# Sécurité, Confidentialité & Infrastructure technique

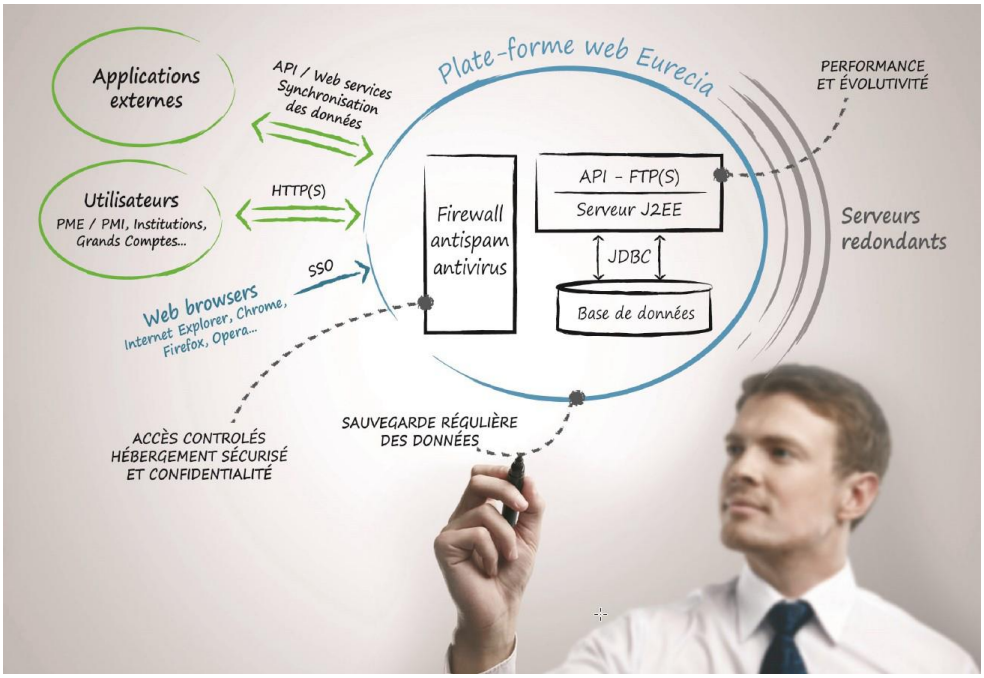
v 1.5

# SECURITE LOGIQUE

## 1. Infrastructure technique

Le logiciel SIRH Eurécia repose sur :

- une architecture logicielle Java en mode SAAS et multi-tenante.
- une architecture système entièrement virtualisée avec VMWare.




### Technologies Java

- Architecture multi-tiers et disponible 24h/24, 7j/7
- Taux de disponibilité de 99,7%
- Technologies open-source Java, JSP, Struts, Hibernate, Spring
- Interopérabilité et ouverture vers le système d'information du client
- Environnement confidentiel et sécurisé

### Serveurs Applicatifs

Basé sur des technologies open-source fiables, performantes et largement éprouvées :

- Système d'exploitation Linux Debian
- Serveur web Apache
- Serveurs d'application Jboss / Tomcat
- Serveurs de base de données MariaDB

# 2. Authentification

### Authentification intégrée

Le mot de passe d'un utilisateur doit respecter les exigences suivantes :

- Une longueur minimale de 8 caractères
- Contenir au moins un chiffre, une lettre minuscule et une lettre majuscule
- Le nouveau mot de passe devra être diffèrent des 3 derniers mots de passe.

Le nombre de tentatives d'authentification à la plateforme Eurécia est limité à 5. Au-delà, le compte de l'utilisateur est bloqué pendant 15 minutes.

### Single Sign-On

Eurécia permet la connexion par SSO au travers du protocole SAML 2.0 **(**Security Assertion Markup Language)**.** Grace à SAML, l'authentification des utilisateurs est gérée en autonomie par la DSI (ex : LDAP) et Eurécia n'accède qu'aux informations strictement nécessaires.
Pour en savoir plus

# 3. Sécurisation des flux web

La plateforme Eurécia est disponible uniquement en HTTPS (TLS).

Les requêtes saisies en http sont automatiquement redirigées de http vers https, de manière totalement transparente pour l'utilisateur.

