KEYNECTIS

Cible de sécurité

K·EEP®

Cible de sécurité
V1.7 25 avril 2011 – K.EEP® Server

Protecteur d'identité
Protecteur de liberté
dans un monde connecté

11-13 rue René Jacques - 92131 Issy Les Moulineaux Cedex - France - Tél. : + 33 (0)1 55 64 22 00 - Fax : + 33 (0)1 55 64 22 01 - www.keynectis.com

CIBLE DE SECURITE : K.EEP® SERVER

Version du document :	1.7	**Nombre total de pages :**	36
Statut du document :	☒ Projet	☐ Version finale	
Rédacteur du document :	DS	KEYNECTIS	

Liste de diffusion :	☒ Externe	☒ Interne KEYNECTIS	
	Public		KEYNECTIS

Historique du document :

Date	Version	Rédacteur	Commentaires	Vérifié par
25/04/2011	1.7	JYF	Précision sur type de navigateur au § 3.3.2	
15/04/2011	1.6	EM	Précision sur modèle d'utilisation	
14/04/2011	1.5	EM	Précision sur modèle d'utilisation	JYF
14/04/2011	1.4	EM	Prise en compte commentaires CESTI	JYF
06/10/2010	1.3	EM	Intégration commentaire CESTI	
14/05/2010	1.2	EM	Intégration commentaire	
	1.1	EM	Intégration commentaire	
	1.0	EM	Intégration commentaire	
	0.9	EM	Intégration commentaire	
	0.8	EM	Intégration commentaire	
06/04/2010	0.7	EM	Intégration commentaire	
	0.6	EM	Intégration commentaire	RB
	0.5	LR	Relecture	LR
	0.4	JYF	Relecture	JYF
	0.3	TDV	Relecture	TDV
	0.2	RB	Relecture	RB
29/03/2010	0.1	EM	Création du document	

SOMMAIRE

TABLE DES ILLUSTRATIONS

1 INTRODUCTION

Ce document est réalisé dans le cadre de l'évaluation du produit K.EEP®. Ce document est une cible de sécurité selon le référentiel CSPN pour la TOE (Target Of Evaluation) qui est un logiciel de coffre-fort électronique.

Le but du coffre-fort électronique est de répondre aux besoins de conservation de documents et de preuves électroniques.

Le logiciel K.EEP® de KEYNECTIS permet de protéger des documents électroniques et de les archiver. Il garantit leur confidentialité et le contrôle d'accès à ces documents en consultation. En plus du chiffrement de documents, le coffre fort apporte les mécanismes de sécurité de scellement, d'horodatage et de chaînage permettant de conférer aux documents une valeur probante.

K.EEP® assure les fonctionnalités suivantes :

- Mise au coffre de documents en garantissant leur confidentialité et leur intégrité ;
- Recherche des documents en ligne ;
- Restitution de documents de manière intègre dans le temps ;
- Contrôle d'accès aux documents par le biais d'un coffre virtuel (ou espace de stockage)
- Donne une valeur probante des documents (création d'enveloppes sécurisées, signées et horodatées).

2 IDENTIFICATION DU PRODUIT

Éditeur	KEYNECTIS
Lien vers l'éditeur	http://www.keynectis.com
Nom commercial du produit	K.EEP® v1.2
Numéro de version évaluée	K.EEP® server v 2.9.1
Catégorie de produit	Coffre-fort électronique

3 ARGUMENTAIRE DU PRODUIT

3.1 Description générale du produit

3.1.1 Modèles d'usage de la TOE

La TOE peut-être mise en œuvre selon trois modèles:

- Modèle n°1: la TOE est opérée en mode SaaS (Software as a Service) depuis les installations de KEYNECTIS et avec les personnels de KEYNECTIS. Les Clients des SI déposant des documents et des SI accédant à la TOE afin d'effectuer des recherches et récupérer des documents ne disposent pas de privilèges d'administration technique (administrateur socle technique et détenteur de données d'activation) et applicative du ou des coffres (utilisateur de la TOE autre que Client). Les fonctions d'administration technique et applicative du ou des coffres sont assurées par les personnels de KEYNECTIS.
- Modèle n°2: la TOE est opérée en mode SaaS (Software as a Service) depuis les installations d'un tiers de confiance (similaire à KEYNECTIS) et avec ses propres personnels. Les Clients des SI déposant des documents et des SI accédant à la TOE afin d'effectuer des

recherches et récupérer des documents ne disposent pas de privilèges d'administration technique (administrateur socle technique et détenteur de données d'activation) et applicative (utilisateur de la TOE autre que Client) du ou des coffres. Les fonctions d'administration technique et applicative du ou des coffres sont assurées par les personnels du Tiers de confiance.

- Modèle n°3: la TOE est opérée en mode internalisé depuis les installations d'un hébergeur et avec ses propres personnes. Le Client de la TOE est le propre SI de l'hébergeur pour y déposer ses documents et les SI accédant à la TOE afin d'effectuer des recherches et récupérer des documents. Les fonctions d'administration technique (administrateur root et détenteur de données d'activation) et applicative (utilisateur de la TOE « Client déposant ») sont réalisées par des personnels de l'hébergeur selon une politique de séparation des rôles. En particulier, les fonctions technique de mise en œuvre et de maintien en conditions opérationnelles et de sécurité de la TOE ne sont pas assurées par les personnes qui détiennent les fonctions de mise en œuvre opérationnelle du coffre et inversement.

Dans les 3 modèles ci-dessus, le déploiement, le paramétrage, la mise en route opérationnelle et la formation des utilisateurs sont assurés par KEYNECTIS.

3.1.2 Logiciel K.EEP®

Le produit K.EEP® est une suite logicielle qui gère des coffres forts électroniques qui permettent de stocker des documents de manière sécurisée. Le produit logiciel K.EEP® de KEYNECTIS est une solution de coffre-fort électronique centralisé.

En effet, un coffre associe à chacun des documents stockés une enveloppe de sécurité qui garanti son intégrité (avec la signature électronique), sa confidentialité (avec le chiffrement) et une date et une heure sûres de dépôt (avec l'horodatage). De plus, le coffre lie entre eux (selon le principe de chaînage) l'ensemble des documents déposés dans un coffre par ordre de dépôt afin de détecter toute destruction d'un ou plusieurs documents dans un même coffre. Pour ce faire, le produit logiciel K.EEP® s'appuie sur les services K.Stamp® et Certify.Center®. Ces deux services peuvent être déployés en tant que produits logiciels indépendants.

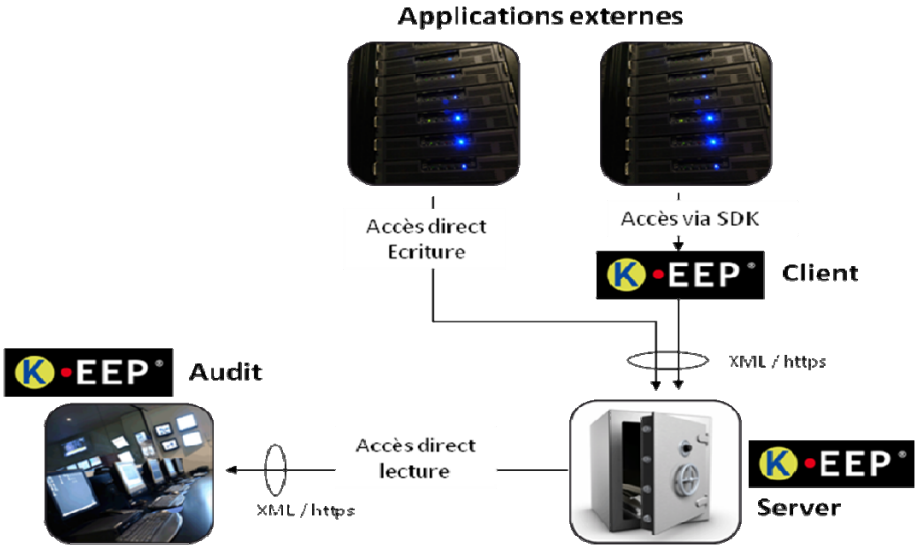

Figure 1 : Architecture K.EEP

La suite logicielle K.EEP® est composée de trois composantes :

- K.EEP® server : c'est le cœur de l'application du coffre fort électronique qui reçoit les documents (transmis par le Client), crée les enveloppes sécurisées associées et stocke les documents avec leurs enveloppes sécurisées. Il permet de gérer des coffres pour chacun des Clients. K.EEP® utilise les logiciels suivants :

    - Certify.Center® : c'est le service qui met en œuvre la signature des documents ;
    - K.Stamp® : c'est le service qui met en œuvre l'horodatage pour délivrer des contremarques de temps ;

- K.EEP® Client : est un ensemble de bibliothèques JAVA facilitant l'intégration avec K.EEP® server. Ce module prend en charge la communication avec un ou plusieurs coffres, les appels protocolaires et la gestion de la répartition de charge vers plusieurs coffres. Par exemple, dans le cadre des jeux en ligne, K.EEP® Client est utilisé par la partie récupération de trace de jeux du frontal de l'Opérateur de Jeux (ci après appelée « sonde ») pour transmettre des traces de jeux (ci après appelé « document ») au coffre K.EEP® server. Le Client n'est pas obligé d'utiliser K.EEP® Client, il peut implémenter un client K.EEP® (dépôt) conformément aux spécifications et aux guides élaborés par KEYNECTIS ;

- K.EEP® Audit : est un outil permettant le téléchargement et la vérification des enveloppes sécurisées et l'extraction des documents contenus dans l'enveloppe. K.EEP® audit est utilisé par l'ARJEL pour les audits sur les traces de jeux stockées dans le coffre (K.EEP® server). Le Client n'est pas obligé d'utiliser K.EEP® Audit, il peut implémenter un client K.EEP® (consultation) conformément aux spécifications et aux guides élaborés par KEYNECTIS.

