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-2012/01

Worldline Signer Server
Version 1.0

Paris, le 29 février 2012

Le directeur général de l'agence nationale
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-2012/01

Nom du produit

Worldline Signer Server

Référence/version du produit

v1.0

Catégorie de produit

Identification, authentification et contrôle d'accès

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Développeur(s)

ATOS WorldLine

19 rue de la vallée Maillard, 41000 Blois
France

Commanditaire

ATOS WorldLine

19 rue de la vallée Maillard, 41000 Blois
France

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, 78180 Montigny le Bretonneux
France

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

1.1. Présentation du produit

Le produit évalué est Worldline Signer Server, v1.0 développé par ATOS WorldLine.

Le produit Worldline Signer Server est un package permettant de réaliser les fonctions de :
- signature de données par apposition de « cachet serveur » ;
- vérification de cachet serveur associé à des données ;
- horodatage de données ;
- vérification de l'horodatage de données.

Il est ainsi possible de réaliser les opérations de création et de vérification de cachets serveur pour une application appelante. L'application appelante est en dehors du périmètre de l'évaluation. Le produit Worldline Signer Server est typiquement utilisé en conjonction avec une application d'archivage, fournissant ainsi des éléments de preuve sur l'archivage des données.
Le produit se décompose en deux parties distinctes :
- une interface Java générique offrant les méthodes de base (création et fermeture de service, création et vérification de cachets serveur) ;
- un système de paramétrage (statique ou dynamique) regroupant toute la description du service qui sera implémenté par le produit.

Le produit n'est pas destiné à une utilisation directe par un humain, il n'y a pas d'interface homme-machine.
Toute la sécurité physique et logique de la machine sur laquelle la cible de l'évaluation est installée est en dehors du périmètre de l'évaluation.

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

☐ 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 les éléments suivants :

Module	Environnement Java	Fichier
Worldline Signer Server, version 1.0	JRE 1.5	wlss-bundle-cspn-1.0.0-jdk1.5.zip
	JRE 1.6	wlss-bundle-cspn-1.0.0-jdk1.6.zip
IAIK	JRE 1.5 JRE 1.6	iaik_cms-4.1.jar iaik_jce-3.181.jar iaik_tsp-2.01.jar iaik_xades-1.3.2_1.16.jar iaik_xect-1.17.jar

La version du produit est vérifiable en exécutant la commande suivante :

- jarsigner -verify wlss-bundle-cspn-1.0.0-jdk1.5.jar pour la version JRE 1.5

ou

- jarsigner -verify wlss-bundle-cspn-1.0.0-jdk1.6.jar pour la version JRE 1.6

En cas de vérification positive, le message est : « jar verified »
En cas de vérification négative, un message d'exception est retourné par l'utilitaire.

Ces éléments sont aussi disponibles dans le bordereau de livraison du produit.

Ils peuvent aussi être vérifiés sur les sites internet du développeur à l'adresse suivante :

- http://www.atosworldline.com/worldlinesigner

Un premier lien pointe vers une page WorldLineSignerServer et un second lien pointe vers une page de suivi des versions.

L'empreinte (SHA256) du module est fournie dans le fichier :

- « condensat- wlss-bundle-cspn-1.0.0-jdk1.5.txt » pour Java 1.5 ou
- « condensat- wlss-bundle-cspn-1.0.0-jdk1.6.txt » pour Java 1.6.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- génération interne ou externe de signature électronique ;
- vérification interne de signature électronique ;
- vérification de la chaine de certificats ayant servie à la signature électronique ;
- horodatage avec un jeton généré en interne ou en externe ;
- vérification interne d'un jeton d'horodatage.

1.2.4. Configuration évaluée

La configuration évaluée est celle par défaut.

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

Une charge de travail de 35 hommes x jours a été consacrée à l'évaluation de Worldline Signer Server conformément à ce qui est prévu lors d'une évaluation CSPN d'un produit comportant des mécanismes cryptographiques.

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 fonctions 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

Logiciels :

- Worldline Signer Server version 1.0 : fichiers: wlss-bundle-cspn-1.0.0-jdk1.6.zip
- Librairies IAIK, Fichiers : iaik_cms-4.1.jar, iaik_jce-3.181.jar, iaik_tsp-2.01.jar, iaik_xades-1.3.2_1.16.jar, iaik_xect-1.17.jar
- Windows XP SP3
- JRE 1.5 Update 22 et JRE 1.6 update 25
- Driver de la carte à puce utilisée (ci-dessous)

Matériels :

- Carte à puce conforme à PKCS#11 (Gemalto)

2.3.2.2. Particularités de paramétrage de l'environnement

L'installation du produit ne nécessite aucun paramétrage particulier.