# 4. Flux réseau

Seuls les flux indispensables sont ouverts au niveau des pare-feux : SSH pour l'administration, SNMP pour la supervision, sauvegarde, DNS, NTP, ….

# 5. API

Eurécia propose une API de type REST en GET.

Elle permet, par WebServices, la récupération de l'ensemble des données saisies dans Eurécia.

La sécurisation des accès se fait par token (passé dans le Header de la requête).

Le nombre de tentatives d'authentification aux WebServices d'Eurécia est limité à 10.

Au-delà, l'adresse IP utilisée est bloquée pendant 60 minutes.

Pour en savoir plus

# 6. Sécurité des données

## En base de données

- Un algorithme de hachage SHA256 salé (irréversible) est utilisé pour le mot de passe.
- Un algorithme de chiffrage AES/CBC pour les informations dites sensibles (ex : bancaires) ayant besoin d'être lues.

## Sur système de fichiers

Les fichiers transférés sur le logiciel Eurécia sont stockés sur des baies NetApp dédiées dans des volumes dédiés auxquels seuls les hyperviseurs de Eurécia ont accès.

Les fichiers sont ensuite classés selon une arborescence propre à chaque client.

# 7. Cloisonnement des données

Le cloisonnement des données est assuré par un **TENANT_ID** associé à chaque client, utilisé dans chaque requête et lié à chaque objet métier stocké en base de données.

L'application Eurécia gère la sécurité sur l'ensemble des transactions effectuées au travers de cet ID qui est validé avec l'utilisateur en session.

# 8. Sauvegarde

Les dumps de base de données sont réalisés 2 fois par jour avec une rétention de 2 mois par société permettant de restaurer l'état d'un client à une date précise.

Des dumps de l'ensemble de la base de données sont réalisés quotidiennement.

Ils sont stockés sur des volumes sécurisés chez notre hébergeur.

En complément de la sauvegarde des données du logiciel (bdd + fichiers), des snapshots des serveurs sont réalisés quotidiennement.

L'ensemble des données sont stockées sur des volumes NetApp qui ont des snapshots quotidiens, de plus le NetApp a une redondance sur un site distant.

*Voir le schéma d'architecture en annexe 1*

# 9. Pare-feu Applicatif WAF Cloudflare

Notre application et nos services Web sont fournis au travers du WAF (Web Application Firewall) de CloudFlare (https://www.cloudflare.com/fr-fr/lp/waf-x/). Ce pare-feu est conforme à la norme PCI 6.6. Cloudflare nous permet également d'optimiser les flux réseaux et le chargement des pages partout dans le monde.

# 10. Pare-feux

Nos environnements disposent de deux niveaux de pare-feu :

- Un pare-feu de type Cisco ASA en tête de réseau qui protège toutes les machines et définit pour chacune d'elles les flux autorisés.
- Chaque machine dispose en plus de son propre pare-feu logiciel sur lequel des restrictions supplémentaires sont implémentées pour limiter les accès de chaque flux selon une liste blanche prédéfinie.

Seuls les flux nécessaires au bon fonctionnement de Eurécia sont autorisés.

# 11. Plan de reprise d'activité

Notre plan de reprise d'activité est assuré à deux niveaux (*voir le schéma d'architecture en Annexe 1*) :

## La réplication des baies NetApp de site à site

L'ensemble des datastores est répliqué ceci nous permet de remonter ces derniers sur le site de secours pour relancer notre infrastructure grâce à la virtualisation VMWare.

## Un environnement actif sur le site de secours

Pour plus de facilité et assurer une reprise d'activité plus rapidement, plusieurs nœuds applicatifs sont actifs ainsi qu'un réplica de la base de données MariaDB. Ceci afin de garantir que l'infrastructure du site de secours est fonctionnelle en permanence et faciliter la reprise d'activité.

Nos engagements varient selon les types d'incidents rencontrés et sont dans le pire des cas :

- Objectif de délai de reprise (RTO) de 4h maximum
- Objectif de point de reprise (RPO) de 5h maximum

En pratique notre infrastructure nous permet d'avoir un **RTO de 2h** car le site de secours est actif et un **RPO de quelques minutes** car les réplications MariaDB et NetApp garantissent l'intégralité de la redondance des données sur nos deux sites avec un latence de quelques minutes maximum.

