



*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-2017/01**

### **Worldline eGambling SB**

### **Version 2.0**

*Paris, le 13 février 2017*

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

Guillaume POUPARD  
[ORIGINAL SIGNE]



## 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 présumées 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@ssi.gouv.fr](mailto:certification@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	<b>ANSSI-CSPN-2017/01</b>
Nom du produit	<b>Worldline eGambling SB</b>
Référence/version du produit	<b>Version 2.0</b>
Catégorie de produit	<b>Stockage sécurisé</b>
Critères d'évaluation et version	<b>CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)</b>
Commanditaire	<b>Worldline</b> ZI A – Rue de la pointe 59113 Seclin France
Centre d'évaluation	<b>Oppida</b> 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux France
Fonctions de sécurité évaluées	<b>Canal TLS entre les acteurs et le coffre-fort</b> <b>Chiffrement des données archivées</b> <b>Chainage des données archivées</b> <b>Scellement des données archivées</b> <b>Fonctions d'administration et de gestion des utilisateurs</b> <b>Fonctions d'administration technique sécurisées</b> <b>Protection des données de configuration</b> <b>Protection anti déni de services</b> <b>Protection de l'intégrité des clients de consultation</b>
Fonction(s) de sécurité non évaluées	<b>Néant</b>
Restriction(s) d'usage	<b>Oui (cf. §3.2)</b>

# 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 CSPN sont disponibles sur le site Internet [www.ssi.gouv.fr](http://www.ssi.gouv.fr).

# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT EVALUE .....	7
1.2.1. <i>Catégorie du produit</i> .....	7
1.2.2. <i>Identification du produit</i> .....	7
1.2.3. <i>Fonctions de sécurité</i> .....	7
1.2.4. <i>Configuration évaluée</i> .....	8
<b>2. L’EVALUATION .....</b>	<b>9</b>
2.1. REFERENTIELS D’EVALUATION .....	9
2.2. CHARGE DE TRAVAIL PREVUE ET DUREE DE L’EVALUATION.....	9
2.3. TRAVAUX D’EVALUATION .....	9
2.3.1. <i>Installation du produit</i> .....	9
2.3.2. <i>Analyse de la documentation</i> .....	9
2.3.3. <i>Revue du code source (facultative)</i> .....	9
2.3.4. <i>Analyse de la conformité des fonctions de sécurité</i> .....	9
2.3.5. <i>Analyse de la résistance des mécanismes des fonctions de sécurité</i> .....	10
2.3.6. <i>Analyse des vulnérabilités (conception, construction, etc.)</i> .....	10
2.3.7. <i>Accès aux développeurs</i> .....	10
2.3.8. <i>Analyse de la facilité d’emploi et préconisations</i> .....	10
2.4. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES .....	10
2.5. ANALYSE DU GENERATEUR D’ALEAS.....	11
<b>3. LA CERTIFICATION .....</b>	<b>12</b>
3.1. CONCLUSION .....	12
3.2. RESTRICTIONS D’USAGE.....	12

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est le « Worldline eGambling SB, version 2.0 » développé par *WORLDLINE*.

Ce produit est destiné à être utilisé par l'AUTORITE DE REGULATION DES JEUX EN LIGNE (ARJEL) afin d'horodater, de chiffrer et d'archiver des données collectées par un opérateur de jeux et paris en ligne.

La figure ci-dessous détaille l'architecture du produit.

