CSPN - Cible de sécurité

Auteur: A. VERBEKE
Version: 2.0
Date du document: 19 septembre 2016

Validité du document

Identification		
Client	**Projet**	**Fournisseur**
	Archivage des transactions de jeux en ligne	Worldline

Validité du document				
Actions	**Date**	**Nom**	**Fonction**	**Visa**
Rédaction initiale	29/04/2010	Cahon	Chef de projet	
Mise à jour	06/09/2010	Delassus	Chef de projet	
Mise à jour	28/09/2010	Delassus	Chef de projet	
Mise à jour	18/10/2010	Delassus	Chef de projet	
Mise à jour	24/12/2014	Koenig	Chef de projet	
Mise à jour	25/03/2015	Gourlay	Chef de projet	
Mise à jour	18/01/2016	A. Verbèke	Responsable d'équipe	
Mise à jour	15/07/2016	L. Vaugein	Chef de projet	
Mise à jour	19/09/2016	A. Verbèke	Responsable d'équipe	
Validation	20/09/2016	T. Belot	RSSI	
Validation	20/09/2016	D.Ramblewski	Directeur Projet	

Historique des modifications			
Date création	**Date application**	**V.R.**	**Evolution**
06/09/2010	10/09/2010	1.1	Ajout
28/09/2010	28/09/2010	1.2	Modification
18/10/2010	25/10/2010	1.3	Modification
24/12/2014		1.4	Modification
25/03/2015		1.4.1	Modification
18/01/2016	08/02/2016	1.5	Modifications : - N° de version évaluée - Taille max d'une trace - Protection des données de configuration - Précautions d'utilisation du client de consultation
15/09/2016	10/10/2016	2.0	Modifications liées à la version 2.0 du produit

Table des matières

Glossaire

Acronyme	Signification
SB	Safe Box
GSB	Gambling Safe Box
HSM	Hardware Security Module
CCEAL	Common Criteria Evaluation Assurance Level
CSPN	Certification de Sécurité de Premier Niveau
RSA	Type de chiffrement
TLS	Transport Layer Security
ARJEL	Autorité de Régulation des Jeux En Ligne
HTTPS	Hyper Text Transfer Protocol Secure
PKI	Public Key Infrastructure
FIPS	Federal Information Processing Standard
SHA	Secure Hash Algorithm
XADES-T	XML Advanced Electronic Signatures - Timestamp
RFC	Requests For Comments
SSH	Secure SHell

1 Identification de la cible d'évaluation

Catégorie	Identification
Organisation éditrice	Worldline
Lien vers l'organisation	http://worldline.com/fr/accueil.html
Nom commercial du service	Worldline eGambling SB
Numéro de version évaluée	2.0
Catégorie de produit	Stockage sécurisé

2 Argumentaire

2.1 Description générale du service

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*. Worldline propose aux opérateurs de jeux un service de coffre-fort électronique : Worldline eGambling SB.
C'est ce service qui est la cible d'évaluation en vue d'une CSPN.

2.2 Description de l'environnement prévu d'utilisation du service

Le service de coffre-fort électronique est utilisé au sein d'un frontal dont l'objectif est de recueillir et d'archiver les données échangées entre les joueurs et la plateforme de l'opérateur de jeux à l'occasion des opérations de jeux.
Le frontal est constitué également d'un *Capteur* dont la fonction est la création de traces. La fonction de création de traces correspond au formatage des données circulant entre le joueur et la plateforme de jeu puis au transfert de ces données vers le module coffre-fort du frontal.
La *plateforme de jeu* est le système d'information principal de l'opérateur dédié à une activité de jeu en ligne ou de pari en ligne, il s'agit des moyens matériels et logiciels qui assurent plus particulièrement la gestion complète des opérations de jeux ou de paris en ligne.