Voici quelques exemples d'incidents et leurs conséquences sur notre environnement :

| Incident | Objectif de délai de reprise (RTO) | Objectif de point de reprise (RPO) | Commentaires |
|---|---|---|---|
| Panne disque | Pas d'interruption de service | Aucune perte | Les disques sont redondés dans les baies de stockage |
| Panne serveur applicatif | Pas d'interruption de service | Aucune perte | Les serveurs sont en cluster.<br><br>Perte de sessions, déconnexions potentielles |
| Panne serveur de données principal | 1h | Une à deux seconde | Les serveurs applicatifs sont re-configurés pour utiliser le serveur de réplication |
| Panne de la baie de stockage principale | 2h | Une à deux secondes pour les données métiers<br><br>15 minutes pour les fichiers | Les serveurs applicatifs (du site de secours) sont reconfigurés pour utiliser le serveur de réplication. Le point de montage des fichiers est reconfiguré sur le NetApp secondaire |
| Panne d'une baie de stockage secondaire | Pas d'interruption de service | Aucune perte | Perte de sessions, déconnexions potentielles |
| Destruction du site principal<br><br>(ex : perte totale du réseau, défaut d'alimentation électrique total, incendie…) | 2h | Une à deux secondes pour les données métiers<br><br>1 heure maximum pour les fichiers | Les serveurs applicatifs (du site de secours) sont reconfigurés pour utiliser le serveur de réplication. Le point de montage des fichiers est reconfiguré sur le NetApp secondaire |

| | | | |
|---|---|---|---|
| Destruction d'un site secondaire | Pas d'interruption de service | Aucune perte | Perte de sessions, déconnexions potentielles |

Dans l'objectif d'assurer une qualité maximale à nos utilisateurs nous prévoyons de :

- Ajouter un site de secours actif supplémentaire chez un hébergeur différent (OVH)
- Améliorer notre infrastructure pour proposer un PCA entre nos sites et garantir une continuité de service même si un site est défaillant.

# 12. Suivi des failles de sécurité

Eurécia a mis en place un système de gestion des vulnérabilités pour l'ensemble des serveurs.

La solution de gestion IKARE proposée par la société ITRUST permet de réaliser une veille permanente et d'agir sur les vulnérabilités identifiées en un temps minimum.

Le label ITrust Sécurity Metrics est basé sur les exigences ISO 27001, CVSS 2.0 et sur les meilleures pratiques de sécurité.

*Voir le détail du label en annexe 2.*

De plus, au moins une fois par an, Eurécia réalise un audit de sécurité sous la forme d'un test de pénétration réalisé par la société iTrust afin de rester à un niveau optimal de sécurité en fonction des règles de l'art comme le confirme *l'attestation d'iTrust en annexe 3*.

# 13. Administration des environnements

Le personnel d'administration dispose de comptes super utilisateurs nominatifs et unipersonnels sur tous les systèmes de la plate-forme.

Tous les accès se font en SSH avec l'usage d'une clé SSH personnelle.

Les actions nécessitant des privilèges super utilisateur sont consignées dans les journaux systèmes.

# SECURITE PHYSIQUE

## 1. Infrastructure globale

Eurécia garantit l'hébergement des données en France dans 2 Datacenters équivalent **Tiers3+** de la société Fullsave.

L'infrastructure d'hébergement de Fullsave dispose d'interconnexions distinctes avec quatre opérateurs de transit Internet, et d'une solution de protection contre les attaques de type DDoS.

Ces mécanismes, destinés à augmenter la résilience de l'accès aux services d'hébergement, sont complétés par des pare-feu de type Cisco ASA, placés en tête du réseau.

### Les accès physiques

Les locaux et infrastructures de l'hébergeur ne sont pas accessibles au public.

L'accès aux Datacenters n'est autorisé qu'aux personnes dûment habilitées par Fullsave, à savoir :

- Les collaborateurs Fullsave.
- Les sous-traitants en charge des différentes maintenances d'infrastructures.

## 2. Protection des infrastructures

### Alarme

Tous les locaux sont sous système d'alarme.

L'entrée dans le Datacenter n'est possible qu'après autorisation et la désactivation de l'alarme par le personnel Fullsave.

### Contrôles d'accès

Les accès aux locaux sont contrôlés par badge et contrôle biométrique.

Les Datacenters sont découpés en zones sécurisées accessibles seulement aux personnes habilitées, enrôlées dans le système biométrique.