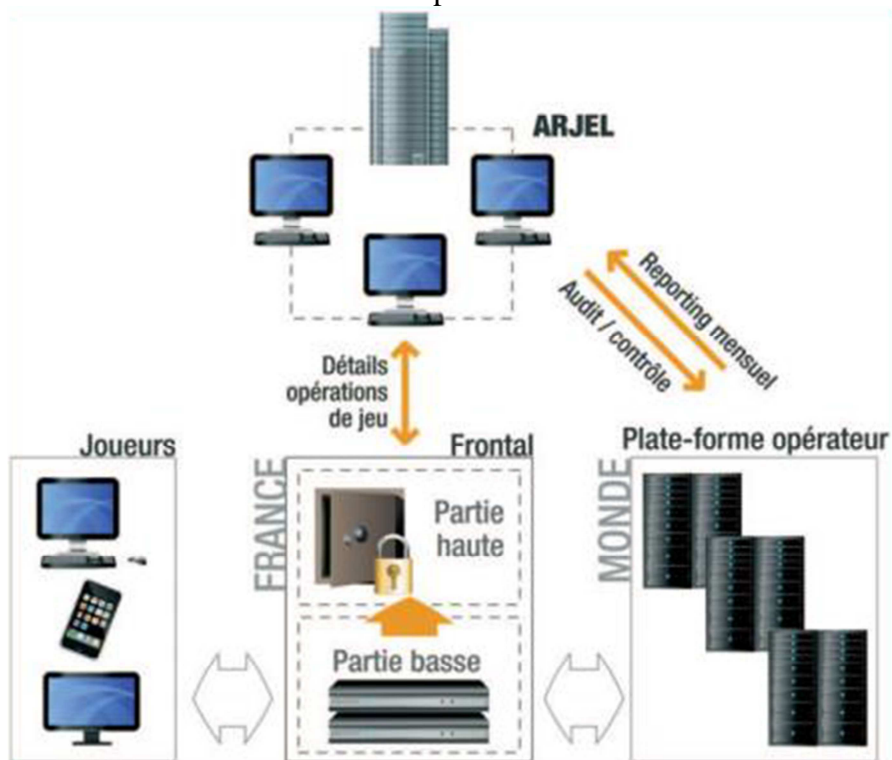


Figure 1 - Architecture de l'infrastructure (le produit Worldline eGambling SB correspondant à « Partie haute » du frontal)

## 1.2. Description du produit évalué

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

### 1.2.1. Catégorie du produit

<input type="checkbox"/> 1 – détection d'intrusions
<input type="checkbox"/> 2 – anti-virus, protection contre les codes malicieux
<input type="checkbox"/> 3 – pare-feu
<input type="checkbox"/> 4 – effacement de données
<input type="checkbox"/> 5 – administration et supervision de la sécurité
<input type="checkbox"/> 6 – identification, authentification et contrôle d'accès
<input type="checkbox"/> 7 – communication sécurisée
<input type="checkbox"/> 8 – messagerie sécurisée
<input checked="" type="checkbox"/> 9 – <b>stockage sécurisé</b>
<input type="checkbox"/> 10 – environnement d'exécution sécurisé
<input type="checkbox"/> 11 – terminal de réception numérique ( <i>Set top box</i> , STB)
<input type="checkbox"/> 12 – matériel et logiciel embarqué
<input type="checkbox"/> 13 – automate programmable industriel
<input type="checkbox"/> 99 – autre

### 1.2.2. Identification du produit

Nom du produit	Worldline eGambling SB
Numéro de la version évaluée	2.0

Les empreintes SHA-256 des différents packages constituant la TOE et correspondant à la version certifiée du produit sont les suivantes :

Package	Empreinte (SHA-256)
gsb-extraction-jar-with-dependencies.jar	e0a82fe368c6303a43107ef04013ed82c0b32b234c9694711286d6e0790d08dc
gsb-injecteurs-jar-with-dependencies-reprise4.jar	946fb0af829c0d6ff4a0836f5faac3d39c4db6755528122306d7b57b9a4c5c1e
gsb-archiveAPI-1.1.5-jar-with-dependencies.jar	f2802c7280cad18f65bedcdce8d888bb55fea3fe9f54f6f58968e9216b50be06

### 1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- le canal TLS entre les acteurs et le coffre-fort ;
- le chiffrement des données archivées ;
- le chaînage des données archivées ;
- le scellement des données archivées ;
- les fonctions d'administration et de gestion des utilisateurs ;
- les fonctions d'administration technique sécurisées ;
- la protection des données de configuration ;

- la protection anti-déni de services ;
- la protection de l'intégrité des clients de consultation.

