Groupe LINAGORA

Cible de sécurité CSPN

LinSecure – Coffre-fort électronique pour le jeu en ligne

Version 1.4 Le 30/10/2010

Identifiant : **Linagora_DOC_LinSecure_Cible-de-securite-CSPN**

Fichier original : **Linagora_DOC_LinSecure_Cible-de-securite-CSPN_1.4.odt**

Groupe LINAGORA
80, rue Roque de Fillol
92800 PUTEAUX
FRANCE

Tél. : +33 (0)1 46 96 63 63
Fax : +33 (0)1 46 96 63 64

http://www.linagora.com/

SIRET : 431 473 669 00056

Diffusion : Publique

Réf. : 7244-01

Historique des modifications

Version	Date	Auteur	Objet de la modification
0.1	26/08/2010	Yann TOURDOT	Création du document – 1re version présentée à Linagora
0.2	03/09/2010	David CARELLA	Relecture, corrections et compléments.
0.3	21/09/2010	Yann TOURDOT	Suppression de l'hypothèse ACCES_PHYSIQUE_RESTREINT.
0.4	12/10/2010	David CARELLA	Mise à jour : schémas d'architecture.
1.0	25/10/2010	Sébastien BAHLOUL	Relecture et adaptations suite au point avec M. Davy.
1.1	26/10/2010	David CARELLA	Relecture. Mise à jour : schémas d'architecture.
1.2	30/10/2010	David CARELLA	Prise en compte des remarques de Yann TOURDOT.
1.3	23/03/2011	David COUTADEUR	Mise à jour des numéros de version des softs utilisés
1.4	14/11/2011	David COUTADEUR	2 précisions ajoutées à la demande de l'ANSSI

Table des matières

1 Identification

1.1 Identification de la cible de sécurité

Ce document décrit la cible de sécurité de LinSecure, une application de coffre-fort électronique pour le jeu en ligne.

Titre de la ST	**LinSecure – Coffre-fort électronique pour le jeu en ligne – Cible de sécurité CSPN**
Version de la ST	1.4
Auteur	OPPIDA (Yann TOURDOT), Groupe LINAGORA
Référence	`Linagora_DOC_LinSecure_Cible-de-securite-CSPN`

Cette cible de sécurité a été élaborée en vue d'une évaluation CSPN.

Le produit évalué permet de tracer les opérations réalisées sur un système et de les conserver de manière sécurisée, c'est-à-dire en garantissant leur confidentialité et leur intégrité.

Ce document décrit le produit évalué, précise les hypothèses sur l'environnement du produit, les menaces qui portent sur le produit et les fonctions de sécurité du produit.

1.2 Identification du produit

Catégorie	Identification
Organisation éditrice	Groupe LINAGORA
Lien vers l'organisation	`www.linagora.com`
Nom commercial du produit	LinSecure
Numéro de la version évaluée	1.0
Catégorie de produit	Stockage sécurisé

1.3 Organisation du document

Le chapitre 1 identifie le produit évalué.

Le chapitre 2 décrit le produit évalué.

Le chapitre 3 décrit l'environnement technique et les hypothèses sur l'environnement.

Le chapitre 4 décrit les biens sensibles à protéger par le produit évalué.

Le chapitre 5 décrit le profil des agents menaçants et les menaces.

Le chapitre 6 décrit les fonctions de sécurité du produit évalué.

2 Argumentaire (description) du produit

2.1 Description générale du produit

Dans le cadre de l'ouverture du marché français des jeux d'argent et de paris en ligne, la loi prévoit que les opérateurs titulaires d'un agrément procèdent à l'archivage en temps réel sur un support matériel situé en France métropolitaine de l'ensemble des transactions de jeux entre le joueur et la plate-forme technique de l'opérateur de jeux.

Ce support est communément nommé « coffre-fort électronique ». LINAGORA propose aux opérateurs de jeux un service de coffre-fort électronique : LinSecure.

C'est ce service qui est la cible de d'évaluation en vue d'une Certification Sécurité de Premier Niveau (CSPN).

2.2 Présentation de l'architecture

L'architecture générale du coffre-fort est organisé autour des différents services suivant :