Le K.EEP® Client et le K.EEP® Audit ne sont pas dans le périmètre de la cible CSPN.

Dans les faits, K.EEP® audit est un sur ensemble de K.EEP® Client. Par conséquent, lorsqu'il n'est pas nécessaire de faire la distinction entre ses 2 composants, alors le terme Client K.EEP® est aussi employé.

Le système de stockage K.EEP® utilise un mécanisme de bases données réparties et de gestion des données sur des systèmes de fichiers disque (Cf. Figure 2 ci-dessous).

Cette gestion répartie de stockage rend K.EEP® simple à administrer et plus performant en écriture et en consultation. Sa capacité d'évolution en termes de volumétrie est quasi illimitée par l'ajout de coffres logiques et de serveurs de stockage physiques associés.

L'ensemble K.EEP® server et serveur de stockage sont hébergés et mis en œuvre dans le même environnement physique et logique d'un hébergeur.

Le ou les Client(s) met(tent) en œuvre le Client K.EEP® en fonction de leur besoin (Client et/ou Audit).

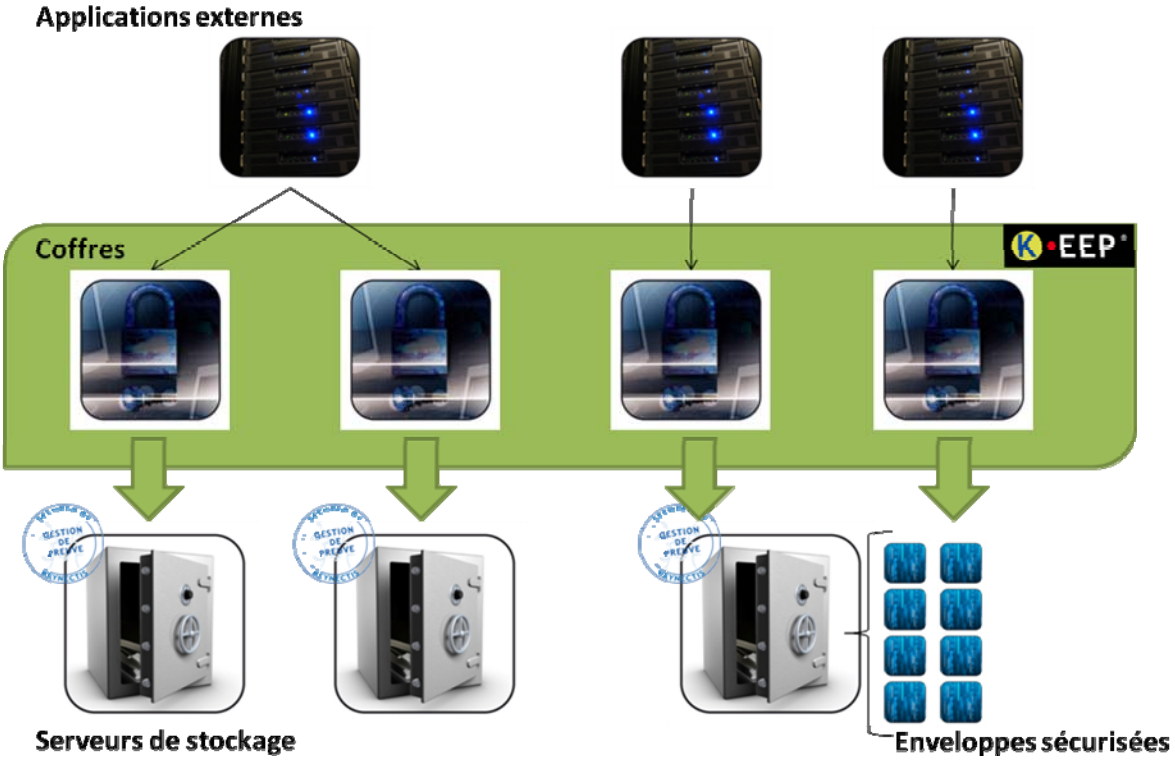

Figure 2 : Architecture générale K.EEP

3.1.3 Définition

3.1.3.1 Coffre

Un coffre est une porte d'accès à des espaces de stockage logique de la plateforme K.EEP® et est garant de la sécurité de document(s) contenu(s) dans des espaces de stockage.
Au sein de cet espace de stockage sont configurés :

- Les habilitations d'accès par les applications externes ;
- La capacité de stockage et la durée de validité du coffre (c'est la durée d'utilisation autorisée pour un Client déposant) ;
- La connexion au serveur de stockage dans lequel seront archivées les enveloppes sécurisées.

Une application externe peut accéder à plusieurs coffres. L'authentification d'une application externe se fait par le moyen d'un certificat client SSL.

3.1.3.2 Client

Un client est une application externe ou une machine qui accède au coffre afin de déposer, consulter et/ou retirer des documents contenus dans les enveloppes sécurisées. La configuration d'un coffre permet d'avoir des Clients avec tout ou partie des habilitations « read », « search » et « write ». Un Client utilise les outils K.EEP® Client et/ou K.EEP® Audit ou le Client implémente un client K.EEP® (dépôt ou consultation) conformément aux spécifications et aux guides élaborés par KEYNECTIS.

3.1.3.3 Serveur de stockage

Un serveur de stockage est un serveur physique sur lequel sont archivées les enveloppes sécurisées. Un coffre est associé à un et un seul serveur de stockage. Un serveur de stockage est constitué d'une base de données et dispose d'une capacité suffisante pour accueillir la volumétrie de documents souhaitée.

3.1.3.4 Document

Un document est un ensemble de données électroniques d'un seul tenant transmis par un Client pour mise au coffre. Par exemple, dans le cadre des jeux en ligne, un document est un ensemble de « traces de jeux en ligne » comme définit par l'ARJEL.

3.1.3.5 Méta information

C'est un complément d'informations qui accompagnent le document et qui sont remplies par le Client (via K.EEP® Client ou équivalent en fonction du choix du Client) et K.EEP ® server. Ces compléments d'informations sont contenus dans l'enveloppe sécurisée signés et horodatés. Les métas informations sont composées de :

- L'empreinte des documents ;
- La référence des documents.
- L'empreinte de chaînage ;

3.1.3.6 Enveloppe sécurisée

L'enveloppe sécurisée est la donnée créée par K.EEP® contenant un ou plusieurs documents transmis par un Client pour les archiver. L'enveloppe est dite sécurisée car les données insérées y sont chiffrées, scellées et horodatées. Les enveloppes sont chaînées entre elles.

Le chiffrement des données se fait à l'attention d'un ou plusieurs certificats X509.
L'enveloppe est scellée par une signature électronique et horodatée.

Une enveloppe sécurisée contient les éléments suivants :

- Document chiffrés ;
- Métas informations ;
- Signature effectuée sur les métas informations ;
- Contremarque de temps pour former une enveloppe XADES-T.

3.2 Description de la manière d'utiliser le produit

3.2.1 Mise au coffre d'un document ou de données électroniques

A la réception d'une demande de dépôt d'un document, K.EEP® réalise une mise au coffre temporaire dans la base de données (serveur de stockage) avant de délivrer un accusé de réception auprès du déposant.

La mise sous enveloppe sécurisée du document et son archivage sont différés. Ce mode est adapté à l'offre « jeux en ligne » (définie par l'ARJEL) afin d'optimiser les performances du coffre qui dans ce

cas de figure est contraint de traiter un très grand nombre de documents (qui sont des traces de jeux, encore appelées évènements). De plus ce mode différé donne la possibilité de regrouper un ensemble de document (évènements) dans une même enveloppe sécurisée afin d'optimiser les traitements informatiques de compression, de chiffrement et de signature électronique.

Le traitement par lot est paramétrable au niveau du coffre selon deux critères :

1. une durée maximale au delà de laquelle une nouvelle enveloppe devra être générée ;
2. un nombre maximal de document.

Si la durée maximale est, par exemple, configurée à 300 secondes, et le nombre maximal de documents à 100, dans ce cas :

- au plus 100 évènements pourront figurer dans une enveloppe ;
- pendant les périodes de faible activité, une enveloppe comportant entre 1 et 100 documents sera générée toutes les 300 secondes.

3.2.1.1 La réception du document

La réception du document consiste en les étapes suivantes :

Etape 1 : Authentification du Client « déposant » autorisé sur le coffre.

L'application cliente dite « déposant » établit un canal sécurisé https via une session TLS mutuellement authentifiée par certificat X.509v3. Le logiciel K.EEP® vérifie l'habilitation du profil à déposer des documents.

Si le déposant ne spécifie pas le coffre dans sa demande, le logiciel K.EEP® sélectionne le premier coffre de la liste des coffres accessibles par le déposant en écriture.
Un coffre est éligible si le déposant dispose de l'habilitation en écriture, si le coffre est dans un état actif, si le coffre est toujours dans sa période d'activité et s'il n'a atteint aucun quota fixé en configuration (nombre de transactions).

Etape 2 : Stockage Temporaire
Le document est enregistré dans la base de données de stockage.

Etape 3 : En cas de succès, un accusé de dépôt est retourné au déposant pour débloquer la poursuite de la transaction.

3.2.1.2 Mise au coffre du document

La mise au coffre de document est déclenchée par le coffre K.EEP® sur l'atteinte d'un nombre maximal d'événements ou une durée maximale qui est un paramètre du coffre (exemple durée maximale égale à 300 secondes, se reporter au § 3.2.1 ci-dessus).
Cette mise au coffre consiste en les étapes suivantes :

Etape 1 : Récupération de l'ensemble des documents (le nombre maximum de document par enveloppe est également un paramètre de du coffre).
K.EEP® récupère les documents en attente d'archivage dans la base de données de stockage.