#### **1.2.4. Configuration évaluée**

La configuration évaluée correspond à la version déployée dans le cadre de l'utilisation faite par l'ARJEL.



## 2. L'évaluation

### 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

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

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

### 2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

#### 2.3.1. *Installation du produit*

##### 2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

L'installation du produit étant réalisée par Worldline l'évaluateur n'a pas eu à installer le coffre-fort Worldline eGambling SB.

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

Néant.

##### 2.3.1.3. Durée de l'installation

Néant.

##### 2.3.1.4. Notes et remarques diverses

Néant.

#### 2.3.2. *Analyse de la documentation*

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit.

#### 2.3.3. *Revue du code source (facultative)*

L'évaluateur a effectué une revue du code source et estime que le code est simple à lire et s'appuie sur des modules Java clairement définies.

#### 2.3.4. *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

### **2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité**

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation de l'ARJEL et pour le niveau d'attaquant visé.

### **2.3.6. Analyse des vulnérabilités (conception, construction, etc.)**

#### **2.3.6.1. Liste des vulnérabilités connues**

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

#### **2.3.6.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert**

Une seule vulnérabilité non connue à ce jour a été identifiée lors de l'évaluation. Cependant, dans le contexte défini par la cible de sécurité [CDS] et les conditions d'utilisation du produit par l'ARJEL, elle n'est pas exploitable.

### **2.3.7. Accès aux développeurs**

Sans objet.

### **2.3.8. Analyse de la facilité d'emploi et préconisations**

#### **2.3.8.1. Cas où la sécurité est remise en cause**

La menace d'altération des traces peut être réalisée par un administrateur, volontairement ou par négligence. Ces derniers doivent donc être sensibilisés à l'utilisation du produit, conformément à l'hypothèse ADMIN\_CONFIANCE de la [CDS].

#### **2.3.8.2. Recommandations pour une utilisation sûre du produit**

Aucune recommandation particulière n'est formulée par l'évaluateur. Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

#### **2.3.8.3. Avis d'expert sur la facilité d'emploi**

Le produit est globalement bien documenté et son utilisation est simple.

#### **2.3.8.4. Notes et remarques diverses**

Cependant une remarque concernant la documentation portant sur le client de validation des archives a été faite par l'évaluateur. Cette dernière pourrait être améliorée pour préciser les modalités des contrôles du caractère sain des archives extraites du coffre.

## **2.4. Analyse de la résistance des mécanismes cryptographiques**

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

## **2.5. Analyse du générateur d'aléas**

L'analyse du générateur d'aléas n'a pas mis en évidence de vulnérabilités exploitables dans les conditions d'emploi considérées.

## 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 2.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

### 3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification, dans les conditions d'utilisation décrite dans [ARJEL] en particulier :

- les administrateurs en charge du maintien en condition opérationnelle du produit Worldline eGambling SB doivent être sensibilisés à la SSI, compétents et de confiance ;
- l'accès physique aux constituants du produit doit être protégé de manière à prévenir toute altération par ce biais ;
- les secrets dont l'ARJEL est propriétaire doivent être opérés dans des conditions de confidentialité adaptées.

## Annexe 1. Références documentaires du produit évalué

[CDS]	<i>CSPN - Cible de sécurité</i> Version : 2.0; Date : 19 septembre 2016
[RTE]	<i>Rapport Technique d'Evaluation CSPN EGAMBLING2016v2</i> Référence : OPPIDA/CESTI/EGAMBLING2016v2/RTE ; Version : 1.0 ; Date : 28 novembre 2016

## 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]	<p>Certification de sécurité de premier niveau des produits (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014.</p> <p>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014.</p> <p>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014.</p> <p>Documents disponibles sur <a href="http://www.ssi.gouv.fr/">www.ssi.gouv.fr/</a></p>
[RGS]	<p>Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B_1), voir <a href="http://www.ssi.gouv.fr/">www.ssi.gouv.fr/</a></p>