Offre d’archivage des transactions en ligne
Certification CSPN – Cible sécurité

Date : 2010-09-08
Référence 20100906-CSPN-CibleSécurité-V1.1.doc

VALIDITE DU DOCUMENT

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

Historique des modifications			
Date création	**Date application**	**V.R.**	**Evolution**
06/09/2010	10/09/2010	1.1	Ajout

1 IDENTIFICATION DE LA CIBLE D'EVALUATION

Catégorie	*Identification*
Organisation éditrice	Atos Worldline
Lien vers l'organisation	http://www.atosworldline.fr/Fr/
Nom commercial du service	Worldline eGambling SB
Numéro de version évaluée	1.0
Catégorie de produit	Stockage sécurisé

2 ARGUMENTAIRE

2.1 DESCRIPTION GENERALE 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*. Atos Worldline propose aux opérateurs de jeux un service de coffre-fort électronique : Worldline eGambling SB.

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

2.2 DESCRIPTION DE L'ENVIRONNEMENT PREVU 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.

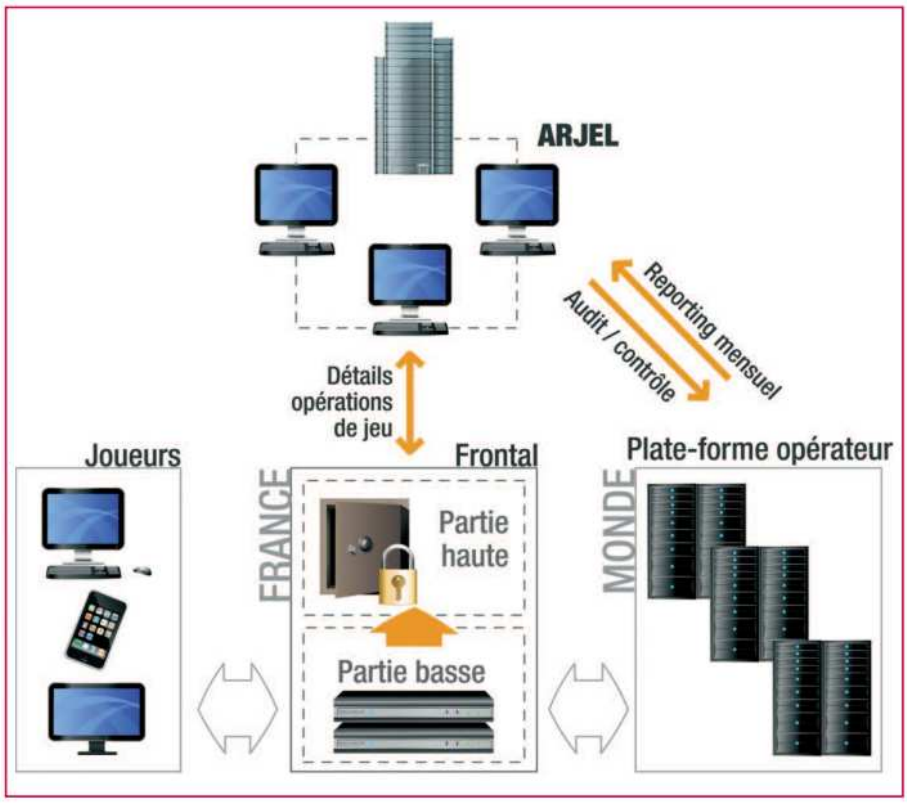

Figure 1 Contexte d'utilisation du coffre-fort ("partie haute" du frontal)

2.3 DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNES ET DE LEUR ROLE DANS L'UTILISATION DU SERVICE

Les utilisateurs du service peuvent être distingués en quatre 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 SSL/TLS, dans le cadre de la négociation d'un tunnel SSL/TLS mutuellement authentifié ;

Les *administrateurs techniques et opérationnels :* profil attribué au personnel technique de l'exploitant du service (ici Atos Worldline), responsable de l'administration et de la supervision technique du coffre-fort, par exemple :

- arrêt/démarrage du coffre,
- 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 fonctionnels* : profil attribué aux personnes physiques de l'ARJEL ou désignées par l'ARJEL, qui peuvent définir des rôles et leur associer un certificat d'authentification. Cette opération est nécessaire à l'initialisation des coffres, puis lors des renouvellements ou des révocations des certificats.