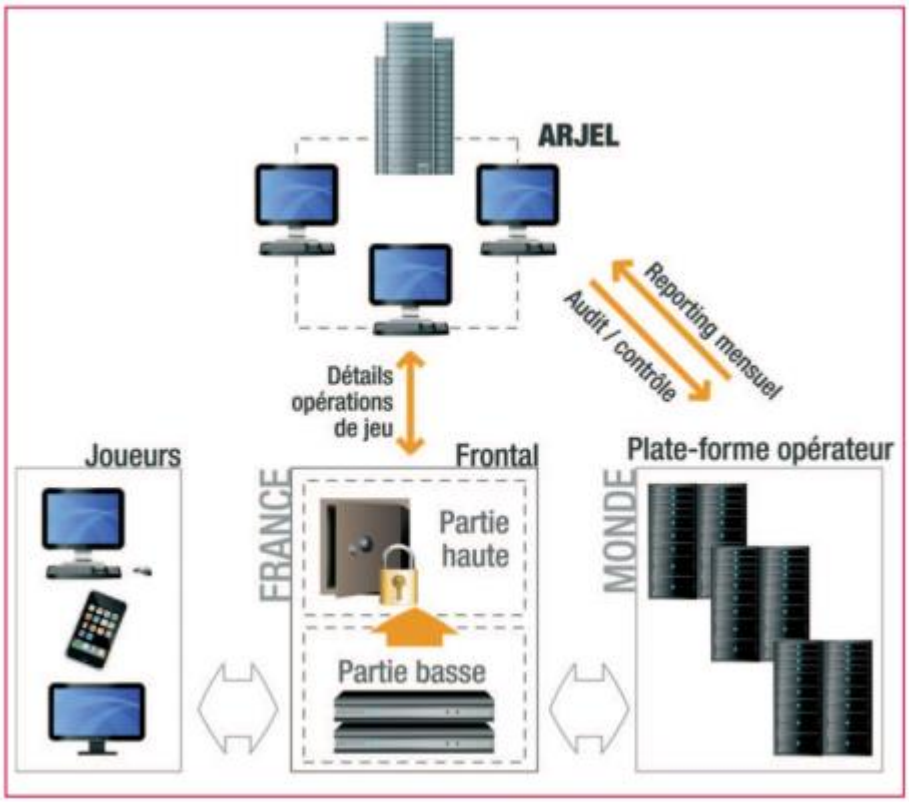

Figure 1 : Contexte d'utilisation du coffre-fort ("partie haute" du frontal)

2.3 Description des utilisateurs concernés et de leur rôle dans l'utilisation du service.

Les utilisateurs du service peuvent être distingués en cinq profils différents :

- Les **déposants** : profil attribué au module Capteur du frontal de l'opérateur. Il permet uniquement de déposer des traces dans le coffre-fort. Le Capteur s'authentifie à l'aide d'un certificat X.509v3 auprès du coffre-fort avec une identité associée à ce profil ;

- Les **lecteurs** : profil attribué aux agents de l'ARJEL dotés des pouvoirs de contrôle et d'audit, qui permet l'extraction des données enregistrées, soit sur support amovible, soit via un dépôt de fichiers accessible à travers un service Web. Les certificats associés à ce profil sont utilisés :

  - soit par des personnes physiques, pour les contrôles réalisés sur site, avec des biclés RSA et un certificat X.509v3 d'authentification conservés sur un support matériel (ex: carte à puce) fourni par l'opérateur,
  - soit par des agents de collecte, pour les consultations réalisées à distance, avec une authentification fondée sur un certificat X.509v3 client TLS, dans le cadre de la négociation d'un canal TLS mutuellement authentifié ;

- Les **administrateurs techniques** *:* profil attribué au personnel technique de l'exploitant du service (ici Worldline), responsable de l'administration et de la supervision technique du coffre-fort, par exemple :
  - arrêt/démarrage des serveurs support du coffre,
  - administration et configuration des serveurs,
  - configuration du médium de stockage,
  - consultation des journaux techniques, notamment en termes de traçabilité des accès locaux et distants, de gestion des erreurs, etc. ;

- Les **administrateurs opérationnels** *:* profil attribué au personnel applicatif de l'exploitant du service (ici Worldline), responsable de l'administration et de la supervision applicative du coffre-fort, par exemple :
  - arrêt/démarrage du coffre,
  - consultation des journaux applicatifs ;

- Les **administrateurs fonctionnels** : profil attribué aux personnes physiques de l'ARJEL ou désignées par l'ARJEL, qui assurent la gestion des utilisateurs du coffre-fort (création des utilisateurs, attribution des rôles, définition/mise à jour des mots de passe, association des certificats d'authentification, etc.).