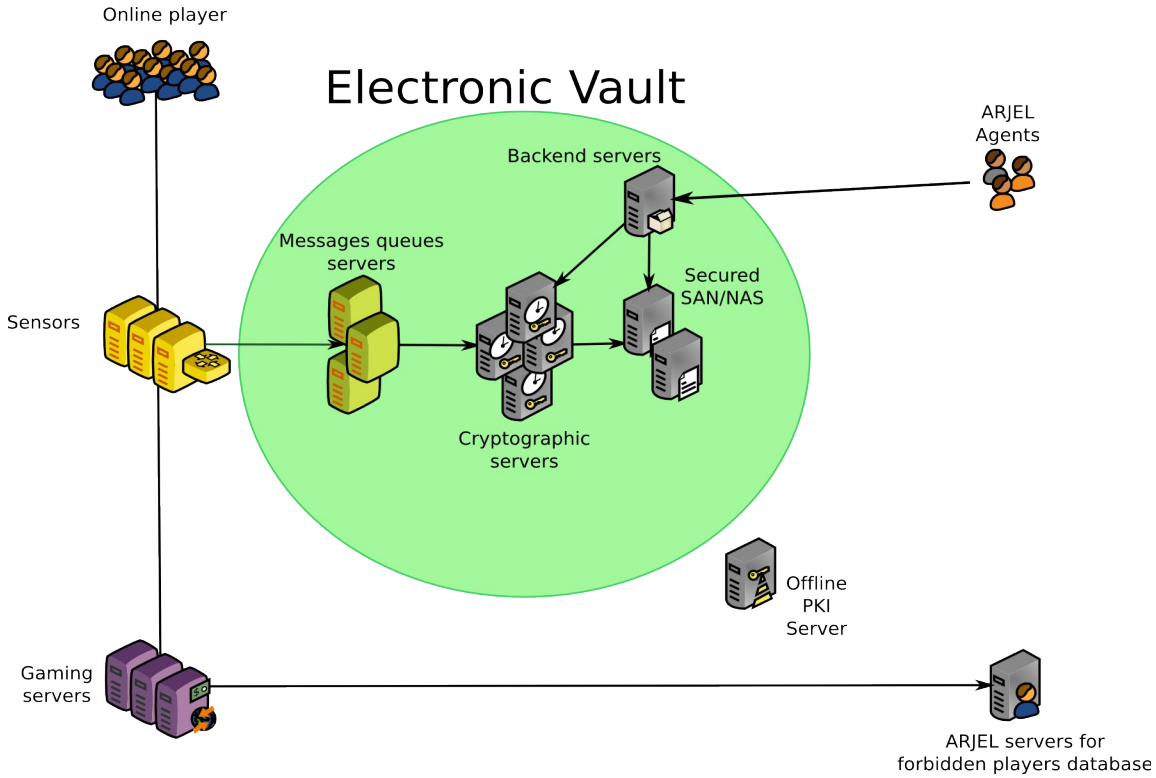


Illustration 2.1: Architecture du coffre-fort LinSecure

L'architecture technique détaillée du coffre-fort est la suivante :

