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-2011/02

ATOS Worldline eGambling SB
Version 1.0

Paris, le 5 mai 2011

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

[Original signé]

Patrick Pailloux

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-2011/02

Nom du produit

ATOS Worldline eGambling SB

Référence/version du produit

Version 1.0

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU

(CSPN, Phase expérimentale)

Développeur(s)

Atos Worldline

ZI A rue de la pointe

59113 Seclin

France

Commanditaire

Atos Worldline

ZI A rue de la pointe

59113 Seclin

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 9
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

Le produit évalué, « Worldline eGambling SB**,** Version 1.0 **»,** est un service de « type serveur web » proposé par Atos Worldline qui donne accès à la fonction coffre-fort électronique dans le cadre des jeux en ligne.

Ce produit est destiné à être utilisé 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 appelé coffre-fort électronique.

C'est le service offert par le produit qui est la cible de l'évaluation en vue d'une Certification de sécurité de premier niveau (CSPN).

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

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF] qui doit être fournie par le développeur.

Logiciek	Version	*Vérification*
OS	LINUX 64 bits Red Hat Enterprise Linux Server release 5.3	*cat /etc/redhat-release uname -a*
Noyau	2.6.18-128.el5	*uname -a*
Java	1.6.0_07	*java -version*
JRE	SUN Java(TM) SE Runtime Environment (build 1.6.0_07-b06)	*java -version*
OpenSSH	OpenSSH_5.2p1	*sshd -v*
OpenSSL	OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008	*openssl version*
Apache	2.2.14 avec OpenSSL/0.9.8o	*httpd -version + lire le contenu du fichier errors*
Tomcat	5.5.25	*sh /usr/local/apache-tomcat-5.5.25/bin/version.sh*
ActiveMQ	5.3.2	*ll /usr/local/activemq/release*
MySQL	5.1.41-AWL-Enterprise-log	*SELECT VERSION()*
Samhain	2.4.6a	*rpm -qf /usr/local/sbin/samhain*

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la définition des attributs de sécurité ;
- l'authentification ;
- la politique de contrôle d'accès ;
- la fonction de contrôle d'accès ;
- la confidentialité et l'intégrité des échanges ;
- les opérations cryptographiques ;
- l'administration des fonctions de sécurité ;
- l'administration des attributs de sécurité ;
- la gestion des profils utilisateur.

L'utilisation combinée de ces services de sécurité permet de traiter les services de sécurité spécifiques suivants :

- le contrôle de l'accès au coffre-fort ;
- le chiffrement des dépôts (création de l'enveloppe) ;
- le scellement des dépôts (création de la trace) ;
- le chaînage des traces ;
- la signature de la configuration du coffre-fort.

1.2.4. Configuration évaluée

La configuration évaluée est la version 1.0 telle que décrite dans la cible de sécurité [ST].

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 prévue lors de la demande de certification était conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours. L'évaluation s'est déroulée d'octobre à décembre 2010.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [ST] 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 [ST] (chapitre « Argumentaire »).

2.3.1.2. Biens sensibles manipulés par le produit

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

2.3.1.4. Fonctions de sécurité

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

2.3.1.5. Utilisateurs typiques

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

2.3.2. Installation du produit

Le produit évalué est un service. Il n'y a donc pas d'installation du produit par l'utilisateur.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée.

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
Dépôt d'un lot de transactions via l'interface de la file d'entrée (cas nominal et diverses variantes)	Réussite
Dépôt d'un lot de transactions via l'interface web service (cas nominal et diverses variantes)	Réussite
Contrôle de la qualité des archives déposées à travers diverses interfaces (cas nominal et diverses variantes)	Réussite
Contrôle de l'agrégation de traces (cas nominal)	Réussite
Chiffrement (cas nominal)	Réussite
Chaînage horodatage (cas nominal)	Réussite
Reprise de traitement – contrôle d'exhaustivité et de chaînage (cas nominal)	Réussite
Fonction d'archivage sur différentes durées	Réussite
Fonction de consultation	Réussite
Fonction d'extraction	Réussite
Fonction d'administration	Échec
Accès aux interfaces de consultation et d'administration	Réussite
Tests fonctionnels divers	Réussite

2.3.6. Fonctionnalités non testées

L'application de vérification de l'intégrité des traces et leur déchiffrement est hors du périmètre de la cible de sécurité ; cette exclusion est justifiée par le fait que les dépôts sont stockés et exportés chiffrés et signés, garantissant leur confidentialité et leur intégrité jusqu'à l'ARJEL.

