Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2011/10

K.EEP
Version 2.91

Paris, le 8 juillet 2011

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

[Original signé]

Patrick Pailloux

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2011/10

Nom du produit

K.EEP Server

Référence/version du produit

Version v2.91

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU

(CSPN, Phase expérimentale)

Développeur(s)

KEYNECTIS

11-13, rue René Jacques

92131 Issy les Moulineaux

France

Commanditaire

KEYNECTIS

11-13, rue René Jacques

92131 Issy les Moulineaux

France

Centre d'évaluation

Oppida

4-6, avenue du Vieil Etang - Bât B

78180 Montigny Le Bretonneux

Tél : +33 (0)1 30 14 19 00, Mél : cesti@oppida.fr

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. LE PRODUIT 6

1.1. PRÉSENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT ÉVALUÉ 6
1.2.1. Catégorie du produit 6
1.2.2. Identification du produit 7
1.2.3. Services de sécurité 7
1.2.4. Configuration évaluée 7

2. L'ÉVALUATION 8

2.1. RÉFÉRENTIELS D'ÉVALUATION 8
2.2. CHARGE DE TRAVAIL PRÉVUE ET DURÉE DE L'ÉVALUATION 8
2.3. TRAVAUX D'ÉVALUATION 8
2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité 8
2.3.2. Installation du produit 8
2.3.3. Analyse de la documentation 9
2.3.4. Revue du code source (facultative) 9
2.3.5. Fonctionnalités testées 9
2.3.6. Fonctionnalités non testées 10
2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités 10
2.3.8. Avis d'expert sur le produit 10
2.3.9. Analyse de la résistance des mécanismes et des fonctions 10
2.3.10. Analyse des vulnérabilités (conception, construction…) 10
2.3.11. Accès aux développeurs 10
2.3.12. Analyse de la facilité d'emploi et préconisations 11
2.4. ANALYSE DE LA RÉSISTANCE DES MÉCANISMES CRYPTOGRAPHIQUES 11
2.5. ANALYSE DU GÉNÉRATEUR D'ALÉAS 11

3. LA CERTIFICATION 12

3.1. CONCLUSION 12
3.2. RESTRICTIONS D'USAGE 12

1. Le produit

1.1. Présentation du produit

La suite logicielle K.EEP de KEYNECTIS gère des coffres forts électroniques qui permettent de stocker des documents de manière sécurisée. Cette suite logicielle est une solution de coffre-fort électronique centralisé destinée à être utilisée dans le cadre des jeux d'argent et de paris en ligne.

La suite logicielle K.EEP est constituée de différentes applications :

- K.EEP Server,
- K.EEP Client,
- K.EEP Audit.

Le produit évalué est « K.EEP Server**,** Version 2.91 **»** développé par KEYNECTIS.

Un coffre associe à chacun des documents stockés une enveloppe de sécurité qui garantit 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 (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 le coffre.

Dans le cas d'une utilisation en France, 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.

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☐ 3 – firewall
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☐ 6 - identification, authentification et contrôle d'accès
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☒ 9 – stockage sécurisé
☐ 10 - matériel et logiciel embarqué
☐ 99- Autres

1.2.2. Identification du produit

La version certifiée du produit est identifiable par le numéro de version suivant : K.EEP Server v2.91. Cette information est affichée en pas des fenêtres d'administration du produit lorsque l'utilisateur s'est authentifié.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit certifié sont :

- authentification et autorisation des utilisateurs accédant à K.EEP Server ;
- création et sécurisation de l'enveloppe pour mise au coffre avec K.EEP Server ;
- chaînage des enveloppes dans un coffre sur K.EEP Server ;
- gestion de clés secrètes AES pour chiffrement de document ;
- administration de K.EEP Server ;
- audit et statistiques sur K.EEP Server.

Les services de sécurité suivants sont exclus de la cible de sécurité :

- dépôt de document dans un coffre sur K.EEP Server avec K.EEP Client ;
- récupération d'une enveloppe dans un coffre sur K.EEP Server avec K.EEP Audit ;
- vérification de l'enveloppe dans un coffre avec K.EEP Audit ;
- extraction de documents d'une enveloppe sécurisée avec K.EEP Audit ;
- gestion des coupures de service.