2.4 Description de la manière d'utiliser le service

Le service Worldline eGambling SB propose des interfaces permettant :

- aux déposants de déposer des traces dans le coffre-fort via le protocole ActiveMQ sur une connexion TLS ou via une connexion HTTPS ;
- aux lecteurs de collecter les traces via une application de collecte également fournie par Worldline ;
- aux administrateurs fonctionnels de configurer les droits et certificats via une interface TLS.

2.5 Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le service

Pour fonctionner, le service a besoin des éléments suivants :

- un ou des capteurs qui créent les traces (c'est-à-dire qui formatent les données circulant entre le joueur et la plateforme de jeu) puis qui les transfèrent vers le service de coffre-fort électronique ;
- d'une PKI permettant de générer et de gérer le cycle de vie des certificats électroniques utilisés par le service ;
- d'une source de temps fiable.

2.6 Description des hypothèses sur l'environnement

2.6.1 ARJEL_CONFIANCE

Il est considéré pour l'évaluation que les lecteurs et les administrateurs fonctionnels (personnels de l'ARJEL ou désignés par l'ARJEL) sont de confiance.

2.6.2 PKI_FIABLE

Il est considéré pour l'évaluation que les PKI utilisées pour générer et gérer le cycle de vie des certificats utilisés par le service sont fiables. C'est-à-dire qu'elles ne permettent pas de divulguer ou de rendre possible la divulgation des clés privées qu'elles gèrent.

2.6.3 TEMPS_FIABLE

Il est considéré pour l'évaluation que la source de temps collectée par le service, au travers du serveur d'horodatage, est fiable.

2.6.4 CLE_CHIFFREMENT

Il est considéré pour l'évaluation que les secrets propriétés de l'ARJEL sont opérés dans des conditions de confidentialité adaptées (ex : clé privée stockée sur carte à puce).

2.6.5 SOCLE_TECHNIQUE

Il est considéré pour l'évaluation que le service est installé sur un système sain, correctement et régulièrement mis à jour, notamment par des correctifs liés à la sécurité. La configuration du système hôte est durcie selon les bonnes pratiques de sécurité.

2.6.6 PROTECTION_PHYSIQUE

Il est considéré pour l'évaluation que l'accès physique aux équipements techniques composant la plateforme cible est conçu de manière à prévenir toute altération par ce biais.

2.6.7 ADMIN_CONFIANCE

Il est considéré pour l'évaluation que les administrateurs techniques et opérationnels en charge du maintien en condition opérationnelle du produit Worldline eGambling SB sont sensibilisés à la SSI, compétents et de confiance.

2.6.8 INTERFACES_EXTERNES

Il est considéré pour l'évaluation qu'une authentification mutuelle est systématiquement requise afin d'accéder aux interfaces externes du service. Seule la présentation d'un certificat client valide permet d'accéder aux fonctionnalités. Toutes les données transitant entre les utilisateurs et le service sont chiffrées.
Les interfaces externes accessibles sont exclusivement :

- Le protocole ActiveMQ sur une connexion TLS ou une connexion HTTPS pour le dépôt de traces.
- Le site web d'administration pour les administrateurs fonctionnels.
- Le Web Service de Consultation, Recherche et Extraction pour les lecteurs.

Un filtrage sur l'adresse IP source est mis en œuvre sur les équipements de sécurité du frontal.

2.6.9 HSM_FIPS

Le HSM est certifié FIPS 140-2.

2.6.10 CONSERVATION_AUTHENTIFICATION

Il est considéré pour l'évaluation que les secrets d'authentification aux fonctionnalités de la cible d'évaluation (certificats clients, couples user/mot de passe) sont opérés dans des conditions de confidentialité adaptées par leurs propriétaires (Worldline, ARJEL, ou opérateur de jeux).

2.6.11 SECURITE_PROFIL_LECTEUR

Il est considéré pour l'évaluation que le poste de travail des utilisateurs de type lecteur du produit respecte les conditions suivantes :

- Les correctifs de sécurité OS et logiciels sont déployés et à jour.
- Le poste est opéré dans des conditions de sécurité physique et logique qui l'immunisent des menaces extérieures et des intervenants illégitimes. (ex : poste isolé d'internet, équipé d'un anti-virus et/ou d'un firewall, gestion des droits des utilisateurs restreints, etc.)