2.4 DESCRIPTION DE LA MANIERE 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 SSL ou via une connexion HTTPS ;
- aux lecteurs de collecter les traces via une application de collecte également fournie par Atos Worldline ;
- aux administrateurs fonctionnels de configurer les droits et certificats via une interface TLS.

2.5 DESCRIPTION DES DEPENDANCES PAR RAPPORT A DES MATERIELS, DES LOGICIELS ET/OU DES MICROPROGRAMMES DU SYSTEME 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 HYPOTHESES 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 la PKI utilisée pour générer et gérer le cycle de vie des certificats utilisés par le service est fiable. C'est-à-dire qu'elle ne permet pas de divulguer ou de rendre possible la divulgation des clés privées qu'elle gère.

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 la clé de déchiffrement des traces déposées par un opérateur est confidentielle. Cette clé est entièrement contrôlée par l'autorité émettrice et est stockée de manière sécurisée. Seuls les agents dotés des pouvoirs de contrôle et d'audit ont la possibilité d'utiliser cette clé.
Le déchiffrement des pièces numériques collectées ne fait pas partie du périmètre d'évaluation.

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 supposé être contrôlé de manière à prévenir toute altération par ce biais.
Les administrateurs systèmes en charge du maintien en condition opérationnelle des serveurs sont sensibilisés à la SSI, compétents et de confiance.

2.6.7 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 SSL ou une connexion HTTPS pour le dépôt de traces.
- Le Web Service 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.

2.6.8 HSM_FIPS

Il est considéré pour l'évaluation que le HSM a fait l'objet d'une certification FIPS 140-2.

2.6.9 CONSERVATION_AUTHENTIFICATION

Il est considéré pour l'évaluation que les certificats clients ainsi que les données d'authentification d'accès aux fonctionnalités de la TOE sont stockés dans un espace sécurisé.

2.7 DEFINITION DU PERIMETRE DE L'EVALUATION

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).

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 via des queues et des web services. Cette couche assure un haut niveau de disponibilité ainsi que l'acquittement de réception des traces 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 le dépôt des archives.

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.

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.
- Le boitier HSM assure les fonctions de chiffrement nécessaires au fonctionnement de la plateforme.

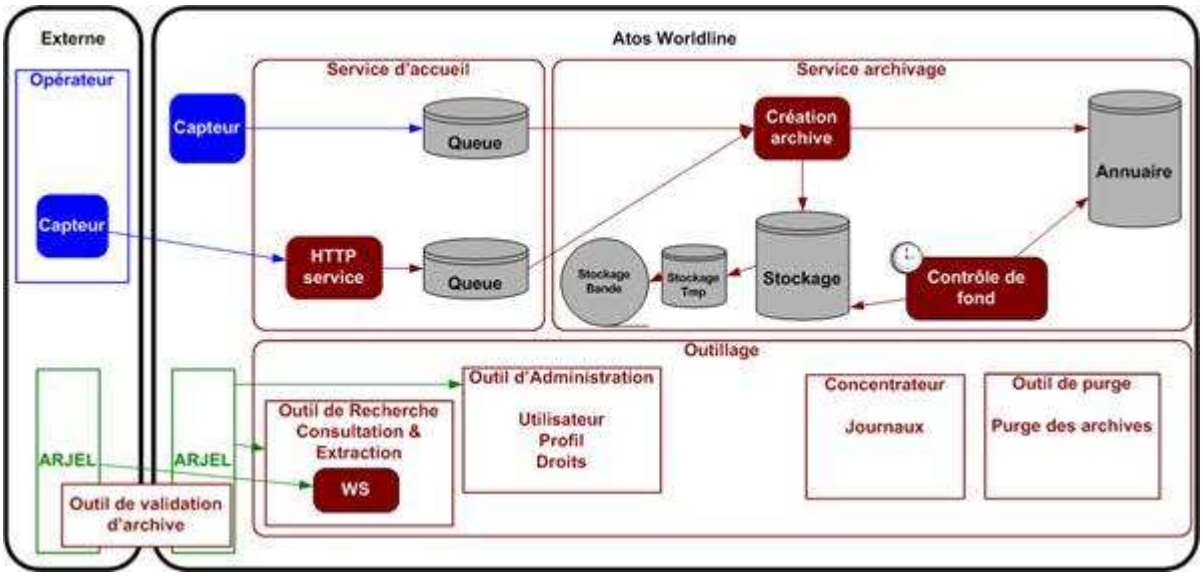

Figure 2 Architecture de la cible d'évaluation

La figure ci-dessous présente l'architecture technique de la plateforme :