Etape 2 : Préparation de l'enveloppe
Le logiciel K.EEP® chiffre les données et les ajoute à l'enveloppe.
Le logiciel K.EEP® ajoute à l'enveloppe les méta-informations suivantes :

- Les empreintes des documents ;
- L'empreinte de la signature de l'enveloppe précédente pour chaînage ;
- Les identifiants des documents contenus dans l'enveloppe.

Etape 3 : Scellement de l'enveloppe
K.EEP® signe électroniquement l'enveloppe. Cette signature se fait auprès du service Certify.Center®. Le format de signature est XADES-T avec un jeton d'horodatage RFC 3161.

Etape 4 : Archivage
L'enveloppe sécurisée est enregistrée dans la base de données de stockage.

3.2.2 Recherche d'un document dans un coffre

Cette consultation des coffres consiste en les étapes suivantes :

Etape 1 : Authentification du demandeur
L'application cliente dit « lecteur » établit un canal sécurisé https via une session TLS mutuellement authentifiée par certificat X.509v3. Le logiciel K.EEP® server vérifie l'habilitation du profil à rechercher des documents.

Etape 2 : Recherche selon les critères
Le logiciel construit la liste des documents correspondant aux critères de recherche de l'utilisateur. Cette liste est limitée à 100 références.

Etape 3 : En cas de succès, la liste des documents et les métas-informations associées sont retournées à l'utilisateur.

3.2.3 Téléchargement d'une enveloppe

Le téléchargement d'une enveloppe consiste en les étapes suivantes :

Etape 1 : Authentification du demandeur
L'application cliente dit « lecteur » établit un canal sécurisé https via une session TLS mutuellement authentifiée par certificat X.509v3. Le logiciel K.EEP® server vérifie l'habilitation du profil à télécharger des documents.

Le logiciel K.EEP® server vérifie que le lecteur dispose des habilitations de lecture sur le coffre contenant l'enveloppe demandée.

Etape 2 : Récupération de l'enveloppe dans base de données de stockage du coffre
K.EEP® récupère l'enveloppe depuis la base de données.

Etape 3 : En cas de succès, l'enveloppe sécurisée est retournée au demandeur.

3.3 Description de l'environnement prévu pour l'utilisation du produit

3.3.1 Matériels

Matériel	Description	Version Minimale
Serveur HP	Serveur matériel	ProLiant DL380 G6 ou DL360 G6

Bull	RCM	Version EAL4+
Luna PCI	RCM	Version FIPS 140 – 2 level 2

3.3.2 Logiciels

Les utilisateurs de la TOE qui utilisent les IHM doivent utiliser un navigateur internet de type Internet Explorer ou Firefox.

Le logiciel K.EEP® server est installé sur un socle technique logiciel constitué des éléments du tableau suivant :

Apache (serveur web)	httpd-2.2.3-45.el5
Mod_ssl (serveur web)	mod_ssl-2.2.3-45.el5
OpenSSL (serveur web)	openssl-0.9.8e-12.el5_5.7
Java JDK	Java version « 1.6.0_24 »
Oracle (serveur base de données)	Oracle Database 11g Enterprise Edition Release R2 11.2.0.1.0
Linux RedHat	Red Hat Enterprise Linux Server release 5.6 (Tikanga)
Bouncycastle (serveur cryptographique)	bcmail-jdk16-1.45.jar bcprov-jdk16-1.45.jar bctsp-jdk16-1.45.jar
JBoss	ks-jboss-4.0.3SP1-FCS

3.4 Description des hypothèses sur l'environnement

3.4.1 Hypothèses sur les Utilisateurs de la TOE

3.4.1.1 H_bi-clés_Utilisateur

Les utilisateurs qui sont des personnes physiques ou des machines utilisent les services de la TOE en utilisant chacun une bi-clé et un certificat. Pour les personnes physiques, la bi-clé et le certificat sont sur carte à puce et pour les machines la bi-clé et le certificat sont dans un module cryptographique logiciel ou matériel.

3.4.1.2 H_Protection d'une clé privée associée à un certificat

Les utilisateurs de la TOE (humain et machine) sont responsables de la protection en confidentialité, en intégrité et en disponibilité des clés privées associées aux certificats qu'ils détiennent. Ces certificats sont soit obtenus auprès d'une IGC de confiance externe à la TOE. Les clés privées sont dans tous les cas utilisées par l'acteur pour mettre en œuvre des fonctions de la TOE.

3.4.2 Hypothèses concernant le personnel de l'hébergeur de K.EEP® server et du serveur de stockage

3.4.2.1 H_Porteur de données d'activation

Les données d'activation sont des données secrètes associées à une bi-clé cryptographique et/ou à une ressource cryptographique matérielle qui la contient et permettant de mettre en œuvre sa clé privée associée. Les personnels ayant un rôle « Porteur de données d'activation » sur les RCM hébergeant les clés K.EEP® doivent être de confiance. Ils doivent disposer de la formation et des éléments nécessaires pour assurer correctement leur mission.

3.4.2.2 H_Attribution de rôle (Cf. § 3.7)

Les utilisateurs de l'environnement de la TOE de type Administrateur Socle technique (Cf. § 3.7.2) ne peuvent pas avoir de rôle de type « utilisateur de la TOE » (Cf. § 3.7.1), excepté pour l'Administrateur Root qui peut éventuellement disposer du rôle AuditManagement. Le compte administrateur root et les autres rôles de l'environnement de la TOE ne peuvent pas être détenus par un Administrateur système.

3.4.3 Hypothèses concernant l'environnement IT de l'hébergeur de K.EEP® server et du serveur de stockage

3.4.3.1 H_Machines hôtes

Les machines hôtes hébergeant les composantes de la TOE doivent leur fournir les ressources nécessaires à son fonctionnement.

L'accès aux fonctions d'administration des machines hôtes est restreint aux seuls administrateurs systèmes de celles-ci.

L'installation et la mise à jour de logiciels sur les machines hôtes est sous le contrôle des administrateurs systèmes.

Les machines hôtes doivent journaliser les actions réalisées sur la TOE (en tant que logiciel hébergé par les machines hôtes) et sur les logiciels hôtes de la TOE.

Les machines hôtes doivent être configurées à l'état de l'art des règles de configuration et de protection pour parer les vulnérabilités publiques.

Les machines hôtes utilisées pour la mise en œuvre des modules logiciels de la TOE ne doivent supporter aucun autre logiciel applicatif.

3.4.3.2 H_Réseau de l'hébergeur

Les échanges entre les machines hôtes qui hébergent la TOE avec d'autres machines de l'environnement de la TOE et le Client via un réseau sont contrôlés par des pare-feux contrôlant et limitant les échanges.

3.4.3.3 H_Communication entre la TOE et les serveurs de stockage

L'hébergeur assure et garanti la sécurité des communications entre la TOE et les serveurs de stockage de manière à garantir que seule la TOE peut accéder de manière logique au serveur de stockage.

3.4.3.4 H_Certify.Center® et K.Stamp®

L'hébergeur assure et garanti la sécurité des communications entre K.EEP® (partie coffre) et les serveurs qui hébergent les services Certify.Center® et K.Stamp® de manière à garantir que seule la TOE peut accéder de manière logique à ces services.

3.4.3.5 H_Sauvegarde_Serveur de stockage

Les administrateurs de la TOE doivent disposer de moyens permettant de sauvegarder, de contrôler par rapport à un état de référence, et de restaurer l'ensemble des enveloppes sécurisées contenues dans les serveurs de stockage. Cette sauvegarde se fait à partir des données issues des bases de données des serveurs de stockage.

3.4.3.6 H_Stockage temporaire

Le stockage temporaire effectué par K.EEP® server des documents avant création des enveloppes, nécessite de la part de l'hébergeur de mettre en place des mesures afin de garantir la non-altération des données stockées ainsi de manière temporaire.

3.4.3.7 H_machine hôte K.EEP® server

L'adresse IP du SI Client est connue à l'avance et permet de mettre en place des règles de filtrage réseau, à l'aide de pare-feux, entre le SI Client et la composante K.EEP® server. La communication entre le SI Client et la TOE est réalisée en utilisant le Client K.EEP® ou l'équivalent du K.EEP® Client (en fonction du choix du Client).

3.4.3.8 H_Temps de référence

Les machines hôtes qui supportent la TOE doivent avoir une horloge interne qui est synchronisée avec un temps de référence UTC. Le temps de référence est une approximation locale du temps UTC qui est obtenue à partir d'une ou plusieurs sources de temps dont la précision est connue par rapport à une ou plusieurs sources UTC(k). L'horodatage produit par K.EEP® (K.Stamp®) est réalisé à l'aide d'une source de temps de confiance (par exemple une antenne GPS ou serveur de temps NTP) et dont la communication est protégée par les mesures de sécurités mises en œuvre par l'hébergeur.

3.4.3.9 H_ Service cryptographique_K.EEP® serveur (RCM)

La RCM a pour fonction de générer, protéger, détruire, importer des clés cryptographiques et de permettre leur utilisation de manière sûre à partir des éléments communiqués par la TOE.

Le module cryptographique est également en charge de l'authentification de l'ensemble des rôles de confiance qu'il utilise (porteur de données d'activation) pour la création et la gestion des clés.

On suppose que l'ensemble des composants logiciels et/ou matériels assurant l'interface entre la TOE et le RCM gère (ouvrir/fermer) un canal de communication garantissant l'intégrité et l'exclusivité de la communication. Les modules cryptographiques sont administrés par des postes d'administrations dédiés à ce type d'opération. L'importation et l'exportation des clés cryptographique par la RCM, ne peut pas se faire sur demande des composantes de la TOE. Dans tous les cas, la RCM est conçu de telle manière que :

- L'importation des clés cryptographiques doivent nécessiter au moins un porteur de données d'activation avec son secret pour réaliser l'opération ;
- L'exportation des clés cryptographiques soit interdite.