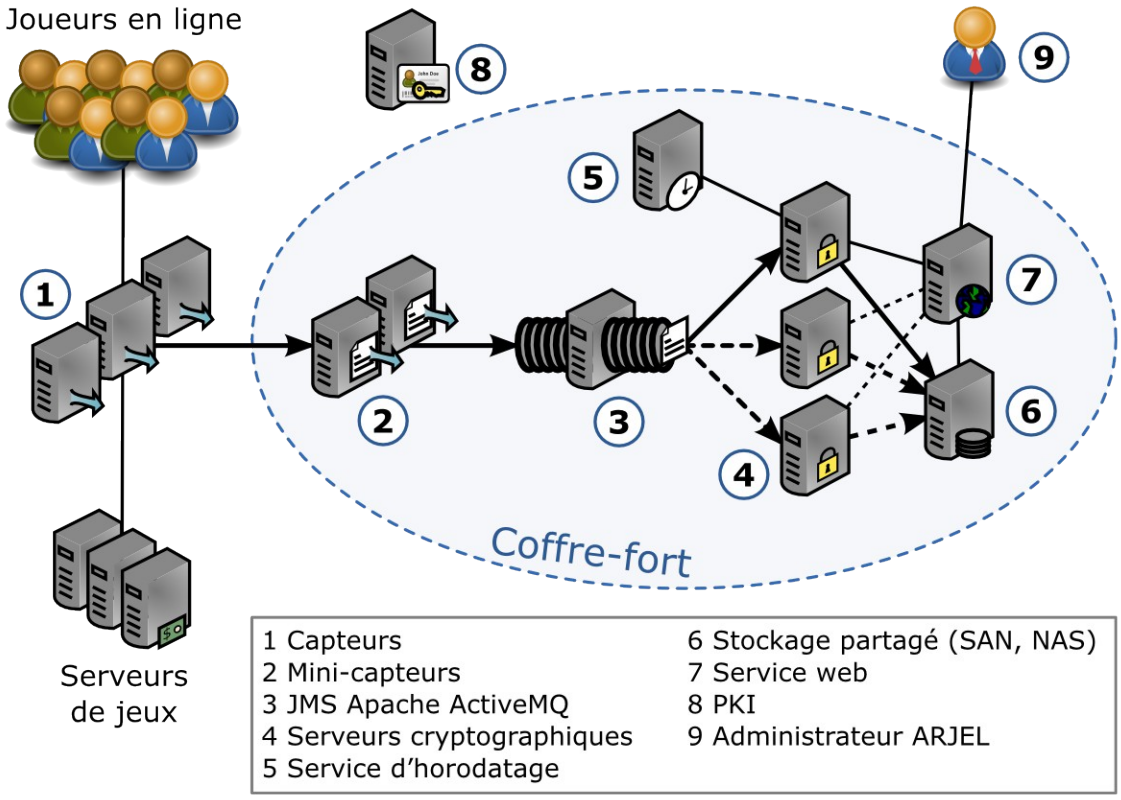


Illustration 2.2 : Détails des composantes

Cette architecture est une vue éclatée des différents services. Suivant les configurations matérielles retenues par l'opérateur, certains services sont susceptibles d'être hébergés sur le même environnement.

2.3 Cinématique d'utilisation du coffre-fort

1. **Actions du capteur :**

a) Lecture de la requête :

Le capteur s'intercale entre le joueur et la plate-forme de jeux afin de récupérer les requêtes envoyées par le joueur vers la plate-forme de jeux. Cette captation s'effectue en tenant compte de la réponse du serveur de jeux de façon à s'assurer de l'accord de l'opérateur sur la consistance des échanges et pour éviter une attaque par injection de données erronées.

b) Création de l'empreinte XML :

En fonction du contexte de jeux, le capteur va extraire les informations utiles de la requête HTTP et créer la trace XML au format demandé par l'ARJEL.

c) Envoi sur le coffre-fort :

La dernière étape consiste à interagir avec le coffre-fort afin d'obtenir la confirmation du dépôt de la trace. Dans le cas positif, la requête de l'utilisateur est libérée par le capteur (hors TOE) ; mais dans le cas négatif, la requête est bloquée par le capteur (hors TOE) afin de ne pas autoriser de transactions sans traces.

2. Actions du coffre-fort

a) Prise en compte des traces :

Le coffre-fort va détecter la présence sur le système de fichier partagé avec les capteurs d'un nouveau fichier représentant un événement de jeu. Il va en vérifier la cohérence (schéma XML) et les déposer dans sa file de traitement. La confirmation de cette première action au niveau du coffre-fort permet au capteur de libérer la requête de l'utilisateur. Cette confirmation est marquée par sa suppression du système de fichiers partagé et la création d'un fichier d'acquittement dans un autre espace uniquement lisible par le capteur. En cas de problème lors de la phase de prise en compte du fichier de trace de l'événement (que ce soit pour une question de format, d'indisponibilité de la file principale ou autre), ce fichier d'acquittement sera suffixé par une extension d'erreur notifiant le capteur de la situation d'échec. Le capteur doit alors bloquer la requête pour indiquer à l'utilisateur le rejet de l'opération.

b) Consommation et sécurisation des événements par les coffres :

Chaque coffre-fort consomme des fichiers de la file : pour chacun il assigne un identifiant unique, signe, chiffre et horodate les données, pour les sauvegarder sur le système de fichiers qui lui est affecté (et dédié).

2.4 Composantes de la solution du coffre-fort

Les composants choisis sont Open Source :

- ActiveMQ pour l'implémentation et la gestion des files de messages JMS ;
- Xerces pour la validation du format de trace ARJEL ;
- JMX pour le statut des coffre-forts ;
- BouncyCastle pour l'horodatage et le calcul d'empreinte SHA-256 ;
- JaxB, javax.security et javax.xml.crypto.dsig pour la signature XAdES-T ;
- Apache XML Security API pour le chiffrement XML ;
- Maven2 pour le packaging ;
- JaxWS Maven Plugin pour la génération des classes « `fr.arjel` » depuis le WSDL ;
- Système d'exploitation allégé et durci Debian stable.

2.5 Portée de la cible de sécurité pour le coffre-fort LinSecure

La cible de sécurité de la CSPN sur le coffre-fort LinSecure comporte :

- les serveurs de files acceptant les messages des capteurs ;
- les serveurs cryptographiques traitant les services de chiffrement, de signature et d'horodatage ;
- les serveurs de récupération des traces (web services) accessibles par l'ARJEL.

Cette cible s'appuie sur un certain nombre de pré-requis :

- un filtrage réseau sur les ports utilisés à l'exception de tout autre ;
- des restrictions sur l'accès physique aux serveurs.

Sont hors du périmètre de la cible :

- les capteurs ;
- l'espace de stockage dédié entre les serveurs de coffre-fort et les serveurs de récupération des traces ;

NOTE_STOCKAGE_1 : l'espace de stockage dépend de l'architecture retenue par l'opérateur. Si un stockage de type SAN ou NAS est choisi, les pré-requis à l'installation de l'architecture sont soit une connexion physique locale à la baie ou aux baies hébergeant l'architecture (que ce soit un commutateur Ethernet, dans le cas d'un NAS, ou un commutateur fibre, dans le cas de l'interconnexion d'un SAN), ou soit que les échanges soient sécurisés par un mécanisme de type VPN avec authentification forte mutuelle de type VPN (avec des caractéristiques cryptographiques répondant aux exigences du RGS), dans le cas d'un stockage résilient entre deux centres d'hébergement.