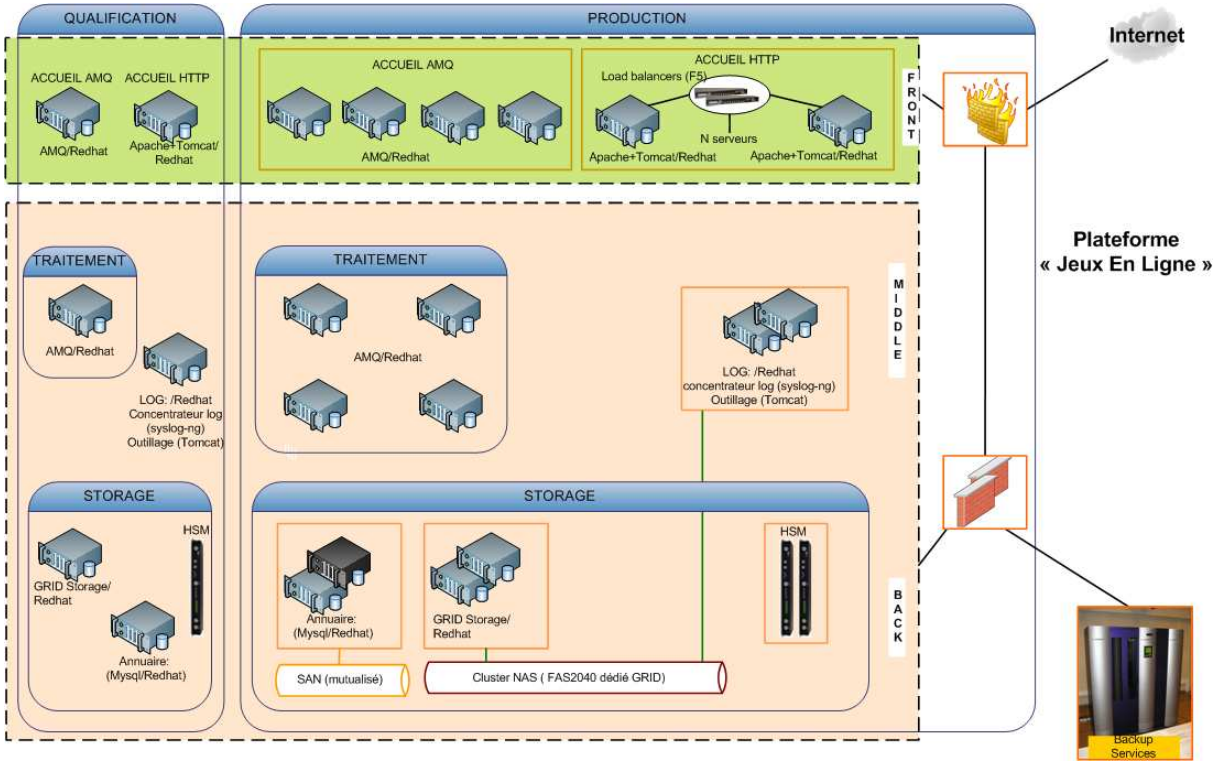

Figure 3 Architecture technique de la plateforme

Cette figure présente deux environnements : QUALIFICATION et PRODUCTION. A noter la présence sur cette figure des firewalls « FRONT » et « MIDDLE ».

D'un point de vue déploiement des services :

Le service d'accueil est déployé sur les serveurs nommés « ACCUEIL AMQ, ACCUEIL HTTP »

Le service d'archivage est déployé sur les serveurs identifiés « TRAITEMENT »

Les services d'outillage sont déployés sur les serveurs identifiés « LOG » (les journaux des différents serveurs de plateforme sont concentrés sur ces serveurs.

4 DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Les biens sensibles essentiels sont :

- Les Traces déposées par le Capteur et stockées dans le coffre-fort.

  Les traces doivent être protégées en **Disponibilité** (tout effacement non autorisé doit être impossible), 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 TOE à protéger en **Intégrité**.
- Les secrets cryptographiques (clés de chiffrement et de signature) sont protégés en **Intégrité** et en **Confidentialité** par le HSM.
- Les données d'authentification aux fonctionnalités, à savoir les certificats et les données de connexion, sont protégées en **Intégrité** et en **Confidentialité** par le système d'exploitation hôte.

5 DESCRIPTION DES MENACES

Les agents menaçants pour le service sont :

- Les utilisateurs illicites du service : il s'agit de personnes ou de machines malveillantes ayant un accès au service mais n'ayant pas l'autorisation d'utiliser les fonctionnalités offertes par le service ;
- Les administrateurs techniques et opérationnels malveillants.

Rappel : les *lecteurs* et les *administrateurs fonctionnels*, personnes physiques de l'ARJEL ou désignées par l'ARJEL, ne sont pas considérés comme des attaquants potentiels, par hypothèse.

5.1 DEPOT ILLICITE

Une personne ou une machine malveillante réussit à déposer de façon illicite des traces dans le coffre-fort.

5.2 COLLECTE ILLICITE

Une personne ou une machine malveillante réussit à collecter de façon illicite les traces déposées dans le coffre-fort.

5.3 ALTERATION DES TRACES

Un administrateur technique ou opérationnel réussit à altérer (ajout, modification, effacement) les traces déposées dans le coffre-fort.

5.4 DENI DE SERVICE

Une personne ou une machine malveillante réussit à rendre indisponibles les services de dépôt et/ou de collecte des traces.

5.5 ALTERATION DE LA CONFIGURATION

Une personne ou une machine malveillante réussit à accéder et / ou à altérer la configuration de la TOE en vue de diminuer son niveau de sécurité.

6 DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

6.1 AUTHENTIFICATION MUTUELLE ENTRE LE DEPOSANT ET LE COFFRE-FORT

En mode dépôt par ActiveMQ comme en mode dépôt par HTTPS, l'authentification est assurée d'une part par un nom d'utilisateur et le mot de passe associé et d'autre part par certificats X509v3. Les certificats seront enregistrés par le capteur de l'opérateur et par le coffre-fort et assurerons une authentification mutuelle. En complément les adresses IP des capteurs seront préalablement connues du système.

6.2 CHIFFREMENT DES DONNEES ARCHIVEES

Les données archivées sont chiffrées au moyen de la clé publique de l'ARJEL pour en assurer la confidentialité. Seule l'ARJEL, détentrice de la clef privée associée à la clef publique, pourra les déchiffrer.

Le chiffrement est réalisé par les algorithmes suivants :

- Chiffrement des données en AES-128 ;
- Chiffrement de la clé AES-128 avec la clé publique de l'ARJEL en RSA 2048

6.3 CHAINAGE DES DONNEES ARCHIVEES

Le chaînage des données archivées est réalisé en liant un lot de données déposées à une empreinte de la signature du lot de données précédent (signature générée par la fonction de scellement des dépôts) et en incluant l'identifiant d'évènement unique à l'opérateur. L'empreinte est calculée à l'aide d'une fonction de hachage SHA-256. Elle n'est pas calculée au moment de l'ajout, mais est conservée en mémoire depuis l'opération précédente.

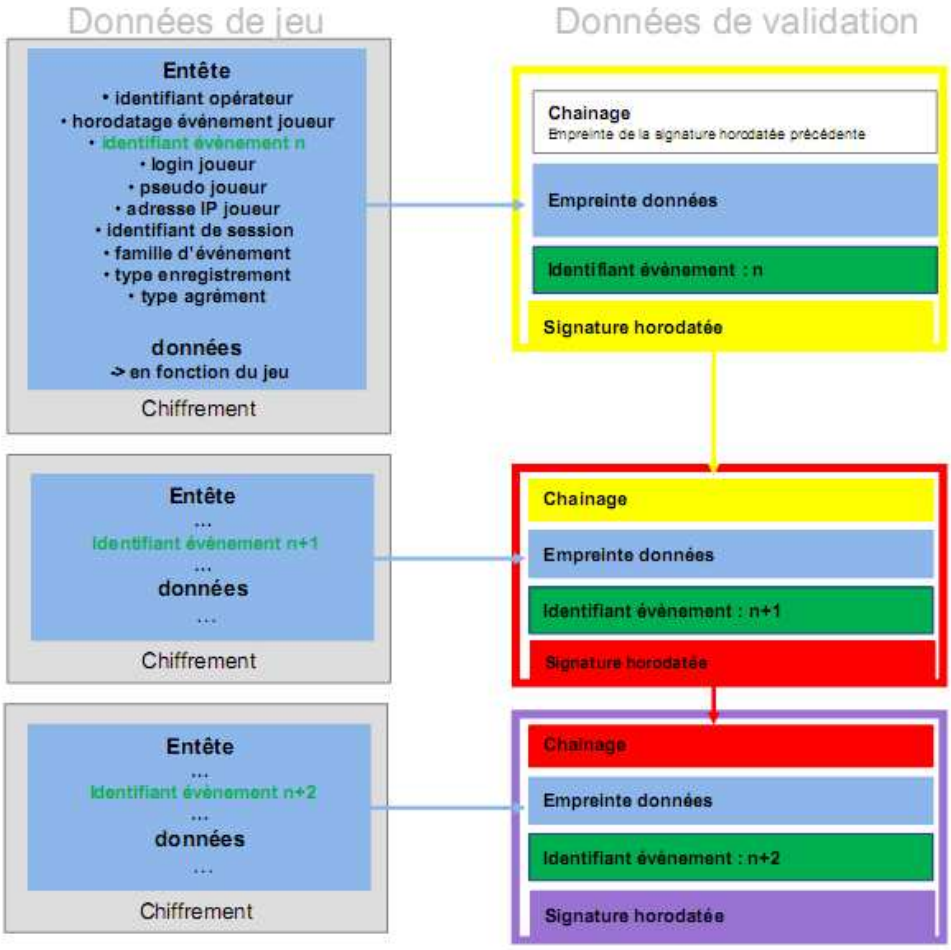

Figure 4 Chainage des dépôts

6.4 SCELLEMENT DES DONNEES ARCHIVEES

Le scellement des données 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 interne à Atos qui est lui-même synchronisé avec une horloge atomique.

Le format de signature est XADES-T avec un jeton d'horodatage conforme à la RFC 3161.

6.5 FONCTIONS D'ACCES AUX DONNEES ARCHIVEES ET D'EXTRACTION

L'accès aux données archivées (chiffrées) n'est autorisé qu'aux *lecteurs* préalablement authentifiés grâce à un certificat x509.

Toutes les opérations d'accès et d'extraction de ces données archivées sont réalisées via un tunnel TLS initialisées depuis des adresses IP préalablement connues de la solution

La vérification du chainage et du scellement des données ainsi que leur déchiffrement peuvent être réalisés par une application fournie par Atos mais hors du périmètre de cette évaluation.

6.6 FONCTIONS D'ADMINISTRATION ET DE GESTION DES UTILISATEURS DU COFFRE-FORT

L'accès aux fonctions d'administration et de gestion des utilisateurs du coffre-fort (gestion des certificats des utilisateurs) n'est autorisé qu'aux *administrateurs fonctionnels* préalablement authentifiés grâce à un certificat x509.

Toutes les opérations d'administration et de gestion des utilisateurs du coffre-fort sont réalisées via un tunnel TLS initialisés depuis des adresses IP préalablement connues de la solution.

6.7 FONCTIONS D'ADMINISTRATION TECHNIQUE

L'accès aux fonctions d'administration technique n'est autorisé qu'aux administrateurs systèmes (en plus des administrateurs système, il y a les administrateurs réseau et les personnes en charge de la supervision des applications). Toutes ces personnes doivent être nominativement autorisées 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.