AMOSSYS

EVERTRUST

Cible de sécurité CSPN

Produit STREAM version 1.3.0

Référence : CSPN-CDS-STREAM v1.3.0-1.30

Date : 28/04/2025

Référence interne : EVT002

Copyright AMOSSYS

Siège : Immeuble Le Ouessant • Bâtiment B • 11 rue Maurice Fabre • 35000 Rennes • France • **www.amossys.fr**

SIRET : 493 348 890 00051 • **NAF** : 6202 A • RCS Rennes B 493 348 890 • SAS au capital de 38.000 Euros

FICHE D'EVOLUTIONS

Révision	Date	Description	Rédacteur
0.01	11/04/2023	Création du document	Émilie PRUNIER
0.02	24/04/2023	Complément d'informations	Emilie PRUNIER
0.03	03/05/2023	Complément d'informations	Emilie PRUNIER
0.04	22/05/2023	Complément d'informations	Emilie PRUNIER
1.00	21/06/2023	Version finale, communiquée à l'ANSSI lors du dépôt du dossier	Emilie PRUNIER/ Gilles POIRET
1.10	16/10/2023	Version mis à jour avant l'évaluation : précision sur le HSM, et mise à jour des COTS et dépendances	Gilles POIRET
1.20	17/06/2024	Précisions apportées sur les hypothèses et le périmètre de l'analyse. Passage en version 1.3.0 du produit.	Gilles POIRET
1.21	30/09/2024	Prise en compte des remarques de l'ANSSI	Gilles POIRET
1.30	28/04/2025	Prise en compte des remarques de l'ANSSI	Gilles POIRET

Ce document a été validé par EverTrust.

SOMMAIRE

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN promu par l'ANSSI, du produit **STREAM**, développé par la société **EverTrust**.

Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation d'**EverTrust**. Les mises à jour de ce document sont effectuées par l'équipe projet d'**AMOSSYS**.

1.2. IDENTIFICATION DU PRODUIT

Éditeur	**EverTrust** 24 rue de Londres 75009 Paris, France
Lien vers l'organisation	https://evertrust.io
Nom commercial du produit	STREAM
Numéro de la version évaluée	1.3.0

1.3. REFERENCES

Pour l'établissement de la présente cible de sécurité, les documents suivants ont été consultés par le rédacteur.

Référence	Description
ADMIN-GUIDE	"Administration Guide", Doc Writer EverTrust R&D
INSTALL-GUIDE	"Installation Guide", Doc Writer EverTrust R&D
ANSSI-PROC	« CERTIFICATION DE SECURITE DE PREMIER NIVEAU DES PRODUITS DES TECHNOLOGIES DE L'INFORMATION », ANSSI-CSPN-CER-P-01_v5.0

Tableau 1 - Références documentaires

1.4. GLOSSAIRE

Acronyme	Description
AC	Autorité de Certification
AIA	*Authority Information Access*
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
COTS	*Commercial Off-The-Shelf*
CRLDP	*Certificate Revocation List Distribution Point*
CRL	*Certificate Revocation List*
CSPN	Certification de Sécurité de Premier Niveau
DN	*Distinguished Name*
DPC	Déclaration des Procédures de Certification
EKU	*Extended Key Usage*

Acronyme	Description
HSM	*Hardware Security Module*
JWT	*Json Web Token*
JWS	*Json Web Signature*
KMS	*Key Management System*
OID	*Object Identifier*
PC	Politique de Certification
PEM	*Privacy Enhanced Mail*
RBAC	*Role Based Access Control*
SAN	*Subject Alternative Name*
TOE	*Target Of Evaluation*
SGBD	Système de Gestion de Bases de Données

Tableau 2 - Glossaire

2. DESCRIPTION DU PRODUIT

2.1. DESCRIPTION GENERALE

Le produit **STREAM** est développé par **EverTrust**, un éditeur de logiciels spécialisé dans la gestion du cycle de vie des certificats numériques.

STREAM se présente comme un logiciel d'autorité de certification (AC). Il gère l'émission et la révocation de certificats X509v3, ainsi que l'émission de la liste des certificats révoqués (CRL). Le logiciel **STREAM** peut héberger plusieurs autorités de certifications distinctes au sein d'une même installation.

Conçu pour être très performant et disponible, il est également très flexible et peut s'adapter à différents environnements, en sécurisant les clés de l'autorité de certificats à l'aide d'un HSM ou d'un KMS Cloud.

STREAM est nativement multilingue et fourni en anglais et en français. Il peut se déployer sur une seule machine ou bien en haute disponibilité à 3 nœuds minimum.