NOTE_STOCKAGE_2 : la connexion des coffres-forts et des serveurs de récupération des traces aux équipements de stockage est assuré avec une authentification simple ayant pour vocation d'un de permettre la mise en place d'une solution en haute disponibilité sans procédure d'exploitation trop complexe. Compte tenu du fait que les traces sont déjà signées et chiffrées, le risque encouru à ce niveau en l'absence d'utilisation d'une authentification mutuelle forte a été précisé avec notre interlocuteur ARJEL et accepté sur le principe lors des entretiens préalables.

- le service de gestion et de délivrance de certificats (IGC) EJBCA ;
- le service NTP stratum-1 sur lequel l'horloge système du service d'horodatage s'appuie ;
- l'ensemble des dispositifs ayant trait à la sécurité des réseaux (pare-feu, IDS/IPS, …).

2.6 Description des hypothèses sur l'environnement

2.6.1 PERSONNEL_ARJEL_CONFIANCE

Le personnel de l'ARJEL ou le personnel désigné par l'ARJEL est de confiance et non hostile.

2.6.2 FILTRAGE_RESEAU

Des équipements de filtrage (pare-feu) protègent les serveurs du coffre-fort électronique et seuls les flux strictement nécessaires sont autorisés.

2.6.3 SERVEURS_SCELLES

Les serveurs mettant en œuvre le coffre-fort électronique possèdent des scellés qui permettent de détecter toute intrusion physique dans ces derniers (accès physique au disque dur, …).

2.6.4 SOURCE_TEMPS_FIABLE

Le serveur de temps fournit au serveur cryptographique une source de temps fiable.

2.6.5 MISE_A_JOUR_SYSTEME

Le système doit être mis à jour dès qu'une mise à jour a été rendue disponible par Linagora.

2.7 Description des profils

Le coffre-fort électronique LinSecure gère les profils suivants.

2.7.1 Service

Le profil « Service » est attribué aux capteurs et ne permet que de déposer les traces sur le serveur de files.

2.7.2 Opérateur

Le profil « opérateur » est attribué aux opérateurs techniques du coffre-fort. Ce profil permet d'effectuer des opérations d'administration courantes sur les serveurs du coffre-fort telles que changements de paramètres disques, réseaux, configuration des services…

2.7.3 ARJEL

Le profil « ARJEL » est attribué aux personnes de l'ARJEL ou désignées par l'ARJEL, qui peuvent définir des rôles au sein du coffre-fort, leur associer un certificat d'authentification et récupérer les traces stockées dans le coffre-fort électronique.

Tous les profils (frontal, opérateur, ARJEL) accèdent au coffre-fort de manière sécurisée suivant la règle du moindre privilège, c'est-à-dire que seuls les privilèges strictement nécessaires sont attribués. Toutes les communications avec le coffre-fort électronique sont protégées en confidentialité, intégrité et contre le rejeu via un chiffrement AES 256 (sur les protocoles SSH ou HTTPS) et une authentification forte (par certificat X.509v3 ou clé SSH) mutuelle.

2.8 Tableaux des flux inter composants

		Destinataire							
		Capteur	Mini-capteur	Apache ActiveMQ	Serveur cryptographique	Service d'horodatage	Service web	Stockage partagé	ARJEL
Émetteur	Capteur		- SSH-FS						
	Mini-capteur	- SSH-FS	-	TCP:61616 SSL(X509)					
	Apache ActiveMQ		TCP:61616 SSL(X509)	- DRBD[1] & HA	TCP:61616 SSL(X509)				
	Serveur cryptographique			TCP:61616 SSL(X509)		- SSL(X509)	JMX SSL(X509)	- SSH-FS	
	Service d'horodatage				- SSL(X509)				
	Service web				JMX SSL(X509)			- SSH-FS	- SSL(X509)
	Stockage partagé				- SSH-FS		- SSH-FS		
	ARJEL						- SSL(X509)		

Dans chaque case on trouve :

- Flux local (si émetteur et destinataire hébergés sur le même serveur)
- Flux distant (si émetteur et destinataire hébergés sur des serveurs différents)

1 Les flux DRBD entre les deux instances ActiveMQ sont sécurisés via AES256, les flux Heartbeat sont sécurisés via SHA-1 (SHA-256 non existant)

3 Description de l'environnement technique de fonctionnement

3.1 Matériel compatible ou dédié

La TOE est évaluée sur un serveur dédié dont la configuration est la suivante :

- CPU : Intel 64 bits bi-processeurs quadri-cœurs ;
- Mémoire : 16 Go ;
- Espace de stockage :
  - Lecteur compact Flash : 16 Go pour la carte Compact Flash,
  - Partitions locales : 50 Go,
- Connexions réseau : 2 Gigabit Ethernet.