Les visiteurs autorisés ne peuvent accéder qu'aux zones pour lesquelles ils sont habilités (salles blanches, Meet-Me-Room, locaux techniques).

Dans les salles, chaque baie dispose de son propre accès par clé ou code et les accès sont tracés et conservés durant 60 jours (déclaration CNIL 1792778).

Il est connecté à un système de détection d'incendie qui déclenche automatiquement le dispositif de protection contre l'incendie après une détection double de fumée et de chaleur (Conforme aux certifications APSAD R7).

## Vidéo surveillance

L'ensemble des locaux de Fullsave est sous vidéo surveillance : les Datacenters et les bureaux, les zones de circulation, les salles blanches, les zones techniques, ainsi que le périmètre extérieur.

Les vidéos sont enregistrées et conservées pendant 60 jours (Déclaration CNIL 1792720).

## Protection incendie

Un système de protection contre l'incendie est actif dans toutes les salles et coursives de circulation, permettant de lutter contre les incendies de solides et de liquides.

Il assure une protection contre la quasi-totalité des risques d'incendie. (Conforme aux certifications APSAD R13 et D2).

Il est connecté à un système de détection d'incendie qui déclenche automatiquement le dispositif de protection contre l'incendie après une détection double de fumée et de chaleur. (Conforme aux certifications APSAD R7).

## Alimentation électrique

Le Datacenter propose une double chaîne électrique complète jusqu'au serveur final :

- Double induction EDF
- Deux groupes électrogènes
- Deux salles onduleurs indépendantes
- Deux tableaux électriques dans chaque salle
- Deux bandeaux d'alimentations dans chaque baie

## Protection contre un dégât des eaux

Les Datacenters sont installés hors des zones inondables. Les salles d'hébergement sont toutes sur un faux-plancher surélevé.

L'espace sous celui-ci est vide d'équipement et pourvu de détecteurs d'eau.

## Zones de livraison

Les zones de livraisons/chargements sont dans un espace sécurisé, distinct des salles blanches.

Les livraisons sont déballées et contrôlées avant d'être amenées en salles blanches.

Les cartons et les différents éléments de transport (palettes, emballages…) ne dépassent pas la zone de contrôle, et n'entrent en aucun cas dans les salles blanches.

# SECURITE ORGANISATIONNELLE

## Entre Fullsave et Eurécia

Les données, documents ou renseignements confiés à FullSave par Eurécia ainsi que tout produit provenant de leur traitement sont couverts par le secret professionnel.

Les administrateurs système de FullSave sont tenus à des obligations particulières :