Une fois correctement installé, **STREAM** propose une interface complète pour gérer le cycle de vie des ACs, et notamment les cérémonies des clés, ainsi qu'un système de gabarits permettant de déterminer le contenu des certificats en termes de durée de vie, usage de clé et usage de clé étendu, d'informations liées à l'AC émettrice (CRLDP, AIA, PC/DPC), et de champs de données (*Distinguished Name* du sujet, *Subject Alternative Name* et extensions diverses).

La garantie de la protection des données s'effectue via plusieurs axes :

- le **contrôle d'accès** : les utilisateurs doivent s'authentifier au serveur par identifiant/mot de passe ou par certificat ;
- la **confidentialité des données** : le transfert des informations s'effectue via un protocole de communication sécurisée.

2.2. PRINCIPE DE FONCTIONNEMENT

Avant la mise à disposition du produit **STREAM** aux utilisateurs, il est nécessaire de suivre la procédure d'installation et de configuration du produit (respectivement [INSTALL-GUIDE] et [ADMIN-GUIDE]).

Le produit **STREAM** est ensuite prêt à utiliser. L'authentification des utilisateurs s'effectue par *login*/mot de passe ou bien par certificat. Un système de gestion des droits RBAC (*Role-Based Access Control)* gère les autorisations d'accès à **STREAM**.

La solution s'administre via une interface d'administration Web, permettant d'accéder à la configuration des principales fonctionnalités du produit :

- Gestion des autorités de certification : possibilité d'importer une autorité de certification externe ou déjà existante et de délivrer une nouvelle autorité de certification racine ;
- Gestion des *Keystores* et des clés : les clés sont regroupées dans des conteneurs de clés appelés *Keystores.* Le produit **STREAM** gère trois types de dépôts de clés : les dépôts de clés logiciels, les PKCS#11 HSMs et les KMS Cloud. Quel que soit le type de *Keystores* mise en place, il est possible pour un utilisateur d'ajouter, de voir et de supprimer une clé d'un *keystore* ;
- Gestion de la sécurité : création de comptes, gestion des rôles et autorisations ;
- Gestion de la publication des CRL : **STREAM** permet de configurer des listes de révocation de certificats pour une autorité de certification. Il est possible pour un utilisateur de voir

  les informations concernant les CRLs des ACs configurées et de les télécharger. Le format standard de l'URL de téléchargement est le suivant :
  http(s)://[stream_url]/crls/CA_internal_name. Cette URL est accessible à tous sans authentification préalable, que ce soit par HTTP ou HTTPS. Les CRLs sont par défaut

générées au format DER. Par ailleurs, **STREAM** offre la possibilité aux utilisateurs de pousser les CRLs dans des buckets S3 dès leur génération**.** Pour ce faire, il est nécessaire de configurer un stockage externe au préalable. La publication dans les annuaires LDAP est également disponible ;

- Gestion système (proxy HTTP et événements) ;
- Gestion des informations de licence ;
- Gestion des modèles (templates) de certificats : il est possible pour un utilisateur de définir un nouveau modèle de certificat. À savoir que **STREAM** utilise la notion de modèle de certificat afin d'ajouter des vérifications supplémentaires lors de l'enregistrement d'un certificat. Il est également possible pour un utilisateur de créer et de gérer son propre EKU (*Extended Key Usage*) à condition qu'il dispose d'un OID.

En outre, l'interface web permet de rechercher et révoquer les certificats émis par **STREAM**, ainsi que d'émettre des certificats sur la base de la présentation d'une CSR PKCS#10. Par ailleurs, cette API permet également aux logiciels tiers, et en premier lieu *EverTrust Horizon*, de s'interfacer avec **STREAM**.

2.3. DESCRIPTION DES DEPENDANCES EXTERNES

Une dépendance externe est non embarquée directement par la TOE. Elle peut être fournie par le système hôte, ou installé séparément. Son maintien en condition de sécurité est assuré par l'administrateur du système hôte.

Cette section liste ces deux types de dépendances, suivant qu'elles soient ou non embarquées dans la distribution du système d'exploitation.

Une seule dépendance non embarquée dans le système est requise : le système de gestion de base de données (SGBD). Seul le SGBD Mongo DB, en version 5.x.x à 6.x.x, est supporté par la TOE.

À cela s'ajoutent les dépendances issues du système hôte, dont la liste est présentée dans le Tableau 3 ci-dessous.