3.2 Système d'exploitation compatible

La TOE est évaluée sur un système dont la configuration est la suivante :

- Système d'exploitation :
  - Distribution GNU/Linux Debian Lenny noyau 2.6.26 durcie ;
- Configuration logiciels :
  - Machine virtuelle Java : JRE 6 Update 22 ou ultérieur,
  - ActiveMQ 5.3.1 pour l'implémentation et la gestion des files de messages JMS,
  - Xerces pour la validation du format de trace ARJEL,
  - connecteur JMX pour le statut des coffre-forts,
  - BouncyCastle 1.45 pour l'horodatage et le calcul d'empreinte SHA-256,
  - JaxB 2.2.1, javax.security et javax.xml.crypto.dsig pour la signature XAdES-T,
  - Apache XML Security API pour le chiffrement XML,
  - JaxWS Maven Plugin pour la gestion du WSDL ;
- Dispositifs cryptographiques :
  - HSM cryptographique : Thales nShield Solo 500/4000 F3.

4 Description des biens sensibles à protéger

Les biens sensibles à protéger par le coffre-fort électronique sont :

- les *Traces* déposées par le capteur et stockées dans le coffre-fort. Ce bien doit être protégé en :
  - **Disponibilité :** Tout effacement autorisé ou non autorisé des traces doit être impossible ;
  - **Intégrité :** Toute modification non autorisée des traces doit être impossible ou détectée ;
  - **Confidentialité :** Toute lecture non autorisée des traces doit être impossible ;
- les *Données de configuration* du coffre-fort. Ce bien doit être protégé en :
  - **Disponibilité :** Tout effacement autorisé ou non autorisé des données de configuration doit être impossible ;
  - **Intégrité :** Toute modification non autorisée des données de configuration doit êt impossible ou détectée ;
  - **Confidentialité :** Toute lecture non autorisée des données de configuration doit être impossible.

5 Description des menaces

5.1 Agents menaçants

Les agents menaçants pour le coffre-fort sont :

Les **attaquants externes** : il s'agit de personnes malveillantes ne disposant ni d'information d'authentification au coffre-fort électronique, ni d'accès physique aux serveurs du coffre-fort électronique et qui ne peuvent interagir avec le coffre-fort électronique que via les éléments exposés sur Internet (capteur, code source LinSecure). Les joueurs en ligne sont par exemple des attaquants externes potentiels.

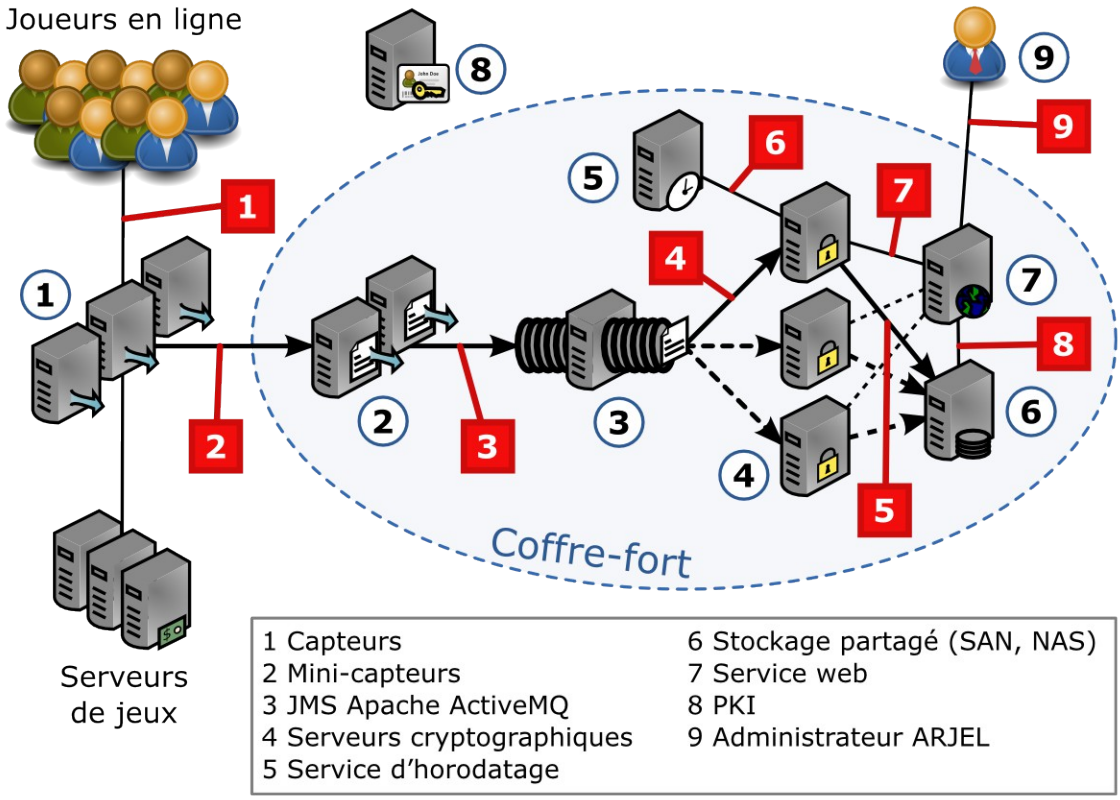
Les **attaquants internes** : il s'agit de personnes malveillantes ne disposant ni d'information d'authentification au coffre-fort électronique, ni d'accès physique aux serveurs du coffre-fort électronique, mais qui, placés sur les réseaux de communication peuvent agir sur les flux échangés entre les serveurs du coffre-fort.