2.7 Définition du périmètre de l'évaluation

La cible d'évaluation est constituée de l'ensemble des éléments techniques (logiciels, matériels et réseaux) qui contribuent à fournir le service de coffre-fort (cf. chapitre suivant pour la description de l'infrastructure supportant le service) ainsi que l'outil mis à disposition des lecteurs pour accéder au service de coffre-fort.

3 Description de l'environnement technique de fonctionnement

La plate-forme est décomposée en 3 couches logiques et dispose de services transverses.

- La couche logique frontale est constituée de serveurs assurant :
  - Les fonctions dépôt et d'acquittement des traces via des queues et des web services. Cette couche garantit un haut niveau de disponibilité par son dimensionnement et ses mécanismes de redondance.
  - Les fonctions de recherche et d'extraction d'archive et d'administration fonctionnelle de la solution.

- La couche intermédiaire est composée :
  - Des serveurs de traitement assurant la constitution des archives à partir des traces déposées par les opérateurs. Cette couche assure en particulier l'agrégation des traces, la compression, le chiffrement, le chainage, le scellement et l'archivage des lots de traces.
  - De boitiers HSM qui stockent la clé privée utilisée pour l'opération de signature RSA, et exécutent cette fonction de signature RSA.

- La couche back office est constituée :
  - Du système de stockage des archives constitué d'un stockage primaire, d'une zone tampon des archives et d'un dispositif de backup. Ainsi, à tout moment, l'archive est présente sur à minima 2 supports (en particulier avant la sauvegarde).
  - Du référentiel de l'archivage permettant la recherche et la restitution des archives.

- Des clients de consultation mis à disposition des lecteurs :
  - Permettant de requêter le référentiel de l'archivage pour obtenir la liste des archives à récupérer,
  - Permettant de télécharger de manière sécurisée les archives, les valider et les décrypter.

- En complément, des services transverses assurent des services spécialisés:
  - Le concentrateur de log assure la collecte de l'ensemble des logs de la plateforme en vue de la constitution des archives de logs.
  - Les outils et services de consultation, purge, indexation, contrôle de fond, et administration des utilisateurs.

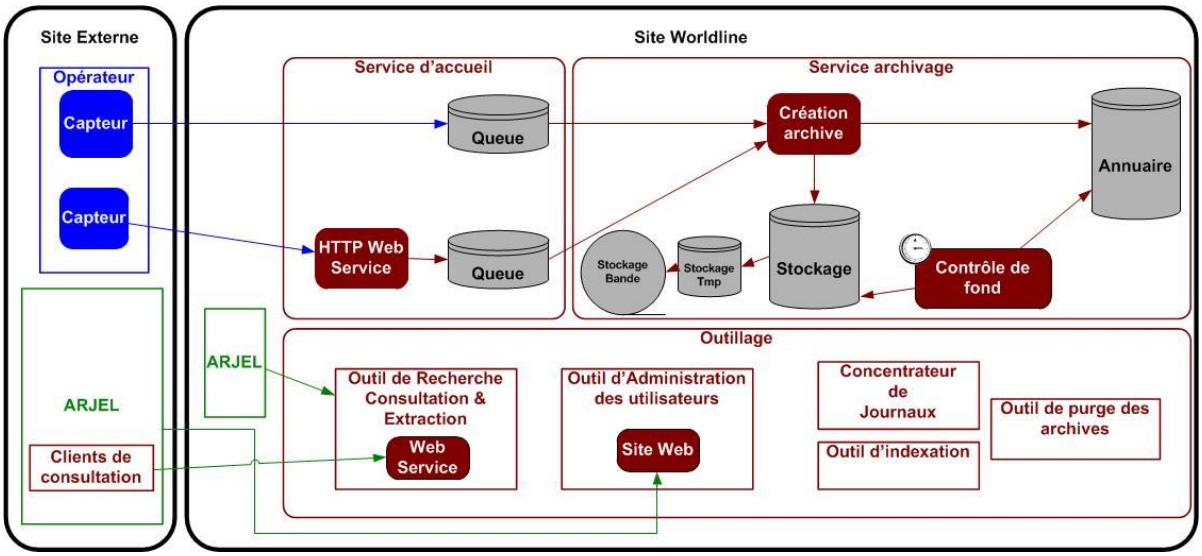

Figure 2 : Architecture de la cible d'évaluation

L'architecture technique est détaillée dans le document GSB005.