COTS	Version utilisée	Toujours maintenu
OpenJDK	17 (version mineure via le système de mise à jour de RedHat)	Oui
NGINX	1.20 (version mineure via le système de mise à jour RedHat)	Oui
Dialog	1.3 (version mineure via le système de mise à jour RedHat)	Oui
OpenSSL	3.0 (version mineure via le système de mise à jour RedHat)	Oui
TAR/ZIP/UNZIP	1.34/3.0/6.0 (version mineure via le système de mise à jour RedHat)	Oui

Tableau 3 - Liste des COTS externes issus du serveur hôte utilisés par le produit

Note : les scripts utilisent également les outils standard disponibles dans la distribution Linux, tels que bash, grep, sed et curl.

2.4. DESCRIPTION DES COTS INTEGRES

Les composants tiers intégrés au produit (COTS) sont présentés dans le tableau suivant. Les colonnes « Dernière version », « à jour » et « toujours maintenu » sont liées à la version utilisée, et non pas, le cas échéant, à la dernière branche du COTS.

COTS	Version utilisée	Dernière version	Patch ou modifications appliquées	À jour	Toujours maintenu
Pekko	1.0.2	1.0.2	-	Oui	Oui
Pekko Management	1.0.0	1.0.0	-	Oui	Oui
AWS SDK (kms, sts, s3)	2.25.60	2.25.60	-	Oui	Oui
BouncyCastle	1.78.1	1.78.1	-	Oui	Oui
MongoDB Community	6.0.15	6.0.15	-	Oui sur la branche Mongo 6 LTS	Oui
Apache Commons Codec	1.17	1.17	-	Oui	Oui
IAIK Wrapper	1.6.11	1.6.11	-	Oui	Oui
Jose4J	0.9.6	0.9.6	-	Oui	Oui
Kamon	2.7.2	2.7.2	-	Oui	Oui
Kanela Agent	1.0.18	1.0.18	-	Oui	Oui
Play! Framework	3.0.3	3.0.3	-	Oui	Oui
Quartz	2.3.2	2.3.2	-	Oui	Oui
Scaffeine	5.2.1	5.2.1	-	Oui	Oui
Scala	2.13.13	3.4.2	-	Oui, sur la branche 2.x	Oui
ScalaPB	0.11.13	0.11.13	-	Oui	Oui
UnboundId LDAP SDK	7.0.0	7.0.0	-	Oui	Oui
ReactiveMongo	1.1.0-RC12	1.1.0-RC12	-	Oui	Oui
Tink	1.13.0	1.13.0	-	Oui	Oui
ICU4J	75.1	75.1	-	Oui	Oui
Guava	33.2.0	33.2.0	-	Oui	Oui
DD-Plist	1.28	1.28	-	Oui	Oui
GRPC-Context	1.64.0	1.64.0	-	Oui	Oui
Logstash Logback	7.4	7.4	-	Oui	Oui
Vue.js	3.4.27	3.4.27	-	Oui	Oui
Quasar	2.16.4	2.16.4	-	Oui	Oui

Tableau 4 – Liste des COTS internes utilisés par le produit

Note : Cette liste ne contient que les dépendances immédiates de STREAM.

2.5. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

2.5.1. Matériel compatible ou dédié

STREAM fonctionne sur des systèmes d'exploitation du type Unix. Les éléments suivants sont considérés comme des prérequis d'un point de vue système et logiciel :

- Un serveur EL [8.x-9.x] x64 (RHEL/Alma/Rocky) fonctionnant avec le réseau configuré et SELinux activé ;
- Un accès au serveur avec des privilèges administrateurs (*root*), via la console d'administration.

La base de données prise en charge par la TOE est Mongo DB en version 6.x.

Dans le cadre de l'évaluation, un HSM de type `Utimaco CryptoServer CP5 LAN (sous forme d'appliance virtuelle)` sera utilisé afin de stocker et protéger les clés cryptographiques d'ACs. Un *middleware* `SecurityServer`, également édité par `Utimaco`, sera installé sur le serveur afin de permettre les communications entre le serveur **STREAM** et le HSM.

2.5.2. Système d'exploitation retenu

EverTrust propose deux modes d'installation :

- Une installation à partir d'un *package* sur un serveur exécutant RHEL/Alma/Rocky 8.x/9.x x64 ;
- Une installation native *cloud* utilisant Kubernetes.

Dans le cadre de l'évaluation, le produit **STREAM** sera installé sur un serveur Rocky Linux 9.4 à jour, les packages nécessaires seront installés via RPM. MongoDB sera installé en version 6.0.15.