Les **opérateurs malveillants** : il s'agit d'opérateurs malveillants qui disposent d'un accès logique (profil « opérateur ») au coffre-fort électronique et de leurs informations d'authentification. Les opérateurs malveillants peuvent également disposer d'un accès physique aux serveurs du coffre-fort électronique.

Rappel : la considération des opérateurs comme attaquants potentiels fait partie des exigences de l'ARJEL **[ARJEL_DET]** et **[ARJEL_CDC]**.

Les points d'attaque, identifiés dans la figure ci-dessous, sont :

- 1, 2 et 9 pour les attaquants externes ;
- 1 à 9 pour les attaquants internes ;
- 1 à 9 pour les opérateurs malveillants.



5.2 Les menaces

Les menaces auxquelles le coffre-fort doit résister sont issues du document [ARJEL_DET]. Dans les scénarios de menaces ci-dessous, lorsque le terme « attaquant » est employé sans préciser s'il s'agit d'un attaquant interne, d'un attaquant externe ou d'un opérateur malveillant, cela signifie qu'il peut s'agir indifféremment de l'un de ces trois profils d'attaquants.

5.2.1 Déni de service

Un attaquant externe ou interne rend indisponible les services du coffre-fort électronique (en envoyant des messages mal-formés par exemple).

Le déni de service par les opérateurs qui dispose d'un accès logique (profil « opérateur ») et physique aux serveurs du coffre-fort électronique ne rentre pas dans le périmètre de cette cible de sécurité.

5.2.2 Saturation de l'espace de stockage des traces

Un attaquant sature l'espace de stockage des traces (en générant légitimement des traces par exemple). Une fois l'espace de stockage saturé l'attaquant tente de réaliser des transactions qui ne seront pas tracées.

Dans le cas d'une saturation, l'espace de stockage a le comportement en cascade suivant :

- lorsque l'espace dédié aux traces sécurisées (signées, horodatées, chiffrées) est rempli, la file de messages augmente ;
- lorsque la file de messages est remplie, la file des traces en clair provenant du capteur (hors périmètre) augmente ;

– par conséquence, le nombre de traces en clair non traitées – et donc non acquittées auprès du capteur – augmente de la même façon.

5.2.3 Altération des traces durant leur transmission

Un attaquant altère les traces (ajout de trace(s) / suppression de trace(s) / modification de trace(s)) ou en prend connaissance lorsque que ces dernières transitent via les réseaux entre les différents serveurs du coffre-fort électronique.

5.2.4 Altération des traces sur le support de stockage

Un attaquant accède à distance aux preuves lorsque ces dernières sont stockées sur les serveurs du coffre-fort électronique et les altère (ajout de trace(s) / suppression de trace(s) / modification de trace(s)) ou en prend connaissance.

5.2.5 Accès aux fonctions d'administration réservées aux opérateurs

Un attaquant (autre qu'un opérateur) accède aux fonctions d'administration du coffre-fort électronique réservées aux opérateurs.

5.2.6 Accès aux fonctions d'administration réservées à l'ARJEL

Un attaquant accède aux fonctions d'administration du coffre-fort électronique et de gestion des traces réservées aux administrateurs de l'ARJEL.

5.2.7 Altération des données de configuration

Un attaquant (autre qu'un opérateur ou un administrateur de l'ARJEL) altère les données de configuration du coffre-fort électronique en accédant de manière logique aux serveurs du coffre-fort électronique ou lorsque les données de configuration transitent via les réseaux de communication.