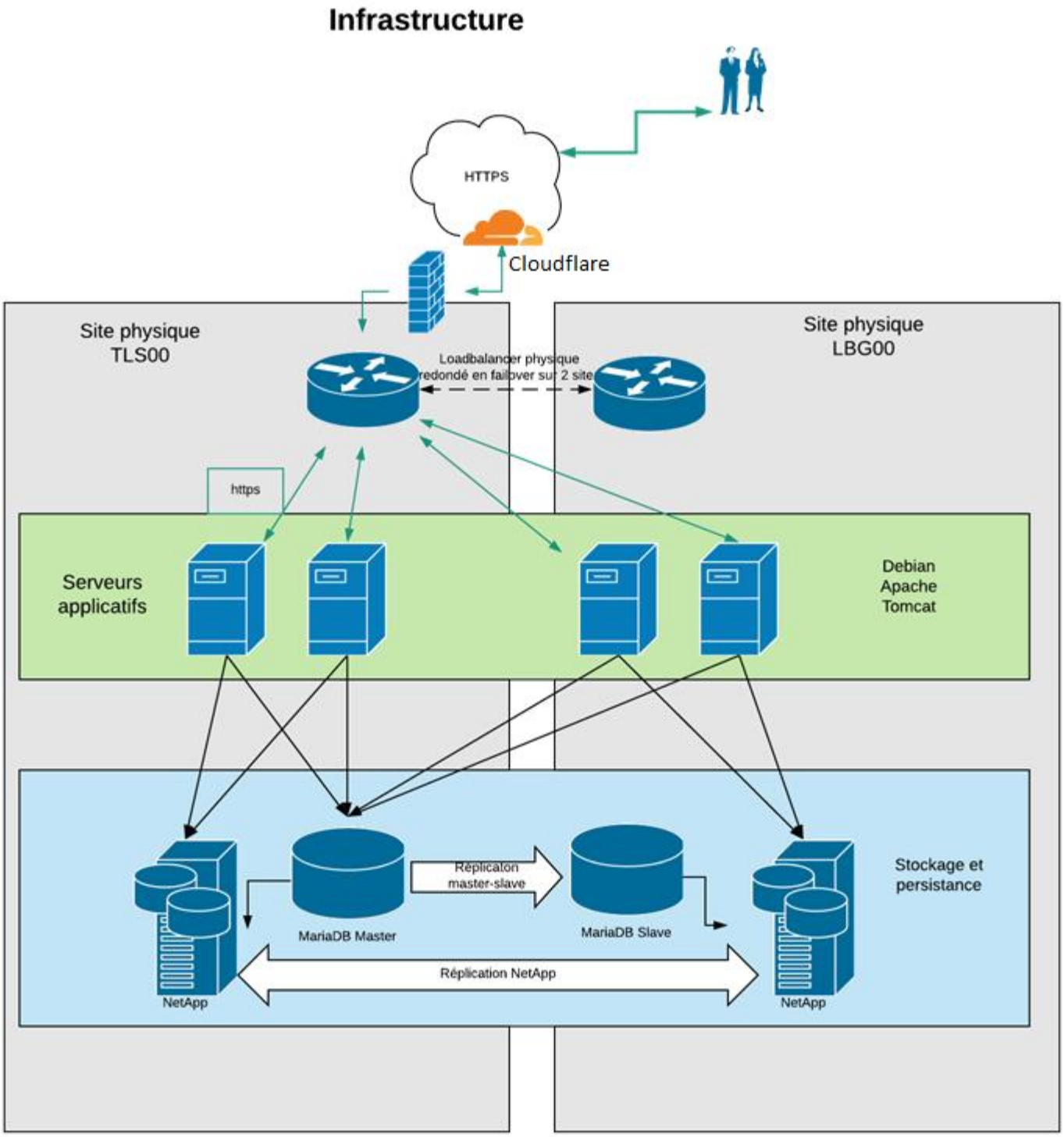
- De **loyauté** : étant investi de larges pouvoirs de surveillance sur les données qui sont hébergées sur les infrastructures de FullSave, le respect de règles d'éthique est attendu de leurs parts.
- De **transparence** : dans l'exercice de leurs missions dans le cadre du règlement intérieur et de la charte informatique de FullSave.
- De **confidentialité** : tenant notamment au secret professionnel. Ils ne doivent pas divulguer d'informations auxquelles ils auraient pu avoir accès lors de l'exercice de leurs fonctions, a fortiori lorsqu'elles sont couvertes par le droit à la vie privée ou le secret des correspondances, à moins qu'une disposition législative ne l'impose (ex. en cas de découverte de contenus illicites).

## Entre Eurécia et son client

L'ensemble des engagements pris par Eurécia sont édités dans les conditions générales de vente.
Pour en savoir plus