L'application de consultation / exportation des archives est hors du périmètre de l'évaluation car elle a déjà été validée par l'ARJEL dans un autre contexte.

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

Parmi les fonctionnalités testées, seule la fonction d'administration présente une non-conformité.

En effet, un « administrateur technique et opérationnel » du service, donc employé de Atos Worldline, a accès à certaines fonctions qui sont normalement de la responsabilité de l'ARJEL ou de ses représentants. Ce point est non conforme à la cible de sécurité qui, de plus, spécifie que les administrateurs techniques ne peuvent être considérés de confiance.

2.3.8. Avis d'expert sur le produit

Le produit est conforme à sa cible de sécurité, à l'exception citée ci–dessus.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1.Liste des fonctions et des mécanismes testés - résistance

Fonction et mécanisme
Interface de dépôt HTTPS
Interface de dépôt ActiveMQ
Interface de consultation / extraction
Interface d'administration fonctionnelle

2.3.9.2.Avis d'expert sur la résistance des mécanismes

L'empilement de plusieurs mécanismes de contrôle d'accès / authentification pour chacune des interfaces du coffre-fort permet de limiter l'accès aux interfaces, par ailleurs restreint aux seules personnes autorisées. L'authentification aux quatre interfaces du coffre-fort est sûre.

La robustesse repose principalement sur la protection des clés privées.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1.Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier.

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

Aucune.

2.3.11. Accès aux développeurs

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

Compte « administrateur technique et opérationnel ».

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 donnée 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.

Authentification des interfaces par les applications.

Les applications utilisant les interfaces « métier » de la plateforme, à savoir le capteur et l'application externe utilisée par les lecteurs, doivent impérativement authentifier (à l'aide d'un truststore contenant le certificat de l'interface de la plateforme par exemple).

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

L'utilisation des interfaces « métier » de la plateforme est simple et intuitive et l'accès aux fonctionnalités est immédiat.

L'utilisation des Web Services (interface de dépôt, interface de consultation / extraction) est simple et d'utilisation intuitive. Le développeur fournit une documentation détaillée et illustrée par des exemples.

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 « Worldline eGambling SB**,** Version 1.0 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST].

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 [ST] et suivre les recommandations énoncées dans le présent rapport.

Le développeur doit fournir à l'utilisateur de la plateforme un moyen clair d'identification de la version en cours.

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.

Annexe 1. Références documentaires du produit évalué

[ST]	*Offre d'archivage des transactions en ligne - Certification CSPN – Cible sécurité ;* - Référence : *20100906-CSPN-CibleSécurité-V1.2.pdf* ; - Date : *28 septembre 2010*
[RTE]	*CSPN : Rapport technique d'évaluation (RTE) - Coffre Fort Worldine eGambling SB* - Référence : *[810] RTE_ATOS_Worldline_eGambling_SB_v1.0.pdf* ; - Date : *30 novembre 2010*
[ANA-CRY]	*Analyse des mécanismes cryptographiques - Coffre fort Worldline eGambling SB ;* - *Référence : OPPIDA/CESTI/847/CRYPTO/1.0 ;* - *Date : 30 novembre 2010*
[GUIDES]	Guide d'utilisation : *Jeux en ligne – Archivage des transactions en ligne – Consultation client – Document utilisateur ;* - *Référence : GSB014.04 DocUtiCollecte.pdf ;* - *Date : 13 août 2010* Guide d'administration : *Jeux en ligne – Archivage des transactions en ligne – Administration, document utilisateur ;* - *Référence : GSB016.01.02UtiAdministration.pdf ;* - *Date : 19 juillet 2010*
[CONF]	*Version-Logiciels&Applicatif.;* - *Référence : GSB027.04. Version-Logiciels & Applicatif.xls;* - *Date : Décembre 2010*

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