6 Description des fonctions de sécurité du produit

6.1 Authentification forte et mutuelle

Entre le capteur et le serveur de files :

- Authentification forte (par clé SSH) entre le capteur (profil « Service ») et le serveur de files et établissement d'un tunnel SSH entre les deux équipements garantissant ainsi la confidentialité, l'intégrité et le non rejeu des données transmises entre le capteur et le serveur de files.

Entre les opérateurs et les serveurs du coffre-fort électronique :

- Authentification forte (par clé SSH) entre les opérateurs (profil « Opérateur ») et tous les serveurs du coffre-fort électronique via un tunnel SSH garantissant ainsi la confidentialité, l'intégrité et le non rejeu des données échangées.

Entre l'ARJEL et le serveur back-end :

- Authentification forte (par certificat X.509v3) entre le personnel de l'ARJEL (profil « ARJEL ») et le serveur back-end du coffre-fort électronique via un tunnel SSLv3 (HTTPS) garantissant ainsi la confidentialité, l'intégrité et le non rejeu des données échangées.

Note : les fonctions suivantes sont ordonnées selon leur exécution chronologique, c'est-à-dire qu'une trace en clair est : **signée, horodatée, chaînée puis chiffrée**.

6.2 Scellement des traces

Le serveur cryptographique signe les traces avec la clé privée de signature associée à un certificat de confiance reconnu par l'ARJEL. La clé privée de signature est stockée dans un module cryptographique matériel (HSM), garantissant ainsi sa confidentialité et son intégrité. L'algorithme de signature est RSA (PKCS #1, v1.5) avec SHA-256, et la taille minimale du module de la clé de signature est 2048 bits.

6.3 Horodatage des traces

Le serveur cryptographique horodate les traces. Pour obtenir une source de temps fiable le service d'horodatage s'appuie sur le temps délivré par le système. Afin d'avoir une source de temps fiable, le système fait appel à un serveur de temps (en dehors du périmètre de l'évaluation) du stratum 1 via une connexion sécurisée native au protocole NTP.

6.4 Chaînage des traces

Le serveur cryptographique chaîne les traces en incluant dans la trace « N » deux références vers la trace « N-1 ». La première référence est l'identifiant de la trace « N-1 ». La seconde référence est l'empreinte numérique SHA-256 des données de validation de la trace « N-1 ». Ces données de validation – incluses dans chaque trace – comprennent la signature et le jeton d'horodatage de la trace.

6.5 Chiffrement des traces

Le serveur cryptographique chiffre les traces – plus précisément les données de jeu – avec la clé publique du certificat de chiffrement de confiance reconnu par l'ARJEL. La clé publique est stockée dans un module cryptographique matériel (HSM), garantissant ainsi son intégrité. L'algorithme de chiffrement est RSA (PKCS #1, v1.5) et la taille minimale du module de la clé de chiffrement est 2048 bits. Seule l'ARJEL détient la clé privée de déchiffrement des traces.

6.6 Sécurisation du coffre-fort

Le système d'exploitation hébergeant le coffre-fort est fortement sécurisé afin d'éviter toute opération de manipulation des données. Il est construit sur une version allégée et durcie de l'environnement Debian dans sa version stable à partir des packages minimaux. Les travaux de sécurisation intervient à plusieurs niveaux :

- sécurisation et limitation des privilèges d'exécution : afin de limiter les possibilités d'interaction par les administrateurs de l'opérateur, les accès seront effectués au sein d'une prison (jail Unix) couplée à une élévation de privilèges très délimitée à travers l'utilisation systématique de l'outil sudo aussi bien pour le contrôle que les traces d'accès que les opérations d'administration,
- blocage des systèmes de fichiers en exécution : le système s'exécutera sur une partition en lecture seule et les autres systèmes de fichiers accessibles en écriture seront montés en lecture sans exécution possible (configuration, logs, stockage temporaire des événements en entrée du coffre-fort, stockage des événements chiffrés en sortie des coffre-forts).

Les accès d'administration pour l'opérateur et d'intervention sur site pour les agents de l'ARJEL seront sécurisés via une connexion SSH sécurisée par des clés.

La connexion pour accéder aux partages de fichiers est sécurisée de serveur à serveur via un accès SSH. Pour des raisons de sécurité, cet accès SSH est rendu disponible par un service SSH qui utilise la séparation des privilèges, dans une prison (jail Unix) dédiée. L'accès sera également protégée par l'usage d'une clé SSH.

6.7 Analyse préalable des risques

Le coffre-fort est sécurisé au regard des attaques logicielles classiques qu'elles nécessitent un accès local ou un accès distant, en partant du principe que si l'opérateur intervient sur le système, son empreinte numérique (hash) sera modifiée. Par exemple l'emprisonnement des environnements administrateurs et opérateurs permettent de limiter l'utilisation de technique d'élévation de niveau de privilèges par *buffer overflow* lié à l'utilisation d'un programme local.