2.6. PERIMETRE DE L'EVALUATION

2.6.1. Périmètre

Le périmètre de l'évaluation est composé de l'autorité de certification. L'analyse portera sur les points suivants :

- La conformité du support cryptographique : paramétrage des clés générées transmis par **STREAM** ;
- L'authentification par certificat et la gestion des rôles utilisateurs ;
- La journalisation des événements de sécurité ;
- La sécurité des communications entre les composants de la solution :
    - Entre le serveur et les postes clients ;
    - Entre les composants **STREAM** sur le serveur.

La configuration des dépendances résultante du processus d'installation est également considérée dans le périmètre (Nginx/MongoDB notamment). C'est également le cas pour la configuration utilisée pour se connecter au HSM.

Les éléments considérés comme hors TOE sont les suivants :

- La génération et le stockage externe des clés dans le HSM. Dans le cadre de l'évaluation, le HSM utilisé sera un HSM `Utimaco CryptoServer CP5`;
- Les fonctionnalités de stockage des clés d'ACs dans des dépôts logiciels ou Cloud KMS ;
- La publication de CRL S3 dans des *buckets* S3 ou dans des annuaires LDAP ;
- L'utilisation d'OpenSSH pour se connecter au serveur est exclue, et il est de la responsabilité de l'installateur de la solution d'en désactiver le fonctionnement.
- L'authentification par mot de passe ;
- Les communications entre le HSM et sa bibliothèque cliente utilisée par la TOE.

La configuration du produit évalué est présentée dans le tableau suivant.

Composant du système global		Inclus dans la cible d'évaluation (TOE)	Non évalué (environnement de la TOE)	
			Supposé de confiance[1]	Est un attaquant potentiel
Composant STREAM	Système d'exploitation Rocky Linux		√	
	Fonctions cryptographiques : BouncyCastle	√		
	Base de données : MongoDB		√	
	NGINX		√	
Composant HSM	HSM `Utimaco CryptoServer CP5 LAN Simulator`		√	

Tableau 5 - Configuration du produit évalué

2.6.2. Plateforme d'évaluation

La plateforme suivante sera utilisée.

[1] La bonne configuration des composants de confiance est susceptible d'être vérifiée durant l'évaluation.