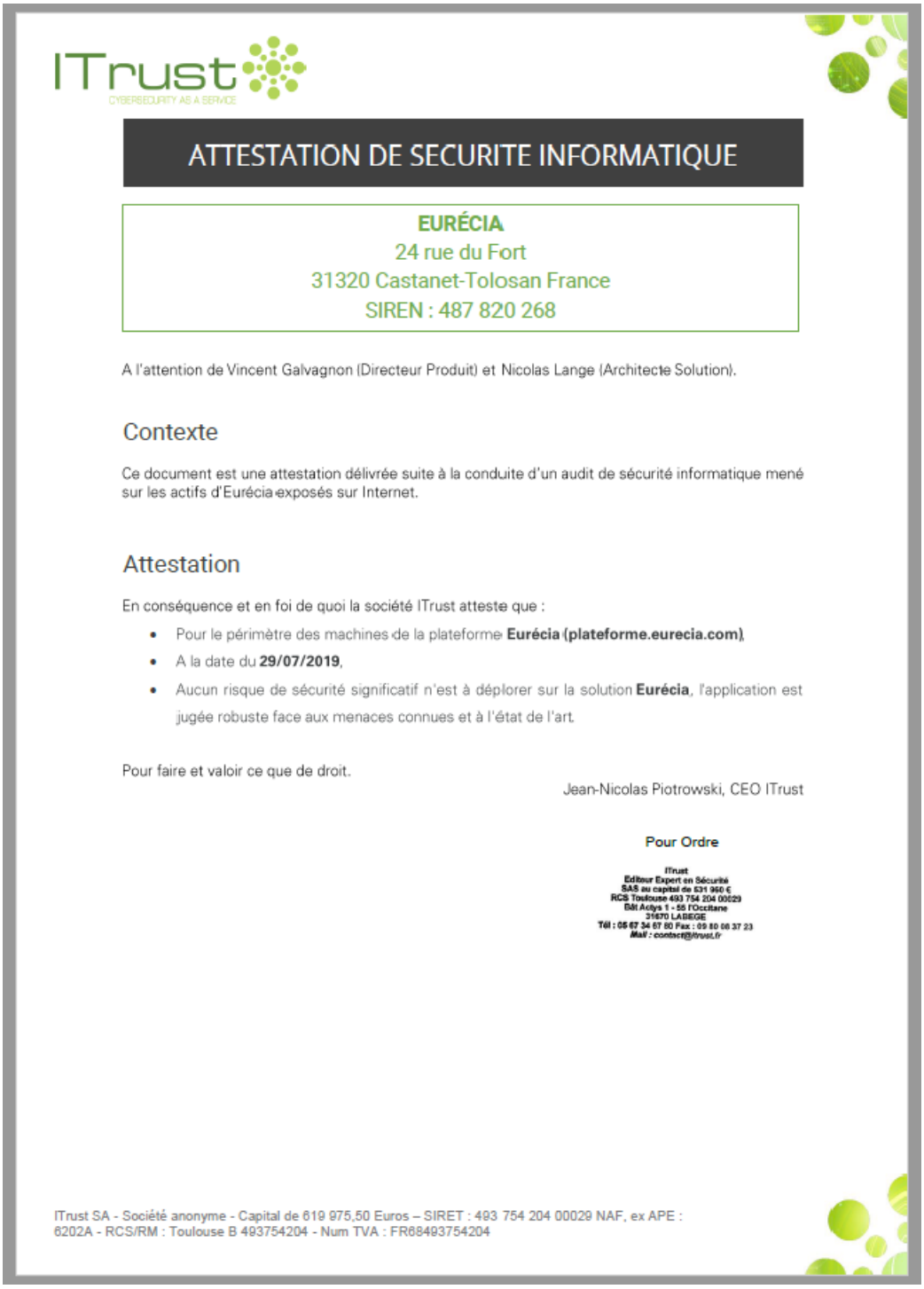
# ANNEXES

## 1. Schéma d'architecture



# 2. Label ITrust Security Metrics

# 3. Attestation de sécurité informatique iTrust



ITrust
CYBERSECURITY AS A SERVICE

## ATTESTATION DE SECURITE INFORMATIQUE

**EURÉCIA**
24 rue du Fort
31320 Castanet-Tolosan France
SIREN : 487 820 268

A l'attention de Vincent Galvagnon (Directeur Produit) et Nicolas Lange (Architecte Solution).

### Contexte

Ce document est une attestation délivrée suite à la conduite d'un audit de sécurité informatique mené sur les actifs d'Eurécia exposés sur Internet.

### Attestation

En conséquence et en foi de quoi la société ITrust atteste que :

- Pour le périmètre des machines de la plateforme **Eurécia (plateforme.eurecia.com)**,
- A la date du **29/07/2019**,
- Aucun risque de sécurité significatif n'est à déplorer sur la solution **Eurécia**, l'application est jugée robuste face aux menaces connues et à l'état de l'art.

Pour faire et valoir ce que de droit.

Jean-Nicolas Piotrowski, CEO ITrust

**Pour Ordre**

ITrust
Editeur Expert en Sécurité
SAS au capital de 531 960 €
RCS Toulouse 493 754 204 00029
Bât Actys 1 - 55 l'Occitane
31670 LABEGE
Tél : 05 67 34 67 80 Fax : 09 80 08 37 23
Mail : contact@itrust.fr

ITrust SA - Société anonyme - Capital de 619 975,50 Euros – SIRET : 493 754 204 00029 NAF, ex APE : 6202A - RCS/RM : Toulouse B 493754204 - Num TVA : FR68493754204