Afin de pouvoir être facilement audité tout en offrant une capacité de montée de version, le système est distribué sur :

- une carte Compact Flash hébergeant le système tel que diffusé par LINAGORA ;
- des partitions sur les espaces disques locaux (volumes RAID) pour le stockage de la configuration locale (`/etc`), des logs (`/var`), des espaces de dépôt des traces à protéger et, éventuellement, des espaces de stockage des traces protégées.

Cette protection permet notamment grâce à un système d'empilage des partitions (pour « `/etc` » et « `/var` ») et de Copy On Write (COW) via le système de fichier Linux AUFS afin de

pouvoir aisément identifier le différentiel entre le système d'origine (installé sur Compact Flash) et le système exécuté par l'opérateur.

Afin de pouvoir garantir l'intégrité des fichiers de la carte Compact Flash, LINAGORA maintiendra une base contenant la somme contrôle de tous les fichiers présents. Ainsi, toute manipulation d'un fichier pourra être facilement identifiée car en cas de modification (que ce soit par un attaquant extérieur, par l'opérateur ou l'hébergeur) d'un exécutable, la somme de contrôle ne correspondra alors plus à l'empreinte pris lors de la phase de mise en ligne.

Par contre le coffre-fort n'est pas protégé par rapport à une attaque de type déni de service. Son accès étant restreint, sa sécurisation au regard de ce type d'attaque repose sur la plateforme et les dispositifs de l'opérateur. En cas d'attaque par déni de service du site de jeu en ligne, il pourrait s'avérer que les capteurs soient amenés à soumettre un grand nombre d'événements dépassant la capacité de traitement instantanée des coffre-forts. De façon coordonné avec l'opérateur, le coffre-fort pourra refuser les événements au delà d'un certain volume. Et cela pour éviter qu'en cas de corruption de l'un des capteurs, il devienne possible pour un attaquant de bloquer l'usage du coffre-fort.

Sigles

Sigle	Désignation
ARJEL	Autorité de Régulation des Jeux en Ligne
CSPN	Certification de Sécurité Premier Niveau
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
NTP	Network Time Protocol
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
RSA	Rivest Shamir Adleman
SHA-256	Secure Hash Algorithm 256
SSH	Secure Shell
SSL	Secure Sockets Layer
XML	Extensible Markup Language

Glossaire

Certificat électronique

Un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.

Condensé

Résultat d'une fonction de hachage à sens unique, c'est-à-dire d'une fonction calculant une empreinte d'un message de telle sorte qu'une modification même infime du message entraîne la modification de l'empreinte. En français, on utilise encore les termes « haché » et « condensé ». Le terme anglais équivalent est « *hash value* ».

Cryptographic Service Provider (CSP) [fournisseur de services cryptographiques]

Couche logicielle permettant à une application d'utiliser des services cryptographiques grâce à une interface programmatique (API) bien définie fournie par le système d'exploitation de la machine hôte.

Object Identifier (OID) [identifiant d'objet]

Suite de caractères numériques ou alphanumériques, enregistrés in conformément à la norme ISO/IEC 9834, qui identifient de manière unique un objet ou une classe d'objets dans l'enveloppe d'une signature électronique.

Prestataire de services de certification électronique

Toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique.

Qualification des prestataires de services de certification électronique

L'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité.

Signataire

Toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de signature électronique.

Signature électronique

Donnée sous forme électronique, jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification pour ces données électroniques.

Signature numérique

Résultat de l'opération cryptographique de signature sur des données à signer et utilisant une clé privée de signature.

Système de création de signature

Le système complet qui permet la création d'une signature électronique et qui inclut l'application de création de signature et le dispositif de création de signature.

Références

Références normatives

Référence	Documents
[CSPN]	**Certification de sécurité de premier niveau (CSPN) des technologies de l'information,** version 2.4, phase expérimentale, nº 915/SGDN/DCSSI/SDR/CCN, 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1.4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1.3.
[XAdES]	XML Advanced Electronic Signatures Version 1.3.2 March 2006 Reference : ETSI TS 101 903

Références informatives

Référence	Documents
[CER/P/01]	**Procédure CSPN-CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information** ANSSI (DCSSI), RGS
[CRYPTO]	**Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques** Version 1.11 24 octobre 2008 ANSSI (DCSSI), RGS
[ETSI-TS-101-733]	**Electronic Signature Formats** Version 1.5.1 15 December 2003 Reference : ETSI TS 101 733
[ARJEL_DET]	**Dossier des exigences techniques** Version 1.0 ARJEL
[ARJEL_CDC]	**Cahier des charges** 17 mai 2010 ARJEL
[ST-CSPN]	**LinSecure – Coffre-fort électronique pour le jeu en ligne** Cible de sécurité CSPN Version 1.4 Référence : Linagora_DOC_LinSecure_Cible-de-securite-CSPN