La figure ci-dessous présente la méthode de connexion ssh aux serveurs des plateformes Worldline, via des bastions. Dans le cadre de la plateforme « Worldline eGambling SB », les serveurs ne sont accessibles que via des bastions « GSB ».

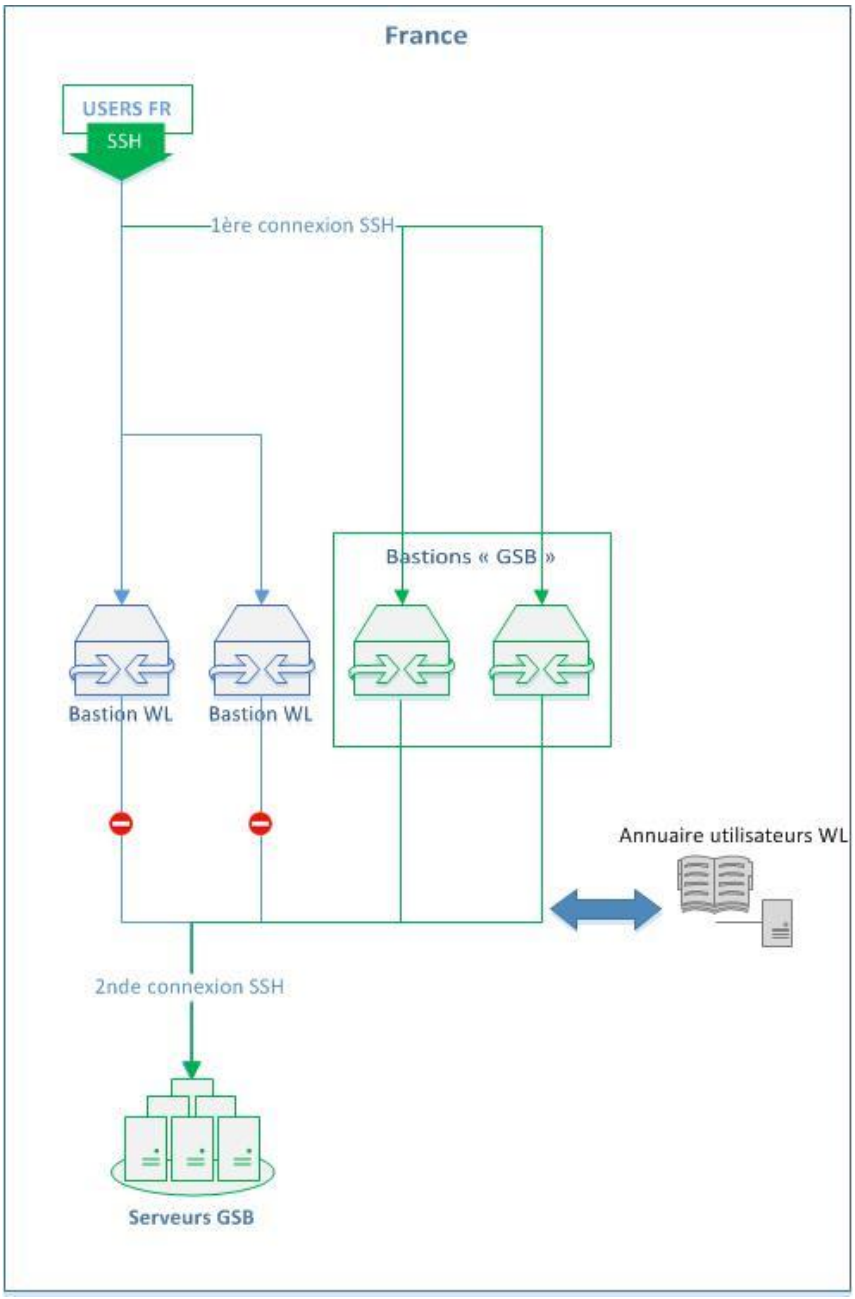

Figure 3 : Architecture des bastions

4 Description des biens sensibles que le produit doit protéger

Les biens sensibles essentiels sont :

- Les Traces déposées par le Capteur et stockées dans le coffre-fort.
  Les traces doivent être protégées en **Disponibilité**, en **Intégrité** (toute modification non autorisée doit être impossible) et en **Confidentialité** (la lecture non autorisée du contenu des traces doit être impossible).

- Les données de configuration de la cible d'évaluation à protéger en **Intégrité, Disponibilité** et en **confidentialité**.

- Les secrets cryptographiques sont protégés en **Intégrité, Disponibilité** et en **Confidentialité** par les HSM.

5 Description des menaces

5.1 Dépôt illicite

Un attaquant réussit à déposer ou injecter de façon illicite des traces dans le coffre-fort.

5.2 Collecte illicite

Un attaquant réussit à collecter de façon illicite les traces envoyées à destination du coffre-fort.

5.3 Consultation illicite

Un attaquant réussit à consulter de façon illicite les traces stockées dans le coffre-fort.

5.4 Altération des traces avant archivage

Les traces déposées dans le coffre-fort sont altérées (ajout, modification, effacement) avant archivage.

5.5 Altération des traces après archivage

Les traces stockées dans le coffre-fort sont altérées (ajout, modification, effacement).

5.6 Déni de services

Un attaquant réussit à rendre indisponibles les services de dépôt des traces, de consultation des traces, et/ou d'administration fonctionnelle.

5.7 Altération de la configuration

Un attaquant réussit à accéder et / ou à altérer la configuration d'un composant du produit de la cible d'évaluation.

5.8 Altération des clients de consultation

Un attaquant réussit à altérer un des clients permettant la consultation des traces. (Par exemple, dans le but de falsifier les traces au moment de leur visualisation).

6 Description des fonctions de sécurité du produit

6.1 Canal TLS entre les acteurs externes et le coffre-fort

Un canal TLS en version 1.2 est établi entre les acteurs suivants et le coffre-fort pour l'utilisation du service :

- Déposants
- Lecteurs
- Administrateurs fonctionnels

L'authentification de ces acteurs sur les services du coffre-fort est assurée par :

- Certificats X509v3 client et serveur
- Filtrage IP
- Nom d'utilisateur et mot de passe associé (uniquement pour les administrateurs fonctionnels)

6.2 Chiffrement des lots de traces

Le chiffrement des lots de traces est réalisé par les algorithmes suivants :

- Chiffrement des données via l'algorithme AES/CBC/PKCS5PADDING avec clé éphémère AES 128 bits;
- Chiffrement de la clé éphémère utilisée pour le cryptage ci-dessus avec la clé publique de l'ARJEL en RSA 2048 via l'algorithme RSA/ECB/OAEPWithSHA-256AndMGF1Padding.

NB : la clé éphémère est créée au début de la procédure d'archivage du lot, et détruite après chiffrement du lot de traces courant.

6.3 Chainage des lots de traces

La fonction de chaînage des lots de traces intègre dans le lot de traces courant l'empreinte générée par la fonction de scellement du lot de traces précédent.
De plus, elle inclut un numéro de série mono-incrémental.

La figure ci-dessous illustre le fonctionnement du chaînage :

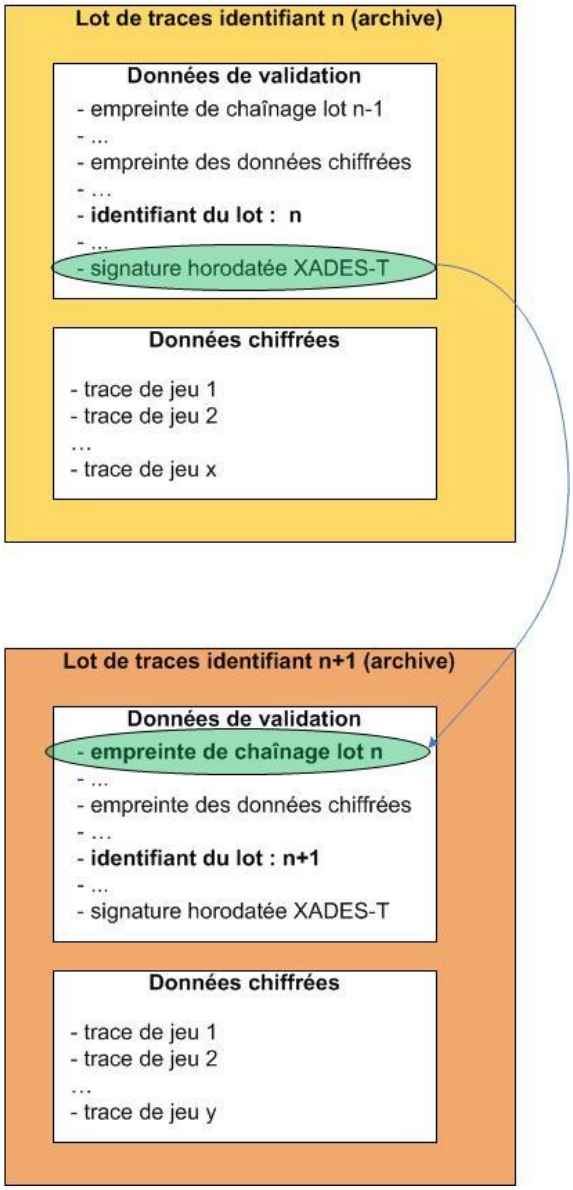

Figure 3 : Chaînage des lots

6.4 Scellement des lots de traces

Le scellement des lots de traces est réalisé par une signature horodatée de l'élément de chaînage et de l'empreinte (SHA-256) des données déposées afin de garantir leur authenticité et de les lier à une heure précise. Pour des raisons de performances, le scellement est réalisé par lots de traces.
La clé de signature RSA-2048bits utilisée est celle présente dans le HSM. La source de temps pour le service est un service de temps ntp (strates 1 et 2, internes à Worldline).
Le format de signature est XADES-T avec un jeton d'horodatage conforme à la RFC 3161.

6.5 Fonctions d'administration et de gestion des utilisateurs

L'accès aux fonctions d'administration et de gestion des utilisateurs du coffre-fort n'est autorisé qu'aux administrateurs fonctionnels.

Cette fonction permet la gestion des mots de passe et des droits des utilisateurs du coffre-fort. Seules les empreintes SHA-256 (+sel) des mots de passe sont stockées.

6.6 Fonctions d'administration technique sécurisées

L'accès aux fonctions d'administration technique n'est autorisé qu'aux administrateurs techniques, nominativement autorisés à accéder aux serveurs.

Les administrateurs techniques accèdent via leur poste de travail à un bastion. Depuis le bastion, l'administrateur se connecte via SSH au serveur souhaité de plateforme.

Les algorithmes de chiffrement utilisés par les administrateurs techniques pour se connecter aux bastions sont les suivants :

- Ciphers aes256-ctr, aes192-ctr, aes128-ctr
- MACs hmac-sha2-512, hmac-sha2-256
- KexAlgorithms diffie-hellman-group-exchange-sha256

6.7 Protection des données de configuration

L'intégrité des données de configuration est contrôlée par l'outil *Samhain*, via l'utilisation d'une fonction de hachage SHA-256.

6.8 Protection anti déni de services

La protection anti déni de services est assurée par des boitiers spécifiques dédiés à cette fonctionnalité, situés en amont du produit Worldline eGambling SB.

L'ensemble des flux réseaux entrants sur le produit sont filtrés par ces boitiers.

De plus, toute trace déposée au coffre-fort électronique d'une taille supérieure à 100ko est rejetée (voir documents contrats d'interface GSB002 et GSB003).

6.9 Protection de l'intégrité des clients de consultation

L'intégrité des clients de consultation des archives doit être contrôlée avant chaque utilisation, conformément aux documents d'utilisation GSB014 et GSB015. L'intégrité est contrôlée via l'utilisation d'une empreinte SHA-256 dont l'originale est imprimée avec la documentation d'utilisation.

7 Couverture des menaces par les fonctions de sécurité du produit

Les tableaux ci-dessous présentent la couverture des menaces identifiées par les fonctions de sécurité du produit.

Menace / Fonctions de sécurité	Canal TLS entre les acteurs et le coffre-fort	Chiffrement des données archivées	Chainage des données archivées	Scellement des données archivées	Fonctions d'administration et de gestion des utilisateurs	Fonctions d'administration technique sécurisées	Protection des données de configuration	Protection anti déni de services	Protection de l'intégrité des clients de consultation
Dépôt illicite	X				X	X	X		
Collecte illicite	X					X			
Consultation illicite	X	X			X	X	X		
Altération des traces avant archivage						X	X		
Altération des traces après archivage			X	X		X			
Déni de services								X	
Altération de la configuration						X	X		
Altération des clients de consultation									X