La RCM doit être une RCM qualifiée au niveau renforcé ou reconnue conforme au standard FIPS 140 – 2 level 2.

3.4.4 Hypothèses concernant le personnel du SI Client

3.4.4.1 H_Administrateur technique

Les personnels ayant un rôle d'administration technique des machines hôtes hébergeant le capteur sont de confiance. Elles doivent disposer de la formation et des éléments nécessaires pour assurer correctement leur mission.

3.4.4.2 H_Attribution de rôle (Cf. § 3.7)

Dans tous les cas, le Client ne peut avoir qu'un seul rôle de type « utilisateur de la TOE » parmi les rôles « Client déposant » et « Client consultation (audit) » (Cf. § 3.7.1).

Si le Client est aussi hébergeur de K.EEP® server et du serveur de stockage (Cf. § 3.1.1 ci-dessus, modèle n°3), alors :

- il ne peut rendre de service de coffre électronique au profit d'un autre Client,
- il ne peut ni détenir le rôle Administrateur Root ni détenir le rôle de porteur de données d'activation
- il n'a que le rôle « Client déposant » et Administrateur système.

Si le Client possède le rôle « Client consultation (audit) » alors il ne peut avoir d'autres rôles sauf les rôles « KeyManagement » et « UserManagement ».

3.4.5 Hypothèses concernant l'environnement SI du Client

3.4.5.1 H_Client

Le Client qui possède un SI connecté à la composante K.EEP® server implémente un client K.EEP® (dépôt et/ou consultation) conformément aux spécifications et aux guides élaborés par KEYNECTIS.

3.4.5.2 H_SI Client

L'environnement du SI Client doit assurer l'identification et l'authentification des utilisateurs qui se connectent, localement ou à distance, au machine du SI Client qui interagissent avec le Client K.EEP®. Le Client protège en intégrité et en confidentialité les clés qui permettent de mettre en œuvre la sécurité demandée par K.EEP® server pour le dépôt et la consultation (audit).

3.4.5.3 H_Capteur

Le capteur récupère les traces de jeux et les transmet au coffre (K.EEP® server) via l'interface protocolaire de K.EEP® server.

Le capteur détecte les interruptions de fonctionnement de K.EEP server, transmises le cas échéant par K.EEP® client ou l'équivalent (en fonction du choix du Client), il les interprète afin d'annuler le jeu concerné.

Le capteur procède à la vérification du respect des schémas XML spécifiés pour les documents transmis à K.EEP® server. K.EEP® server ne fait aucun contrôle.

3.4.5.4 H_Machines hôtes

Les machines hôtes hébergeant les composantes de la TOE doivent leur fournir les ressources nécessaires à son fonctionnement.

L'accès aux fonctions d'administration des machines hôtes est restreint aux seuls administrateurs systèmes de celles-ci.

L'installation et la mise à jour de logiciels sur les machines hôtes est sous le contrôle de l'administrateur systèmes.

Les machines hôtes doivent journaliser les actions réalisées sur la TOE (en tant que logiciel hébergé par les machines hôtes) et sur les logiciels hôtes de la TOE.

Les machines hôtes doivent être configurées à l'état de l'art des règles de configuration et de protection pour parer les vulnérabilités publiques.

Les machines hôtes utilisées pour la mise en œuvre des modules logiciels de la TOE ne doivent supporter aucun autre logiciel applicatif.

3.4.5.5 H_Réseau du Client

Les échanges entre les machines hôtes qui hébergent la TOE avec d'autres machines de l'environnement de la TOE et du Client via un réseau sont contrôlés par des pare feu contrôlant et limitant les échanges.

3.4.6 Hypothèses concernant l'environnement non TI (Client et hébergeur K.EEP® server et serveur de stockage)

3.4.6.1 H_Politique de sécurité

Un ensemble de politiques de sécurité est mis en œuvre pour définir les règles de sécurité dédié à la TOE pour :

- L'organisation générale de l'hébergeur dans laquelle intervient la TOE. Cette organisation concerne notamment les échanges de biens entre la TOE et les Clients ;
- Les rôles de confiance et les opérations à réaliser sur la TOE ;
- Les contraintes temporelles qui sont imposées à la TOE (période de validité d'un certificat, temps de révocation, …) ;
- La sécurité physique et logique du système d'information qui héberge les composants de la TOE.

3.4.6.2 H_Protection physique de la TOE

L'environnement de la TOE doit assurer une protection physique suffisante afin de limiter les risques d'attaque contre l'intégrité de la TOE (matériels et supports de données) par des personnels non habilités à accéder physiquement aux machines qui mettent en œuvre la TOE.

La TOE n'est pas accessible physiquement des utilisateurs de la TOE, en particulier les administrateurs système de K.EEP Server n'ont pas d'accès physique aux machines hôtes hébergeant K.EEP Server, ainsi qu'aux serveurs de stockage et aux RCM de la TOE. Seul le Responsable de sécurité (Cf. § 3.7.2) peut accéder physiquement à la TOE.

3.4.7 Hypothèse sur l'utilisation de la TOE

3.4.7.1 H_Clés de chiffrement des documents contenus dans les enveloppes sécurisées

Une clé de chiffrement de document est dédiée par Client. Pour 2 Clients distincts (au sens entité), il y a nécessairement 2 clés RSA de chiffrement distinctes. Chaque Client est responsable de définir une sauvegarde de sa bi-clé de chiffrement afin de pouvoir déchiffrer les documents pour des raisons de disponibilité. De même, chaque Client est responsable de la protection en confidentialité et en intégrité de sa bi-clé de chiffrement.

3.4.7.2 H_Clés de signature (scellement et horodatage)

Ces clés ne sont jamais sauvegardées. En cas de destruction du RCM ou de la perte de ces clés, il est nécessaire de générer de nouvelles clés. Par contre les certificats correspondant à chacune des clés générées sont sauvegardés à des fins de vérification des enveloppes sécurisées.

3.4.7.3 H_Certificats

Le contenu des certificats des bi-clés sont délivrés par des Autorités de Certification qui répondent aux exigences de KEYNECTIS et des Clients.

3.4.7.4 H_Protection des clés utilisées

La connexion à K.EEP® server nécessite l'emploi d'une bi-clé d'authentification utilisé par le Client pour K.EEP® Client et K.EEP® audit ou l'équivalent (en fonction du choix du Client). Le Client est responsable de la protection en confidentialité et en intégrité de cette bi-clé.

3.4.7.5 H_Bien de l'environnement de la TOE

Les biens utilisés par la TOE et qui sont gérés par l'environnement de la TOE sont donnés dans le tableau ci-dessous.

L'ensemble des clés listées dans le tableau ci-dessous sont obligatoirement distinctes.

Biens	Identifiant du bien	Description
Clé privé RSA de signature des enveloppes sécurisée	BE_1	Clé utilisée pour signer les enveloppes sécurisées. La bi-clé correspondante est dédiée à un coffre. Cet élément est à protéger en confidentialité.
Clé privée de déchiffrement des enveloppes	BE_2	Clé utilisée pour déchiffrer les documents contenus dans l'enveloppe sécurisée. La bi-clé correspondante est dédiée à un coffre. Cet élément est à protéger en confidentialité.
Clé privée de signature de contremarque de temps	BE_3	Clé utilisée pour signer les contremarques de temps des enveloppes sécurisées. La bi-clé correspondante est dédiée au service d'horodatage mais n'est pas nécessairement liée à un coffre ou un client. Cet élément est à protéger en confidentialité.
Clé privée pour l'authentification SSL sur le serveur K.EEP® server d'un utilisateur de la TOE.	BE_4	Clé privée utilisée par un utilisateur de la TOE pour mettre en œuvre des fonctions de K.EEP®. Cet élément est à protéger en confidentialité.
Données d'activation (RCM)	BE_5	Ensemble d'éléments secrets détenus par des porteurs de données d'activation et qui permettent la réalisation d'opérations sous contrôles sur une RCM. Ces éléments sont à protéger en confidentialité.

Accusé de coupure de service	BE_6	Donnée électronique transmise par K.EEP® Client à la sonde pour lui indiquer qu'elle est saturée et ne peut plus rendre son service de cache sécurisé et de transmission vers K.EEP® server.
Certificat d'AC émettrice des certificats des utilisateurs de la TOE	BE_7	Certificat de l'AC qui sert à vérifier les certificats des utilisateurs de la TOE lors des sessions SSL avec K.EEP® server.
Traces d'audit K.EEP® server	BE_8	Journaux contenant des évènements de sécurité stockés par le module base de données du composant K.EEP®.
Configuration K.EEP® server	BE_9	Paramètres permettant la configuration des composants logiciels de K.EEP® server.
Règles d'accès à la TOE	BE_10	Ensemble de règles d'habilitation définit pour autoriser et authentifier les utilisateurs de la TOE en fonction de leur profil. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou vis-à-vis de certain rôle de confiance opéré par l'utilisateur de la TOE.
Certificat d'AC émettrice des certificats SSL de la TOE.	BE_11	Certificat de l'AC qui sert à vérifier les certificats SSL de la TOE lors des sessions SSL avec les utilisateurs de la TOE.

3.4.8 Hypothèse concernant la livraison et l'installation

3.4.8.1 H_Livraison

L'ensemble des fichiers de K.EEP® server est livré avec une fiche de livraison qui contient l'empreinte des fichiers. Cette fiche permet donc de vérifier l'intégrité des fichiers livrés. Cette fiche est communiquée de manière sécurisée à l'hébergeur de K.EEP® serveur.