1.2.4. Configuration évaluée

Matériel	Description	Version minimale
Serveur HP	Serveur matériel	ProLiant DL380 G6 ou DL360 G6
Luna PCI	RCM	Version FIPS 140 –2 level 3

Logiciel	Version
(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-1.6.0_24
Oracle (serveur base de données)	Oracle Database 11g Enterprise Edition Release R2 11.2.0.1.0
Linux RedHat	ES5 Update 5 (Default Install)
Bouncycastle (serveur crpytographique)	(Java) v 1.45
JBoss	ks-jboss-4.0.3SP1-FCS
Linux RedHat	Red Hat Enterprise Linux Server release **5.6** (Tikanga)

Remarque :
Les machines qui sont utilisées en exploitation sont très performantes mais très volumineuses. Pour des raisons purement pratiques, la configuration matérielle utilisée pendant les tests est une machine simplement destinée à mettre en œuvre le produit K.EEP Server. Cette différence matérielle ne remet pas en cause les résultats de l'évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau en phase expérimentale. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La charge de travail a été de 10 jours compte tenu du fait qu'il s'agit d'une réévaluation.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1.Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre « Argumentaire »).

2.3.1.2.Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre « Description des biens sensibles que le produit doit protéger »).

2.3.1.3.Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (Chapitre « Description des menaces »).

2.3.1.4.Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre « Description des fonction de sécurité du produit »).

2.3.1.5.Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre « Argumentaire »).

2.3.2. Installation du produit

2.3.2.1.Plate-forme de test

Pour la plateforme d'évaluation, l'installation et la configuration du socle commun ont été réalisées par le développeur dans ses locaux avant l'envoi des machines au CESTI.

Bien que la cible de sécurité prévoie la possibilité d'utiliser deux modèles de modules cryptographiques, seul le produit « Luna PCI » a été utilisé dans l'évaluation.

2.3.2.2.Particularités de paramétrage de l'environnement

Chacun des modules logiciels cités dans le paragraphe 1.2.4 fait l'objet d'un paramétrage spécifique qui est détaillé dans un manuel spécifique.

2.3.2.3.Options d'installation retenues pour le produit

Le produit en évaluation a été livré au CESTI déjà installé.

2.3.2.4.Description de l'installation et des non-conformités éventuelles

Le produit en évaluation a été livré au CESTI déjà installé.

2.3.2.5.Durée de l'installation

Le produit en évaluation a été livré au CESTI déjà installé.

2.3.2.6.Notes et remarques diverses

Le produit en évaluation a été livré au CESTI déjà installé.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est complexe à utiliser.

2.3.4. Revue du code source (facultative)

Les évaluateurs n'ont pas eu accès au code source.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Administration de K.EEP Server Test des accès avec différents profils d'utilisateurs	Réussite
Authentification et autorisation des utilisateurs de la TOE sur K.EEP Server Test des accès à l'interface d'administration web avec différents profils d'utilisateurs	Réussite
Création et Sécurisation de l'enveloppe pour mise au coffre sur K.EEP Server Tests de bon fonctionnement divers	Réussite
Chaînage des enveloppes dans un coffre sur K.EEP Server Tests de mise en défaut du système	Réussite
Audit et statistiques sur K.EEP Server Test de consultation avec différents profils	Réussite

2.3.6. Fonctionnalités non testées

Néant.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

Les fonctionnalités testées ont reçu un verdict « Réussite ».

2.3.8. Avis d'expert sur le produit

Le produit est relativement complexe. Il est constitué d'un ensemble de modules génériques qui sont assemblés et paramétrés pour délivrer un service donné, ici un coffre fort électronique.
De ce fait, l'installation, l'exploitation et l'utilisation du produit K.EEP Server demandent une forte expertise. Les équipes d'exploitation de KEYNECTICS ont cette expertise mais une formation et un soutien sont nécessaires pour une exploitation externe à KEYNECTICS.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1.Liste des fonctions et des mécanismes testés - résistance

L'avis sur la résistance des mécanismes est donné au §2.3.9.2.

Fonction et mécanisme
mécanisme d'authentification des utilisateurs par certificat de bi-clé
mécanisme de chiffrement des documents mis au coffre

2.3.9.2.Avis d'expert sur la résistance des mécanismes

Ces deux mécanismes sont considérés comme robustes et suffisants dans le cadre d'une évaluation CSPN.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il a été identifié deux vulnérabilités connues et mineures applicables à ce produit. Pour autant, ces vulnérabilités n'ont pas pu être exploitées dans le cadre de l'utilisation du produit pour des jeux en ligne.

2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Les vulnérabilités résiduelles ne sont pas exploitables dans le cadre de l'utilisation du produit pour des jeux en ligne.

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Lors des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une bonne maîtrise de son produit et a été en mesure de répondre aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Le profil « administrateur technique et opérationnel » possède un accès logique aux machines de la plateforme via l'interface d'administration technique. Une vigilance particulière doit être apportée à la gestion des vulnérabilités qui pourraient apparaître sur le socle (système notamment) pour éviter toute escalade de privilèges. Les opérations peuvent dérouler sous la supervision de l'ARJEL pour éliminer ce risque.