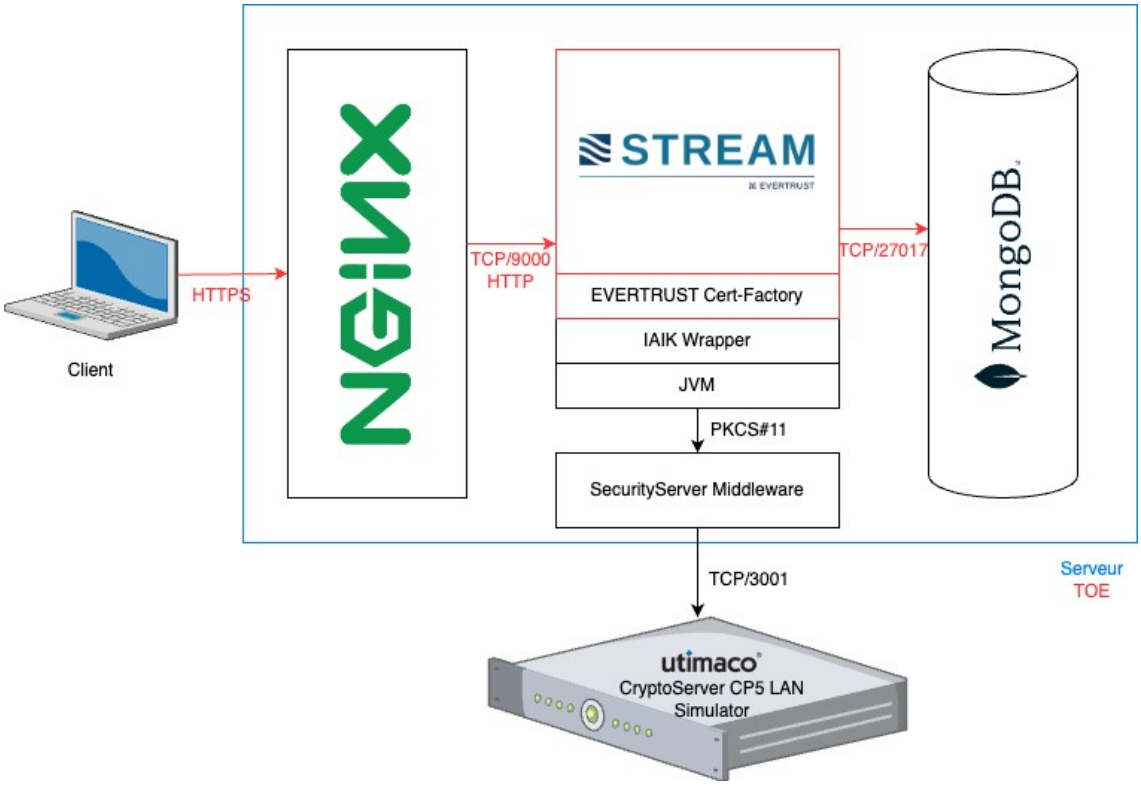

Figure 1 - Plateforme d'évaluation

`EVERTRUST Cert-Factory` correspond à la bibliothèque qui s'interface entre `BouncyCastle` et `IAIK Wrapper`, afin de piloter toutes les fonctions cryptographiques. En effet, lors des requêtes HSM, **STREAM** fait appel à la librairie `Cert-Factory` qui fait appel à `IAIK Wrapper` et qui fait ensuite appel au middleware `Utimaco SecurityServer` via PKCS#11. Cette architecture permet de mutualiser tous les accès cryptographiques entre les différents produits.

Le HSM étant en dehors de l'évaluation, il a été décidé d'utiliser une `appliance logicielle` en lieu et place du HSM physique afin de simplifier les travaux, tout en conservant strictement la même chaîne de connexion.

3. PROBLEMATIQUE DE SECURITE

Ce chapitre décrit le panorama sécuritaire de la TOE. Il consiste en une présentation des acteurs, des ressources stratégiques et des hypothèses.

3.1. DESCRIPTION DES UTILISATEURS DU PRODUIT

Par définition, les utilisateurs concernent les personnes et les services applicatifs qui interagissent avec le produit évalué.

Les rôles suivants sont à considérer dans le cadre de l'évaluation de sécurité :

- **Utilisateur** : les utilisateurs « finaux » utilisant les services proposés par le logiciel **STREAM** et en particulier la possibilité d'enrôler des certificats et de les révoquer ;
- **Utilisateur privilégié** ayant obtenu des droits élevés. Cet utilisateur est par hypothèse de confiance.
- **Administrateur métier** (officier de sécurité, responsable notamment de la configuration métier du produit) ;
- **Administrateur système**.

Il est à noter que tous ces utilisateurs disposent de droits spécifiques dans le produit.

3.2. DESCRIPTION DES BIENS SENSIBLES

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon des critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité, confidentialité et authenticité. Les biens considérés pour l'évaluation sont les suivants :

- **B1.Données métier**

  La base de données stocke les informations suivantes :

- Informations relatives aux certificats (PEM, date et raison de révocation, etc.) ;
- Informations relatives aux droits des utilisateurs (système RBAC de gestion des permissions) ;
- Informations relatives au paramétrage de la gestion des AC (émission des CRLs, gestion des *keystores*).

  Il est à noter que les divers mots de passe utilisés par **STREAM** pour se connecter à des services tiers (PIN HSM, Cloud KMS, S3, annuaire LDAP), sont stockés chiffrés en base de données.

  Besoin de sécurité : disponibilité, intégrité et confidentialité.

- **B2.Données d'authentification**

  Les données permettant aux utilisateurs de s'authentifier auprès de la TOE. Ces données sont stockées dans la base de données de **STREAM**, et contiennent :

- Les noms d'utilisateur et mot de passe hachés pour l'authentification par mot de passe ;
- Le DN du sujet du certificat pour l'authentification par certificat.

  Besoin de sécurité : confidentialité et intégrité.

- **B3.Matériel Cryptographique**

  Le matériel cryptographique utilisé pour signer/vérifier, générer/révoquer des certificats et gérer les clés. Dans le cadre de l'évaluation, un HSM de type `Utimaco CryptoServer CP5 LAN` sera utilisé, permettant ainsi de générer, stocker et protéger au repos les clés d'ACs.

  Besoin de sécurité : disponibilité, intégrité et confidentialité.

- **B4.Configuration**

  Les données relatives à la configuration de la TOE doivent être disponibles et intègres.

  Besoin de sécurité : disponibilité et intégrité.

- **B5.Journaux**

  Les événements de sécurité journalisés par la TOE. Ils sont stockés en base de données. **STREAM** permet d'activer la signature et le chaînage des journaux d'événement (cette fonctionnalité est activée par défaut et désactiver ce comportement nécessite une configuration explicite).

  Besoin de sécurité : disponibilité, intégrité et confidentialité.

- **B6.Système Hôte**

  Le système d'exploitation du logiciel **STREAM**.

  Besoin de sécurité : intégrité.

Les besoins de sécurité de chacun des biens à protéger sont synthétisés dans le tableau suivant.

Biens sensibles	Disponibilité	Intégrité	Confidentialité
Données métier	√	√	√
Données d'authentification		√	√
Matériel Cryptographique	√	√	√
Configuration	√	√	
Journaux	√	√	√
Système Hôte		√	

Tableau 6 - Résumé des besoins de sécurité des biens sensibles

3.3. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement. Les hypothèses sur l'environnement de la TOE à considérer sont les suivantes :

- **H1.Installation intègre**

  Tous les outils nécessaires à l'installation et à la configuration du produit sont intègres. Seuls les composants nécessaires à la TOE ont été installés sur ce serveur dédié.

- **H2.Administrateur métier et système formé**

  Les administrateurs sont de confiance, et formés pour l'utilisation et l'administration du produit et du système d'exploitation support de la TOE. Les administrateurs métier ne délèguent des droits étendus qu'à des utilisateurs finaux de confiance. Le navigateur web qu'il utilise pour les tâches d'administration métier est à jour.

- **H3. Utilisateur final promu administrateur formé et de confiance**

  Certains utilisateurs finaux peuvent se voir attribuer des rôles d'administration. Cela ne peut concerner que des utilisateurs finaux de confiance qui seront alors formés. Le navigateur web qu'il utilise pour les tâches d'administration métier est à jour.

- **H4.Utilisateur final non privilégié**

  Les utilisateurs finaux de la TOE ne disposent pas de privilèges permettant la configuration de celle-ci.

- **H5.HSM fiable**

  La TOE fait appel à un HSM, le HSM étant certifié Critères Communs EAL4+. Il est supposé intègre. Il est administré suivant ses guides de sécurité et d'administration. Notamment, les communications entre le HSM et sa bibliothèque cliente sont configurées de manière sécurisée (chiffrement robuste). De plus, il réalise les fonctions cryptographiques attendues suivant ses spécifications.

- **H6. Plate-forme supervisée**

Une supervision efficiente de la plate-forme hébergeant la TOE est mise en œuvre. Elle concerne a minima ses composants système (processus, disque, cpu, mémoire).

- **H7. Environnement serveur sécurisé**

  La machine hébergeant la TOE se trouve dans une zone sécurisée réputée de confiance. En particulier, elle est protégée physiquement en accès et accessible au seul personnel autorisé.

3.4. DESCRIPTION DES MENACES

Par définition, une menace est une action ou un événement susceptible de porter préjudice à la sécurité de la TOE.

Les agents menaçants à considérer pour l'évaluation de sécurité sont les suivants :

- un attaquant présent sur le réseau. Il peut :
  - tenter d'intercepter les communications réseau ;
  - accéder à l'interface web, mais ne dispose pas d'un compte utilisateur.
- un attaquant disposant d'un compte utilisateur non privilégié sur la TOE. Il pourrait tenter d'élever ses privilèges sur la TOE.

Les administrateurs ne sont pas considérés comme des attaquants (H2/H3).

Par conséquent, la TOE doit résister à ces agents menaçants ainsi qu'aux moyens logiciels mis en œuvre par ces derniers. Ces moyens sont les suivants.

Moyens exploités par les agents menaçants	Moyen mis en œuvre		TOE résistante à un attaquant	
	Logiciel	Matériel	Local	Distant
Vulnérabilité de la session utilisateur	√		√	√
Vol de moyens d'authentification	√			√
Vulnérabilité réseau	√			√
Vulnérabilité du système	√			√

Tableau 7 – Moyens mis en œuvre par les agents menaçants

Les menaces portant sur les biens sensibles de la TOE sont les suivantes :

- **M1.Corruption des données stockées**

  Un attaquant parvient à modifier les données stockées en base de données.

- **M2.Vol des données stockées**

  Un attaquant parvient à voler les données stockées en base de données.

- **M3.Vol des données d'authentification**

  Un attaquant parvient à voler des données d'authentification. Cela peut être fait en interceptant les communications réseau ou à cause d'un mauvais stockage de ces données.

- **M4.Récupération du matériel cryptographique**

  Un attaquant parvient à récupérer une partie du matériel cryptographique utilisé par la TOE.

- **M5.Modification du matériel cryptographique**

  Un attaquant parvient à modifier de façon illégitime le matériel cryptographique utilisé par la TOE.

- **M6.Contournement de l'authentification**

  Un attaquant parvient à contourner le mécanisme d'authentification.

- **M7.Altération des journaux**

  Un attaquant parvient à altérer les journaux du produit dans le but de masquer un événement de sécurité.

- **M8.Usurpation d'identité**

  Un attaquant authentifié réussit à se faire passer pour un autre utilisateur ou un utilisateur non authentifié tente d'usurper l'identité d'un utilisateur authentifié dans le but d'élever ses privilèges sur la TOE.

- **M9.Altération de la configuration**

  Un attaquant parvient à corrompre la configuration du produit à cause d'un mauvais contrôle d'accès ou d'une vulnérabilité de la TOE. L'attaquant serait en mesure d'interrompre le service, d'influencer sur les certificats émis et de créer des utilisateurs.

3.5. DESCRIPTION DES FONCTIONS

3.5.1. Fonctions métier

Les fonctions métiers sont l'ensemble des fonctions actives et mises en œuvre par la TOE pour assurer son fonctionnement et répondre au besoin pour lequel elle a été développée. Ces fonctions métier ne seront pas évaluées en conformité, mais seront prises en compte en tant que vecteurs d'attaque potentiels sur la TOE.

3.5.2. Fonctions de sécurité

Les fonctions de sécurité sont l'ensemble des mesures techniques et des mécanismes mis en œuvre par la TOE pour protéger de façon proportionnée ses biens sensibles contre les menaces identifiées. Les fonctions de sécurité de la TOE à considérer sont les suivantes :

- **FS1.Communications sécurisées**

  Les communications avec la TOE et ses utilisateurs sont réalisées au sein d'un protocole de communication sécurisé.

- **FS2.Authentification et contrôle d'accès**

  La TOE met en place une authentification et un contrôle d'accès**.**

  Un compte X509 utilise le certificat d'authentification de l'utilisateur pour se connecter à la TOE. Dans ce dernier cas, c'est la connexion TLS qui est utilisée pour effectuer l'authentification mutuelle. De plus, des rôles sont assignés aux utilisateurs.

  Les rôles sont intégralement configurables et sont fondés sur des permissions. Pour la partie configuration, chaque section a une permission « audit » et une permission « gestion ». Pour la partie gestion du cycle de vie des certificats, chaque AC dispose d'une permission « enrôler » et d'une permission « révoquer ».

  L'authentification par login/mot de passe, possible pour un compte local à STREAM, est désactivée après la cérémonie des clés qui a lieu juste après l'installation.

- **FS3.Journalisation**

  La TOE journalise les événements de sécurité. Les journaux sont des objets Json contenant un sceau de signature qui correspond à un jeton JWT de type JWS. Le mécanisme de gestion des événements de **STREAM** est le suivant :

- Les événements sont ajoutés dans une collection Mongo (`pending_events`), utilisée comme une file de messages de type *FIFO* (First In First Out). Ces évènements sont signés au format JWT ;
- Toutes les 5 secondes (cette période est configurable), un acteur (*thread* pekko) prend la liste des événements stockés dans la collection « `pending_events` » en respectant la logique FIFO et en vérifiant la signature de chaque évènement ;
- Pour chaque événement de la liste à traiter, la TOE réalise les points suivants :
- Génère le jeton de signature JWT à l'aide :
    - De l'identifiant Mongo de l'événement ;
    - Du hash de l'événement ;
    - De l'identifiant Mongo du dernier événement inséré dans la collection des événements (`events`).
- Insère l'événement enrichi de son « `seal` » dans la collection des événements (`events`) ;
- Supprime l'événement de la collection des événements à traiter (`pending_events`).

  Ces journaux sont stockés dans la base de données Mongo, et accédés par STREAM. Les accès aux journaux sont par conséquent protégés par les mécanismes d'accès à Mongo. Dans le cadre de l'évaluation, il est rappelé que la base est locale sur la machine, écoute sur l'interface locale, et qu'un *login*/mot de passe a été positionné de surcroit afin d'authentifier les accès à la base. Les utilisateurs finaux n'accèdent aux journaux qu'au travers de l'API REST et de l'interface web exposés par STREAM, en fonction de leurs permissions. Enfin, un mécanisme de vérification d'intégrité des évènements permet à un administrateur de constater que le les évènements n'ont pas été altérés en déclenchant une vérification de la signature/chainage des évènements. Ces rapports de vérification sont ensuite stockés, eux-mêmes signés en JWT.

- **FS4.Protection des données**

La TOE protège en confidentialité et en intégrité les données qu'elle stocke en base de données (cf. **FS2.Authentification et contrôle d'accès**). La base de données est installée localement sur la machine où **STREAM** lui-même sera installé, et est donc accessible seulement en local (en écoute sur 127.0.0.1). Le mot de passe permettant de s'authentifier auprès de la base de données est présent dans le fichier de configuration de l'application **STREAM**.

- **FS5.Fonctions cryptographiques et générateurs de nombres aléatoires**

La plupart des fonctions cryptographiques utilisées sont celles du module HSM considéré comme hors TOE. C'est en particulier le cas pour ce qui concerne la génération des clés d'AC et la signature des certificats et CRLs. Le générateur de nombres aléatoires logiciel n'est utilisé pour le stockage des mots de passe et les communications. Il est également utilisé que pour la génération des numéros de série des certificats et des mots de passe utilisés pour les comptes locaux (dans le cadre du fonctionnement normal du produit et de cette TOE, les comptes locaux ne sont utilisés que pendant la phase d'initialisation/cérémonie des clés du produit, en environnement isolé ; seule l'authentification par certificat est ensuite utilisée).

3.5.3. Fonctions désactivées

Les fonctions désactivées sont les fonctions considérées comme étant en dehors du périmètre de l'évaluation (hors-TOE) et non accessibles à un attaquant. Ces fonctions ne seront donc pas considérées lors de l'évaluation, mais leur protection contre une réactivation par un attaquant le sera. Les fonctions désactivées de la TOE sont les suivantes :

- **FD1.Mise à jour**

  La première étape du processus de mise à jour consiste à mettre à niveau le composant **STREAM** lui-même. Par ailleurs, certaines versions de **STREAM** exigent l'exécution de scripts de migration sur la base de données. Le produit est fourni avec un script `streamupgrade` qui gère ce processus de migration.

3.6. MATRICES DE COUVERTURES

3.6.1. Menaces et biens sensibles

La matrice suivante présente la couverture des menaces par rapport aux biens sensibles (les lettres « D », « I », « C » et « A » représentent respectivement les besoins en Disponibilité, Intégrité, Confidentialité et Authenticité).

	Données métier	Données d' authentification	Matériel cryptographique	Configuration	Journaux	Système Hôte
M1.Corruption des données stockées	**ID**	**I**				
M2.Vol des données stockées	**C**	**C**				
M3.Vol des données d'authentification		**C**				
M4.Récupération du matériel cryptographique			**C**			
M5.Modification du matériel cryptographique			**ID**			
M6.Contournement de l'authentification		**C**				
M7.Altération des journaux					**ID**	
M8.Usurpation d'identité		**C**				**I**
M9.Altération de la configuration				**ID**		

Tableau 8 - Couverture des biens sensibles par rapport aux menaces

3.6.2. Menaces et moyens exploités par les agents menaçants

La matrice suivante présente la couverture des moyens exploités par rapport aux menaces retenues.

	Vulnérabilité de la session utilisateur	Vol d'authentifiant	Vulnérabilité réseau	Vulnérabilité du système
M1.Corruption des données stockées				√
M2.Vol des données stockées		√		
M3.Vol des données d'authentification	√	√	√	
M4.Récupération du matériel cryptographique			√	√
M5.Modification du matériel cryptographique				√
M6.Contournement de l'authentification		√		
M7.Altération des journaux				√
M8.Usurpation d'identité	√	√		
M9.Altération de la configuration				√

Tableau 9 - Couverture des moyens exploités par rapport aux menaces

3.6.3. Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par rapport aux fonctions de sécurité. La FS5 Fonctions cryptographiques et générateurs de nombres aléatoires est une fonction transverse et ne couvre pas spécifiquement une menace. Elle n'est donc pas présente dans le tableau ci-après.

	FS1.Communication sécurisées	FS2.Authentification et contrôle d'accès	FS3.Journalisation	FS4.Protection des données
M1.Corruption des données stockées		√		√
M2.Vol des données stockées		√	√	√

M3.Vol des données d'authentification	√	√		
M4.Récupération du matériel cryptographique				√
M5.Modification du matériel cryptographique				√
M6.Contournement de l'authentification	√	√		
M7.Altération des journaux			√	
M8.Usurpation d'identité	√	√		
M9.Altération de la configuration				√

Tableau 10 - Couverture des menaces par rapport aux fonctions de sécurité

Fin du document