3.4.8.2 H_Installation

L'installation est effectuée par les équipes techniques de KEYNECTIS. Lors de l'installation, une configuration durcie du système de coffre est effectuée suivant le guide « DS_CSPN_KEEP_MISE_EN_CONFORMITE ».

3.4.8.3 H_Formation

KEYNECTIS dispense la formation nécessaire aux personnels détenant des rôles de confiance sur la TOE et sur son environnement..

3.4.8.4 H_Support et maintenance

KEYNECTIS met en place un support et une maintenance afin d'assurer la continuité de service.

3.5 Description des dépendances

Ce paragraphe décrit ici les dépendances que peut avoir K.EEP® server avec des matériels et/ou des logiciels.

K.EEP® server ne peut s'interfacer, pour les opérations de dépôt et de consultation (retrait et vérification de document et d'enveloppe) qu'avec des applications qui intègrent les outils K.EEP® Client et Audit ou qui mettent en œuvre les spécifications et exigences décrites pour K.EEP® Client et Audit.

Les utilisateurs de la TOE qui utilisent les IHM doivent utiliser au minimum un navigateur internet (IE 7 minimum) avec un système d'exploitation Microsoft Windows XP Professionnel Version 2002 Service Pack 3.

Les serveurs de stockages utilisent nécessairement le logiciel Oracle.

De manière générale, les dépendances sont données par l'architecture matérielle et logicielle décrite dans les chapitres 3.3 et 4.

3.6 Préconisations pour les outils tiers

L'architecture matérielle et logicielle est décrite dans les chapitres 3.3 et 4.

3.7 Description des utilisateurs typiques concernés

3.7.1 Utilisateur de la TOE

Les utilisateurs de la TOE sont :

- Client avec un profil sur un coffre qui possède l'un et/ou l'autre des types de rôles ci-dessous :
    - « Client déposant » : dépose des documents dans un coffre sur lequel il est autorisé et utilise pour ce faire le logiciel K.EEP® Client ou une implémentation de K.EEP® Client qui suit les spécifications de KEYNECTIS ;
    - « Client consultation (audit) » : recherche et/ou retire et vérifie des documents dans un coffre sur lequel il est autorisé et utilise pour ce faire le logiciel K.EEP® Audit ou une implémentation de K.EEP® Audit qui suit les spécifications de KEYNECTIS ;
- Utilisateur avec un rôle ou profil de confiance dans l'application K.EEP® server : l'ensemble des fonctions d'administrations est découpé en cinq catégories correspondant à cinq rôles d'opérateurs différents possibles :
    - « **WorkspaceManagement** », qui a à charge la gestion de la configuration de K.EEP® ;
    - « **DsManagement** », qui aura à charge le paramétrage des espaces Client de K.EEP® ;
    - « **KeyManagement** », qui a à charge la génération des bi-clés utilisées par K.EEP® pour signer (Certify.Center®) et horodater (K.Stamp®) ;
    - « **UserManagement** », qui a à charge la gestion des utilisateurs (Client) de K.EEP® ;
    - « **AuditManagement** », qui a à charge la consultation des évènements d'audit de K.EEP®.

Toutes les composantes logicielles de la TOE utilisent ces rôles. Tous ces rôles utilisent un certificat électronique pour être authentifiés et autorisés sur un coffre et/ou sur l'application K.EEP® server.

3.7.2 Utilisateur de l'environnement de la TOE

Les acteurs de l'environnement de la TOE sont les suivants :

- Hébergeur de K.EEP® server et serveur de stockage : organisme qui déploie la TOE (K.EEP® server) et l'intègre au sein d'un système d'information. Il est responsable de l'utilisation de la TOE et de son utilisation par le système d'information selon les hypothèses et politiques de sécurité organisationnelles données dans la présente cible de sécurité ;

- Hébergeur Client : organisme qui déploie un client K.EEP® (dépôt et/ou consultation), conformément aux spécifications et aux guides élaborés par KEYNECTIS, et l'intègre au sein d'un système d'information. Il est responsable de l'utilisation de la TOE et de son utilisation par le système d'information selon les hypothèses et politiques de sécurité organisationnelles données dans la présente cible de sécurité ;

- Responsable de sécurité : est responsable de l'application de la politique de sécurité physique et fonctionnelle de tout ou partie de la TOE et de son environnement. Par exemple, il gère les contrôles d'accès physiques et peut déléguer le contrôle d'accès logique à la plate-forme de la TOE. Il est aussi responsable de la sécurité de l'application mise en œuvre à l'aide de la TOE. Ce rôle est définit pour l'hébergeur Client et l'hébergeur K.EEP® server et serveur de stockage ;

- Administrateur socle technique : est chargé de la mise en route, de la configuration et de la maintenance technique des machines hôtes des composantes de tout ou partie de la TOE. Il assure l'administration des machines hôtes et du réseau utilisé par les composantes de la TOE. Ce rôle est définit pour l'hébergeur Client (voir les restriction au § 3.4.4.2) l'hébergeur K.EEP® server et serveur de stockage (voir les restriction au § 3.4.2.2). Le rôle administrateur socle technique est découpé en deux comptes distincts qui sont Administrateur Root et Administrateur Système. L'administrateur Root dispose de l'ensemble des droits d'administration du socle technique de la plate forme. L'Administrateur Système ne dispose que des accès aux fonctions d'exploitation ; arrêt et démarrage des services, configuration du medium de stockage, lecture des journaux, il assure en outre la supervision technique de la TOE ;

- Porteur de données d'activation (porteur de secret) de la ressource cryptographique matérielle (RCM) : ce sont les rôles définis en fonction du module cryptographique pour la mise en œuvre et la gestion du module cryptographique utilisé par la TOE. Les données d'activation ne peuvent être détenues que par les administrateurs système ;

- Développeur : est responsable du code source des logiciels des modules logiciel de la TOE. Il est également en charge de la gestion en configuration des logiciels de la TOE, de la distribution des versions successives aux utilisateurs et de l'information, auprès des utilisateurs, lors de la découverte de problèmes trouvés dans les logiciels.

3.8 Définition du périmètre de l'évaluation

La TOE est composée des logiciels K.EEP® server . Les serveurs de stockage, Les logiciels K.EEP® (Client) et K.EEP® (Audit) ne font par partie de la TOE.

4 ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT DU PRODUIT

4.1 Architecture matérielle

La plateforme K.EEP® server est constituée de :

- Serveur web ;
- Serveur d'application et sa base de configuration ;
- Serveur cryptographique et sa RCM (Ressource Cryptographique Matérielle) ;

- Serveur de stockage et sa base de référence des fichiers.

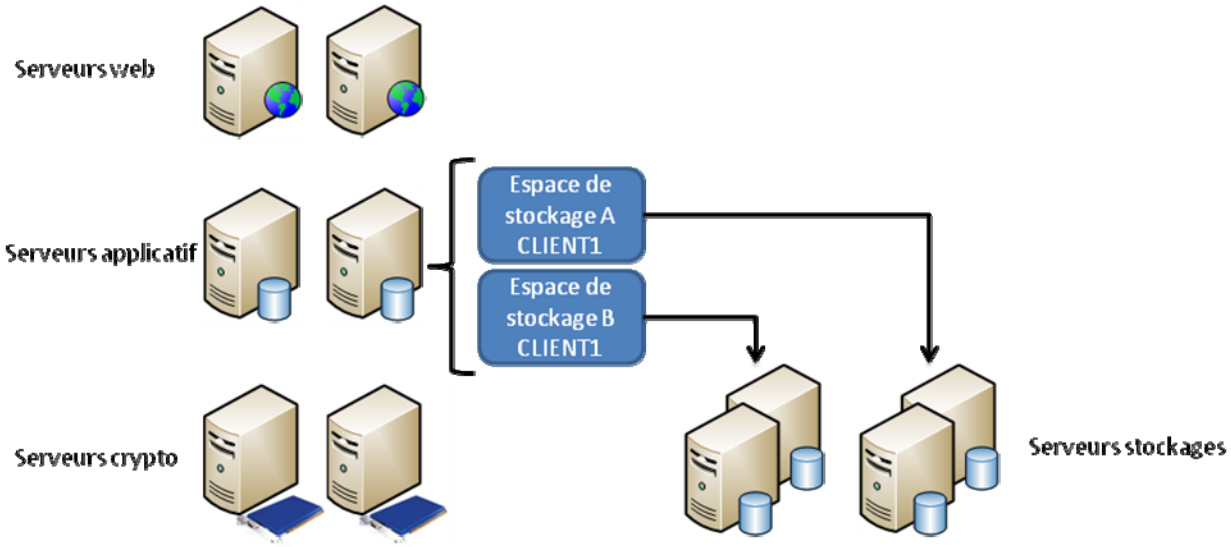

Figure 3 : Architecture physique K.EEP

N.B. : Les 3 premiers serveurs peuvent cohabiter physiquement en fonction des configurations du système hébergeur. Pour des raisons de haute disponibilité de service, il est recommandé de les doubler afin de réduire le risque d'interruption de service.
Le serveur web est une instance d'Apache (v 2.2) avec les modules :

- Mod_ssl : qui permet d'établir des connexions HTTPS avec la plateforme et d'en configurer les accès ;
- Mod_proxy et mod_proxy_ajp : qui permet de router vers le bon serveur applicatif (serveur de signature ou interface d'administration) en fonction de l'URL.

Les serveurs d'application K.EEP® et d'interface d'administration sont des applications web (J2EE) déployées dans des instances de serveur JBoss. La communication entre le serveur Web (Apache) et l'application métier (JBoss) repose sur le protocole AJP mis en œuvre par le module mod_proxy et mod_proxy_ajp.