Pour mémoire, certaines hypothèses fondamentales sont rappelées ci-dessous :
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.

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.

2.3.12.3. Avis d'expert sur la facilité d'emploi

Le produit évalué KEEP Server est constitué de plusieurs modules qui demandent une certaine expertise pour être exploitée efficacement.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Certains mécanismes cryptographiques mis en œuvre par le produit ne suivent pas les recommandations du référentiel [REF-CRY]. Cependant, les écarts constatés ne remettent pas en cause le niveau de résistance aux attaques visées par la CSPN.
Il est recommandé que la mise en conformité de ces mécanismes se fasse lors d'une prochaine évolution du produit.

2.5. Analyse du générateur d'aléas

Les moyens mis en œuvre pour la génération des nombres aléatoires qui sont utilisés dans différentes fonctions permettent d'atteindre le niveau de résistance aux attaques visé par la CSPN.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « K.EEP Server**,** Version 2.91 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS].

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

Malgré l'hypothèse de la cible de sécurité, si l'administrateur ne peut pas être considéré comme étant de confiance, certaines fonctions d'administration de la plateforme ne garantiront pas, seules, la sécurité du produit. Les recommandations du paragraphe 2.3.12.2 permettent d'atteindre le niveau de sécurité visé.

Le présent certificat concerne uniquement la configuration avec « Luna PCI ».

Lors de l'utilisation de la suite logicielle K.EEP, l'utilisateur devra s'assurer que la sécurité repose bien sur les services de sécurité de K.EEP Server décrits dans la cible de sécurité et repris au paragraphe 1.2.3.

Annexe 1. Références documentaires du produit évalué

[CDS]	*K.EEP - CSPN – Cible sécurité* - Référence : *DS_CSPN_KEEP_Cible v 1.7* ; - Date : 25 Avril 2011
[RTE]	*CSPN : Rapport technique d'évaluation (RTE) - K.EEP ;* - Référence : *OPPIDA/CESTI/K.EEP/RTE/3.0* ; - Date : *1er mai 2011*
[ANA-CRY]	*Cotation cryptographique.: K.EEP, version du produit : 2.9 ;* - Référence : CSPN_CRYPTO_K.EEP_v1.1 ; - Date : *7 décembre 2010*
[GUIDES]	*Manuels d'installation* Manuel d'installation plateforme DS ERD_INST_DS_2.9_1.0.doc Manuel d'installation certify center ERD_INST_DS_CERTIFY.CENTER_2.9_1.0.doc Manuel d'installation K.EEP ERD_INST_DS_K.EEP_2.9_1.0.doc Manuel d'installation K.Stamp ERD_INST_DS_K.STAMP_2.9_1.0.doc Manuel d'installation K.Valid ERD_INST_DS_K.VALID_2.9_1.0.doc Manuel d'installation HSS ERD_INST_HSS_2.13_0.2.doc Manuel d'installation du socle technique commun SEQUOIA ERD_INST_SOCLE_COMMUN_SEQUOIA_1.1_1.2.doc *Manuels utilisateur* Manuel utilisateur CERTIFY.CENTER ERD_MU_CERTIFY.CENTER_2.9_1.0.pdf Manuel Utilisateur de la plate-forme DS ERD_MU_DS-2.9_1.0.doc Manuel utilisateur KEEP ERD_MU_K.EEP_2.9_1.0.doc Manuel utilisateur KSTAMP ERD_MU_KSTAMP-2.9_v1.0.doc Manuel utilisateur KVALID ERD_MU_KVALID-2.9_v1.0.doc *Manuels d'exploitation* Manuel d'exploitation Plate-forme DS ERD_EXPL_DS_2.9_1.0.doc Manuel d'exploitation certify center ERD_EXPL_DS_CERTIFY.CENTER_2.9_1.0.doc Manuel d'exploitation K.EEP ERD_EXPL_DS_K.EEP_2.9_1.0.doc Manuel d'exploitation K.STAMP

	ERD_EXPL_DS_K.STAMP_2.9_1.0.doc Manuel d'exploitation ERD_EXPL_HSS_2.13_0.2.doc Manuel d'exploitation du socle technique commun SEQUOIA ERD_EXPL_SOCLE_COMMUN_SEQUOIA_1.1_1.0.doc Manuel d'exploitation K.VALID ERD_EXPL_DS_K.VALID_2.9_1.0.doc
[CONF]	Manuel de configuration HSS ERD_CONFIG_HSS_2.13_0.1.doc

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2. 4, phase expérimentale, n° 915/SGDN/DCSSI/SDR/CCN du 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1. 4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1. 3. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr