de passe robuste et renouvelé régulièrement ;

- prévention contre l'exécution de code et la prise de contrôle à distance avec la restriction des applications et services autorisés ainsi que des privilèges accordés aux utilisateurs ;

- prévention contre les vulnérabilités en mettant à jour les logiciels installés ;

En complément, nous mettons en œuvre :

- Revu du matériel informatique de l'ensemble des salariés une fois par an. Nettoyage avec des logiciels du marché, antivirus, antimalware.
- Sensibilisation régulière sur les enjeux de sécurité : partage d'articles, témoignages.

Surveillance

Nous surveillons l'état de santé et la sécurité de nos serveurs (utilisation des ressources, logs).

Mises à jour
Nous appliquons les mises à jour de sécurité du système d'exploitation de manière automatisée (unattended-upgrades). Nous surveillons les vulnérabilités des dépendances applicatives et planifions leur mise à jour.

Sauvegardes
La base de données est sauvegardée automatiquement par Scaleway tous les jours 00h00. Elle est sauvegardée 7 jours. Le code de l'application est géré via un système de contrôle de version (Git), ce qui permet de restaurer le code source. Il n'y a aucune autre sauvegarde, dite "hors site".

Sécurité dans le développement de l'application

Nos développeurs back-end et front-end sont sensibilisés à la protection informatique et à la sécurité.

Pour la mise en œuvre des processus pour mesurer et garantir la bonne tenue des performances de la solution et leur non régression lors des évolutions de versions, et d'en assurer la performance, nous utilisons l'outil Sentry pour répertorier ce qu'il se passe sur les applications et API.

Nos solutions permettent une reprise sur incident sans perte de données grâce à la redondance du stockage des données.

Un système de double authentification est mis en place pour les administrateurs.

Les mots de passe sont protégés par un token d'authentification. La sécurité du code est préservée des intrusions avec une protection de clé SSH et une double authentification (2FA) sur les services critiques.

Politique de gestion des incidents vis-à-vis de l'Utilisateur

Le circuit d'alerte en cas d'incident de disponibilité, d'intégrité ou de confidentialité vis à vis de l'Utilisateur :
Prévenir les contacts fournis par l'Utilisateur (Responsables de la sécurité des systèmes d'information).
En cas d'incident concernant aussi les données à caractère personnel, le Délégué à la protection des données à caractère personnelles.

Gestion de la réversibilité

Au terme du Contrat ou en cas de rupture anticipée de ce dernier pour quelque cause que ce soit, Authôt restituera à l'Utilisateur une copie de l’intégralité des données dans le même format que celui utilisé par l’Utilisateur. Ou à défaut, dans un format structuré et couramment utilisé (si possible ouvert).

Cette restitution sera constatée par procès-verbal daté et signé par les Parties. Une fois la restitution effectuée, Authôt détruira les copies des Données détenues dans ses systèmes informatiques dans un délai d’un (1) mois et devra en apporter la preuve à l’Utilisateur dans un délai maximal de trois (3) mois suivant la signature du procès-verbal de restitution.

Authôt est tenue à une obligation de résultat concernant la restitution et la suppression des Données communiquées par l’Utilisateur.