La base de données est une instance de serveur Oracle 11g.

Le serveur cryptographique est composé d'un serveur applicatif fourni par KEYNECTIS ainsi qu'un composant physique RCM (Ressource Cryptographique Matérielle). La communication entre l'application métier et la ressource cryptographique se base sur une interface PKCS#11 : Cryptographic Token Interface Standard version 2.11. Cette norme suit une approche orientée objet, avec pour objectif de rendre indépendant les applications vis-à-vis de la ressource matérielle.

La RCM :

- Génère et protège les clés privées du serveur K.EEP® ;
- Signe les enveloppes sécurisées (via Certify.Center®) ;
- Signer des contremarques de temps (via K.Stamp®).

La conception de K.EEP (architecture n-tiers) rend la TOE flexible et évolutive pour répondre à des exigences de performance, de volumétrie et de sécurité.

La conception de K.EEP® donne des réponses adaptées pour chacun de ces points :

- De plus, K.EEP® permet d'exploiter plusieurs coffres en parallèle (voir § 7.1.1.) ;
- Capacité de stockage : là encore, la modularité de l'architecture permet d'étendre (par duplication verticale) la capacité de stockage sans impacter le reste de la plateforme, avec des unités d'upgrade faibles c'est-à-dire des serveurs standards ;
- Performance et débit : ici la seule particularité du coffre par rapport à une application de gestion classique est la gestion de la cryptographie. 2 atouts du produit sont exploités
    a. Le mode asynchrone, décrit brièvement au § 5.1.2 qui permet de ne signer / horodater qu'un paquet d'événement au lieu de signer chaque événement ;
    b. La modularité applicative qui permet de séparer les fonctions cryptographiques de scellement des fonctions de gestion du coffre qui ne requièrent que du CPU et de l'espace de stockage sur les serveurs de stockage ;

    On peut donc dimensionner les serveurs applicatifs pour atteindre les performances requises sans multiplier les serveurs crypto et RCM ;

La latence : K.EEP® utilise les avantages du mode asynchrone qui permet d'acquitter immédiatement la transaction et de n'effectuer les traitements crypto qu'en batch sur des lots (typiquement toutes les 300 secondes). Architecture logicielle

D'un point de vue logiciel, la plateforme K.EEP® est composée d'un applicatif K.EEP® précédé d'un serveur Web qui propose deux interfaces d'accès : une pour l'interface d'administration et une autre pour le service de coffre-fort. L'applicatif K.EEP® se base sur une ressource cryptographique qui aura à charge de signer les enveloppes sécurisées.

Le logiciel de gestion K.EEP® se décompose fonctionnellement en deux serveurs applicatifs :

- Un serveur d'administration qui permet à des opérateurs habilités d'administrer le service.
- Un serveur de service web de coffre fort électronique.

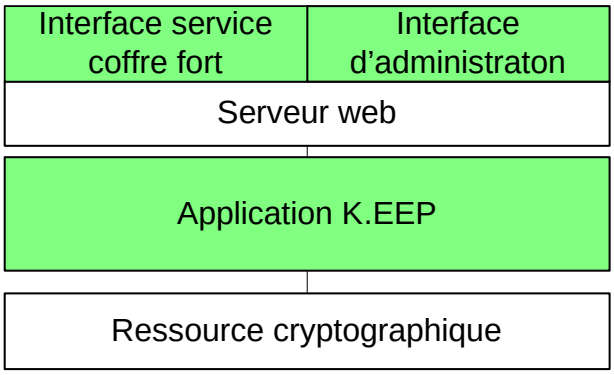

Figure 4 : Architecture logiciel K.EEP®

Tout accès à l'un de ces serveurs sera précédé d'une phase d'autorisation (par connexion HTTPS avec authentification mutuelle) déléguée au serveur Web (Apache). La configuration de cette entité sera donc nécessaire pour :

- Préciser les entités d'opérateur qui auront accès à l'interface d'administration ;
- Préciser les utilisateurs du service.

Pour autoriser l'accès à un serveur, il suffira de préciser les certificats d'AC des entités autorisés pour le serveur correspondant.

4.2 Serveurs de stockage K.EEP®

Un serveur de stockage est un serveur physique sur lequel sont archivées les enveloppes sécurisées. Un serveur de stockage K.EEP® est constitué d'une base de données et dispose d'une capacité suffisante pour accueillir la volumétrie d'archivage souhaitée.

Le serveur doit être dimensionné en fonction des besoins et de la taille souhaitée.

4.2.1 ORACLE

KEYNECTIS a fait le choix d'ORACLE pour sa solution actuelle de coffre fort électronique.
La Fiabilité et la cohérence du stockage sur des gros volumes d'Oracle Database n'est pas à démontrer, lorsque l'on dépasse plusieurs dizaines de gigas octets d'information, il est fondamental que le moteur de gestion de base de données conserve et garantisse la cohérence et la validité des informations et cela même dans des contextes de pannes matérielles et logicielles.

5 BIENS SENSIBLES DEVANT ETRE PROTEGES PAR LE PRODUIT

L'ensemble des clés listées dans le tableau ci-dessous sont obligatoirement distinctes.

Biens	Identifiant du bien	Description
Document	BTOE_1	Ensemble de donnée(s) électronique d'un seul tenant à mettre dans le coffre. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou vis-à-vis de certain rôle de confiance opéré par l'utilisateur de la TOE. Cet élément est aussi à protéger en intégrité.
Demande de dépôt	BTOE_2	Demande construite et transmise par K.EEP® Client qui contient les documents à mettre au coffre. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou vis-à-vis de certain rôle de confiance opéré par l'utilisateur de la TOE.
Enveloppe sécurisée	BTOE_3	Enveloppe construite par K.EEP® server pour un coffre dédié et pour un ensemble de documents dédiés. Une enveloppe sécurisée contient le document chiffré, les métas informations, la signature de scellement et une contremarque de temps. Cet élément est à protéger en confidentialité, au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou vis-à-vis de certain rôle de confiance opéré par l'utilisateur de la TOE. Il est aussi à protéger en intégrité et avoir une date et une heure sûre.
Empreinte de chaînage	BTOE_4	Empreinte de la dernière enveloppe sécurisée créée qui est contenue dans l'enveloppe sécurisée suivante. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte à l'intégrité et la disponibilité de cette donnée.

Meta-information	BTOE_5	Compléments d'informations qui accompagnent le document et qui sont remplis par Client (capteur) et K.EEP® server. Ces compléments d'informations sont contenus dans l'enveloppe sécurisée et signés et horodatés. Les métas informations sont composées de ; l'empreinte de chaînage, de l'empreinte des documents et de la référence des documents. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte à l'intégrité et la disponibilité de cette donnée.
Configuration d'un coffre sur K.EEP® server	BTOE_6	Paramètres permettant la configuration des coffres de K.EEP® server. Cet élément est à protéger en confidentialité et en intégrité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou vis-à-vis de certain rôle de confiance opéré par l'utilisateur de la TOE.
Traces d'audit K.EEP® server	BTOE_7	Journaux contenant des évènements de sécurité stockés par le module base de données du composant K.EEP®. Cet élément est à protéger en confidentialité au sens du cloisonnement vis-à-vis d'un utilisateur de la TOE ou vis-à-vis de certain rôle de confiance opéré par l'utilisateur de la TOE.
Certificat contenant la clé publique RSA de vérification de signature des enveloppes	BTOE_8	Clé utilisée pour vérifier la signature des enveloppes sécurisées. La bi-clé correspondante est dédiée à un ou plusieurs coffres. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte à l'intégrité et la disponibilité de cette donnée.
Certificat contenant la clé publique de chiffrement des enveloppes	BTOE_9	Clé utilisée pour chiffrer la clé AES (BTOE_18). La bi-clé correspondante est dédiée à un ou plusieurs coffres. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte à l'intégrité et la disponibilité de cette donnée.

Certificat contenant la clé publique de vérification de signature de contremarque de temps	BTOE_10	Clé utilisée pour vérifier les contremarques de temps des enveloppes sécurisées. La bi-clé correspondante est dédiée à un ou plusieurs coffres. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte à l'intégrité et la disponibilité de cette donnée.
Certificat contenant la clé publique pour l'authentification SSL sur le serveur K.EEP® server d'un utilisateur Client (déposant et audit) de la TOE.	BTOE_11	Clé et informations du certificat utilisé pour vérifier l'identité d'un utilisateur Client (déposant et audit) lors de session SSL et pour autorisé un utilisateur de la TOE. La bi-clé correspondante est dédiée à un ou plusieurs coffres. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte à l'intégrité et la disponibilité de cette donnée.
Clé publique RSA de vérification de signature des enveloppes.	BTOE_12	Clé utilisée pour vérifier la signature des enveloppes sécurisées. La bi-clé correspondante est dédiée à un coffre. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte à l'intégrité et la disponibilité de cette donnée.
Clé publique de vérification de signature de contremarque de temps.	BTOE_13	Clé utilisée pour vérifier les contremarques de temps des enveloppes sécurisées. La bi-clé correspondante est dédiée à un ou plusieurs coffres. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte à l'intégrité et la disponibilité de cette donnée.
Règles d'accès à la TOE	BTOE_14	Ensemble de règles d'habilitation définit pour autoriser et authentifier les utilisateurs de la TOE en fonction de leur profil. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte à l'intégrité, la confidentialité et la disponibilité de cette donnée.

Référence de document	BTOE_15	Identifiant unique, par coffre, d'un document qui attribué par K.EEP® server est utilisé pour les recherche de document dans le coffre. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte l'intégrité et la disponibilité de cette donnée.
Clé AES	BTOE_16	Clé dédiée au chiffrement de document (BTOE_1) avec l'algorithme AES. Cet élément est à protéger en confidentialité.
Demande de consultation	BTOE_17	Demande construite et transmise par K.EEP® Audit qui contient des demandes de consultation et/ou récupération de document. Cet élément est à protéger par la TOE vis-à-vis d'un utilisateur de la TOE qui interagit avec les interfaces de la TOE afin qu'il ne porte pas atteinte l'intégrité et la disponibilité de cette donnée.

6 DESCRIPTION DES MENACES

La liste des menaces retenues pour la TOE est extraite des méthodes d'attaques au sens du guide **[EBIOS v2]**. Elles sont explicitées par la suite au regard des biens sensibles (Cf. § 5) de la TOE.

En effet, la TOE est une suite logicielle mise en œuvre au sein d'un ou de plusieurs systèmes d'information hébergés. Par conséquent les menaces non retenues pour la TOE sont prises en comptes dans l'analyse de risque des hébergeurs, l'un comme l'autre devant respecter au minimum les exigences de la présente cible de sécurité.

Les menaces applicables à la TOE sont les suivantes :

- Thème 3 – Perte de services essentiels
  - 13- Perte des moyens de télécommunication
- Thème 5 – Compromission des informations
  - 19 – Ecoutes passives
  - 23 - Divulgation
  - 24 – Informations sans garanties d'origines
  - 26 – Piégeage du logiciel
- Thème 6 – Défaillances techniques
  - 30 – Saturation du système informatique
  - 31 – Dysfonctionnement logiciel
- Thème 7 – Actions illicites
  - 36 – Altération des données
- Thème 8 – Compromission des fonctions
  - 38 – Erreur d'utilisation
  - 39 – Abus de droit
  - 40 – Usurpation de droit
  - 41 – Reniement d'action

6.1 Menaces sur la TOE

6.1.1.1 M_Rôle_de_confiance (40 et 24)

Un attaquant (externe) se fait reconnaître comme rôle de confiance sur la TOE afin d'utiliser ou d'altérer des fonctions des modules de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité, l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE. Par exemple, un attaquant essaye de déposer des documents à la place d'un client, de consulter des documents à la place d'un client, de détruire des documents stockés temporairement et/ou de modifier des enveloppes sécurisées contenus dans un coffre.

Cette menace concerne tous les biens de la TOE.

6.1.1.2 M_Rôle_de_confiance autorisé (39)

Un attaquant (interne) autorisé par son rôle de confiance accède aux fonctions des modules de la TOE afin d'utiliser ou d'altérer des fonctions des modules de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité, l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE. Par exemple, un attaquant essaye de déposer des documents à la place d'un client, de consulter des documents à la place d'un client, de détruire des documents stockés temporairement et/ou de modifier des enveloppes sécurisées contenus dans un coffre.

Cette menace concerne tous les biens de la TOE.

6.1.1.3 M_Journalisation (41)

Un attaquant (interne) met en œuvre des fonctions des modules de la TOE et renie cette action en portant atteinte aux données nécessaires à l'élaboration de traces d'audits et de preuves. Cette menace altère les garanties d'imputabilité de la TOE qui porte sur les services de la TOE ainsi que sur sa capacité à mettre en œuvres des coffres pour des utilisateurs de la TOE différents. Par un exemple un rôle autorisé ou non, essaye de modifier les journaux de la TOE afin de cacher certaines actions.

Cette menace concerne tous les biens de la TOE.

6.1.1.4 M_Erreur_d'utilisation (38, 39 et 31)

Un utilisateur ou la TOE commet une erreur lors de l'utilisation des fonctions des modules de la TOE entraînant une utilisation non conforme des fonctions de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité (pour les biens que l'attaquant n'est normalement pas autorisé à gérer), l'imputabilité et la disponibilité des données et de tous ou partie des services de la TOE. Par exemple, le logiciel K.EEP® server peut modifier la référence d'un document et impliquer que les documents mis dans les enveloppes sécurisés ne correspondent pas à ceux stockés dans le serveur de stockage. Un déni de service peut survenir si les accusés de dépôt sont mal gérés et engendrer ainsi une perte de données. L'application K.EEP® server peut se tromper dans l'insertion des empreintes de chaînage et/ou des méta-informations. Une erreur d'utilisation fait qu'un Client est déclaré comme utilisateur de la TOE avec un profil qui lui permet de faire plus qu'un Client (administrer, …).

Cette menace concerne tous les biens de la TOE.

6.1.1.5 M_Altération_des_biens (36 et 26)

Un attaquant (interne ou externe) accède aux moyens de communication des modules de la TOE et altère la transmission des informations (par interception, insertion, destruction, …) qui circulent entre les modules de la TOE et entre les modules de la TOE et les rôles de confiance de la TOE ou altère

les biens de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité (pour les biens que l'attaquant n'est normalement pas autorisé à gérer), l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE.

Cette menace concerne tous les biens de la TOE.

6.1.1.6 M_Divulgation (23 et 19)

Un attaquant (interne ou externe) diffuse des biens de la TOE à d'autres modules de la TOE non censé gérer les données reçues ou à l'extérieur de la TOE. L'attaquant peut ainsi porter atteinte à la confidentialité, l'intégrité, l'imputabilité et la disponibilité des données et de tout ou parties des services de la TOE.

Cette menace concerne les biens de la TOE (BTOE_1, BTOE_2, BTOE_3, BTOE_4, BTOE_5, BTOE_6, BTOE_8, BTOE_9, BTOE_10, BTOE_14, BTOE_15 et BTOE_17).

6.1.1.7 M.Déni de service (13 et 30)

Un attaquant (interne ou externe) perturbe la communication entre le K.EEP® server et le capteur. Cette perturbation a pour but de créer un débordement non contrôlé des documents au niveau de K.EEP® server qui entraînerait une altération des documents et une perte des documents. L'attaque porte ainsi atteinte à la disponibilité et l'intégrité des données.

Cette menace concerne les biens de la TOE (BTOE_1 et BTOE_2).

7 DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

7.1 Fonction_1 : Administration de K.EEP® server

L'ensemble des rôles sont gérés comme suit :

- La création d'un espace de stockage (BTOE_6), et espace associé sur Certify.Center® et K.Stamp®, est à la charge d'un utilisateur de la TOE avec le profil opérateur appelé « **Workspace Management** ». L'utilisateur de la TOE avec un profil « **WorkspaceManagement** » a la possibilité d'activer ou désactiver un coffre. La configuration d'espace de stockage (coffre), et des services Certify.Center® et K.Stamp®, est à la charge d'un profil opérateur appelé « **Ds Management** ». Un espace de stockage (coffre) K.EEP® permet de configurer les éléments suivants :

    - Le(s) certificat(s) de chiffrement (BTOE_9) pour assurer la confidentialité des données à archiver ;
    - Les certificats de signature (BTOE_8) et d'horodatage (BTOE_10) ;
    - Configuration d'un coffre, et des services Certify.Center® et K.Stamp®, (BTOE_6) qui comprend entre autre les éléments suivants :
        - L'adresse URL du service de signature Certify.Center® pour le scellement (signature électronique) des enveloppes à archiver au format XADES-T ;
        - L'adresse URL du service K.Stamp® pour l'horodatage des enveloppes ;
        - Les informations des certificats utilisés ;
        - La période de validité du coffre ;
        - Le quota de nombre maximum d'enveloppes sécurisées à archiver ;

- L'accès au serveur physique de stockage distant (base de données) ;
- Le mode de fonctionnement asynchrone du coffre pour l'archivage. K.EEP® diffère la création de l'enveloppe sécurisée et donne la possibilité de regrouper un certain nombre de documents dans une même enveloppe (lot de documents) :
    - Les deux critères suivants sont paramétrables :
        - Durée maximale entre deux lots (en secondes)
        - Nombre maximal de documents par lot

- Les utilisateurs de la TOE de type Client (BTOE_11) sont déclarés par l'utilisateur de la TOE avec un profil « **UserManagement** ». Les habilitations accès des applications clientes et leur habilitations à utiliser les services du coffre. Un service de coffre offre trois opérations possibles :
    - Enregistrement d'un document (Client déposant) ;
    - Recherche de documents (Client audit) ;
    - Téléchargement d'une enveloppe sécurisée (Client Audit) ;

- L'utilisateur de la TOE avec un profil opérateur appelé « **Key Management** » génère les bi-clés et PKCS#10 suivants :
    - La génération de la bi-clé (BE_1 et BTOE_12) sur l'équipement cryptographique (RCM). Les bi-clés ainsi générées auront le type et la longueur précisés par le système cryptographique positionné par l'opérateur possédant le rôle « **Key Management** » sur Certify.Center® ;
    - La récupération de la demande de certificat (CSR) ainsi émise correspondant à la clé publique précédemment générée (BTOE_12) au format PKCS#10 ;
    - La génération de la bi-clé (BE_3 et BTOE_13) sur l'équipement cryptographique (RCM). Les bi-clés ainsi générées auront le type et la longueur précisés par le système cryptographique positionné par l'opérateur possédant le rôle « **Key Management** » sur l'interface K.Stamp® ;
    - La récupération de la demande de certificat (CSR) ainsi émise correspondant à la clé publique précédemment générée (BTOE_13) au format PKCS#10.

7.2 Fonction_2 : Authentification et autorisation des utilisateurs de la TOE sur K.EEP® server

Les utilisateurs de la TOE (Client et rôle de confiance) du produit K.EEP® server s'authentifient sur l'interface d'administration avant toute opération de configuration, l'interface de dépôt avant tout de de document et interface de lecture avant toute consultation. L'authentification est réalisée à l'aide d'un certificat électronique délivré par une AC reconnue de confiance et installée sur les serveurs web.

L'authentification, l'identification et l'autorisation des utilisateurs de la TOE utilise des règles d'accès (BTOE_14) et le certificat de l'utilisateur (BTOE_12 et BTOE 11) et d'AC (BE_7 et BE_11).

7.3 Fonction_3 : Création et Sécurisation de l'enveloppe pour mise au coffre sur K.EEP® server

Une enveloppe K.EEP® (BTOE_3) est un document au format XML contenant **les données à archiver** (BTOE_1) ainsi que des **méta-informations** (BTOE_5) associées. Les méta-informations (BTOE_5) sont un ensemble structuré d'informations (format XML nœud/valeur) qui accompagne le document (BTOE_1) à archiver. Elles ne seront pas utilisées dans l'opération de recherche de

documents. Le Client déposant est libre de positionner les informations de son choix. Le coffre selon les traitements particuliers qui lui seront demandés pourra également renseigner des informations avant scellement (signature et horodatage) et archivage de l'enveloppe.

Dans le cadre de l'offre « jeux en ligne », les données encapsulées dans l'enveloppe K.EEP® sont un événement ou un lot d'événements au format XML.

Dans le cadre de l'offre « jeux en ligne », le coffre positionne les méta-informations suivantes :

- L'empreinte de chaînage ;
- L'empreinte des documents ;
- La référence des documents.

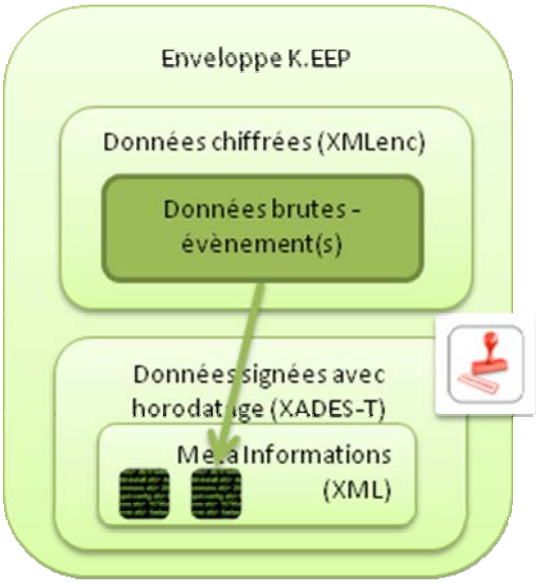

Figure 5 : Enveloppe K.EEP® sécurisée

L'enveloppe sécurisée est constituée des éléments suivants :

- Document chiffré : Le ou les document(s) (BTOE_1) est chiffré en utilisant le standard XMLenc [R1] à l'attention d'un certificat ou de plusieurs certificats (X.509) (BTOE_9). Pour le chiffrement une clé AES dédiée (BTOE_16) pour une enveloppe sécurisée est générée par K.EEP® server. Les données (BTOE_1) sont chiffrés avec la clé AES (BTOE_16) et la clé AES est chiffrée avec la clé de chiffrement (BTOE_9) ;

- Méta-informations signées et horodatées : L'empreinte des données de jeux est enregistrée dans les méta-informations (BTOE_5). L'ensemble des méta-informations (BTOE_5) subit une opération de scellement (signature, scellement, effectuée par le service Certify.Center® avec la clé privée BE_1) et est horodatée (élaboration d'une contremarque de temps effectuée par le service K.Stamp® avec la clé privée BE_3). Le document issu de ce scellement est un document respectant le standard XADES-T [R2] qui constitue l'enveloppe sécurisée (BTOE_3).

Le service K.Stamp® assure la synchronisation avec la source de temps de confiance externe (Se reporter à H_Temps de référence) et l'élaboration et la signature de la contremarque de temps.

L'enveloppe sécurisée ainsi obtenue est archivée sur le serveur de stockage par le logiciel K.EEP® server. Suite à l'acquittement du serveur de stockage signifiant la bonne exécution de l'opération de stockage, le logiciel K.EEP® server supprime le ou les documents qui ont fait l'objet de la création de l'enveloppe sécurisée.

7.4 Fonction_4 : Chaînage des enveloppes dans un coffre sur K.EEP® server

Le coffre fort électronique implémente un mécanisme de chaînage des données au travers du scellement (signature électronique avec la clé BE_1). Ce chaînage a pour objectif de démontrer l'intégrité de la complétude des données archivées dans le temps par rapport aux données précédemment archivées.

Le coffre fort électronique assure ce chaînage en ajoutant aux méta-informations (BTOE_5), faisant partie des données scellées (signature électronique avec la clé BE_1) l'empreinte de la signature précédente (BTOE_4) d'enveloppe sécurisée. Le chaînage pourra ainsi être vérifié par le logiciel auditeur (K.EEP® Audit).

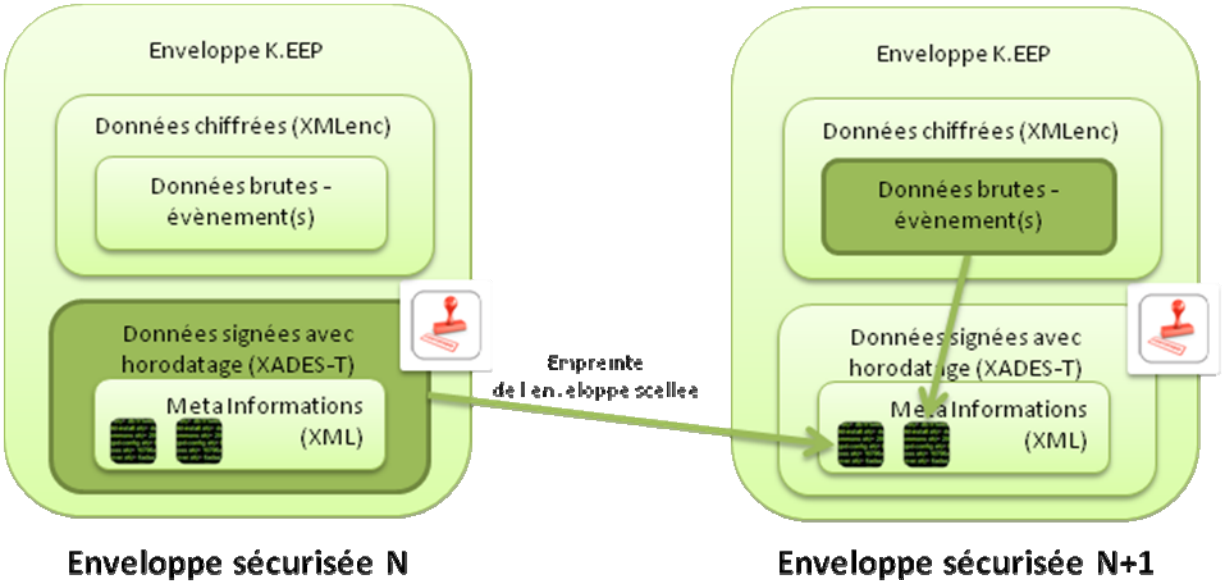

Figure 6 : Modèle de chaînage des enveloppes archivées

7.5 Fonction_5 : Audit et statistiques sur K.EEP® server

L'audit (BTOE_7) est accessible en lecture depuis l'interface d'administration, il journalise toutes les opérations d'administration.

Le produit K.EEP® dispose par ailleurs des journaux de sécurité de sa ressource cryptographique et de journaux système propres à chaque machine.

L'utilisateur de la TOE avec le profil opérateur appelé « Audit Management » peut consulter des informations d'audit lors d'une session SSL, au travers du portail d'administration.

7.6 Fonction_6 : gestion de clé secrète AES pour chiffrement de document

Le logiciel K.EEP® server, pour chaque élaboration d'enveloppe sécurisée, génère une clé secrète AES (BTOE_16) afin de chiffrer le document qui sera contenu dans l'enveloppe sécurisée. Cette clé est ensuite détruite après chaque création d'enveloppe sécurisée.

8 DESCRIPTION DES MECANISMES CRYPTOGRAPHIQUES

Les caractéristiques cryptographiques sont données ici de manières synthétiques dans ce document car à cette cible de sécurité est associé un document « DS_Cotation cryptographique K.EEP® » qui est livré par ailleurs à l'ANSSI dans le cadre de la certification CSPN.

Les caractéristiques sont les suivantes :

Données et/ou fonctions	Algorithme(s)	Taille des clés
Certificat AC	RSA avec SHA	2048 minimum pour RSA et 256 pour SHA
Certificat contenant la clé publique de chiffrement des enveloppes	RSA avec SHA	2048 minimum pour RSA et 256 pour SHA
Certificat contenant la clé publique RSA de vérification de signature des enveloppes	RSA avec SHA	2048 minimum pour RSA et 256 pour SHA
Certificat contenant la clé publique de vérification de signature de contremarque de temps	RSA avec SHA	2048 minimum pour RSA et 256 pour SHA
Certificat contenant la clé publique pour l'authentification SSL sur le serveur K.EEP® server d'un utilisateur de la TOE hors K.EEP® Client.	RSA avec SHA	2048 minimum pour RSA et 256 pour SHA
Empreinte de chaînage	SHA	256
Signature des enveloppes sécurisées	RSA avec SHA	2048 minimum pour RSA et 256 pour SHA
Signature des contremarques de temps	RSA avec SHA	2048 minimum pour RSA et 256 pour SHA
Chiffrement des documents contenus dans les enveloppes sécurisées	RSA avec AES	2048 minimum pour RSA et 256 pour AES
Session SSL avec K.EEP® server	RSA avec SHA	2048 minimum pour RSA et 160 pour SHA

9 GLOSSAIRE

[R1] XML Encryption Syntax and Processing, W3C Recommendation 10 December 2002
[R2] XML Advanced Electronic Signatures (XAdES), W3C Note 20 February 2003