2.3.2.3. Options d'installation retenues pour le produit

Sans objet.

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

Sans objet.

2.3.2.5. Durée de l'installation

L'installation du produit s'est faite conformément à la procédure décrite dans le guide d'administration [GUIDES]. L'installation a duré une dizaine de minutes.

2.3.2.6. Notes et remarques diverses

L'installation est simple et ne requiert aucune compétence particulière de la part de l'utilisateur.

2.3.3. Analyse de la documentation

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

2.3.4. Revue du code source (facultative)

Les évaluateurs ont eu accès au code source.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Génération de cachet serveur	Réussite
Vérification de cachet serveur	Réussite
Protection du code exécutable du produit	Réussite
Protection des biens sensibles en confidentialité	Réussite
Protection des clés et certificats de cachet serveur	Réussite
Protection des informations de provenance externe	Réussite

2.3.6. Fonctionnalités non testées

Sans objet.

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

Sans objet.

2.3.8. Avis d'expert sur le produit

Le produit est conforme à sa cible de sécurité [CDS]. Aucune non-conformité n'a été détectée sur les fonctions de sécurité du produit, notamment sur les fonctions essentielles que sont la création de cachets serveur et la vérification de cachets serveur.

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
Génération de cachet serveur
Vérification de cachet serveur
Protection du code exécutable du produit
Protection des biens sensibles en confidentialité
Protection des clés et certificats de cachet serveur
Protection des informations de provenance externe

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Ces 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 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 à la documentation technique du produit et n'ont pas eu besoin de contacter directement le développeur.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Le produit propose différentes configurations pour les algorithmes cryptographiques.
Le certificat n'est valide que si ces configurations respectent les règles et recommandations de l'ANSSI concernant les mécanismes cryptographiques [REF_CRY]).

2.3.12.2. Recommandations pour une utilisation sûre du produit

Pour une utilisation sûre du produit, il est très important que :
- les hypothèses sur l'environnement soient appliquées, notamment :
  - la machine sur laquelle la cible de l'évaluation est exécutée est correctement administrée par une personne désignée pour cette tache ; (chapitre 2.4.1 de [CDS]),
  - le personnel (administrateurs / intégrateurs / exploitants) est de confiance et est le seul à pouvoir accéder logiquement et physiquement à la machine sur laquelle la cible de l'évaluation est exécutée ;
  - les clés et certificats utilisés pour la création de cachets serveur et la vérification de cachets serveur sont gérés par une IGC dont les pratiques sont conformes au RGS (chapitre 2.4.6 et 2.4.7 de [CDS]) ;
  - l'application appelante est de confiance (chapitre 5 de [CDS]) ;
- les recommandations de l'évaluateur soient appliquées, notamment :
  - les flux NTP doivent être protégés en authenticité.

Le produit ne devrait pas être utilisé en cas de doute sur la sécurité du système.

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

Le produit Worldline Signer Server n'est pas un produit destiné directement à un utilisateur final. Il est intégré à une application plus globale. Son usage est donc transparent pour l'utilisateur.

2.4. Analyse de la résistance des mécanismes cryptographiques

L'analyse de la résistance des mécanismes cryptographiques a montré que les algorithmes annoncés dans le document des spécifications cryptographiques [SPEC-CRY] sont correctement implémentés dans Worldline Signer Server v1.0.

Le mécanisme de brouillage des données sensibles n'est qu'un moyen de retarder l'accès par l'attaquant aux données sensibles stockées en mémoire vive et n'empêchera pas un attaquant ayant accès à la machine de réussir à extraire ces données sensibles. Cependant, comme le mentionne le rapport d'évaluation [RTE], si les hypothèses sur l'environnement sont respectées, notamment celles liées à la sécurité physique et logique de la machine sur laquelle

la cible de l'évaluation est exécutée, aucun attaquant n'a accès à la mémoire vive. Ce mécanisme de brouillage est donc plus une fonction de défense en profondeur.

2.5. Analyse du générateur d'aléas

Le produit évalué n'utilise pas de générateur aléatoire.

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 Signer Server, version v1.0 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.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Worldline Signer Server, Cible de sécurité CSPN ; Référence : WLSign.AUD.0001 version v1.3, Date : 15 mars 2011*
[RTE]	*Rapport Technique d'Évaluation Worldline Signer Server ; référence : OPPIDA/CESTI/BBP/689/1.0, Date : 22 juillet 2012*
[SPEC-CRY]	*Worldline Signer Server, Mécanismes cryptographiques, reference : WLSign.AUD.0003 version v1.1 Date : 15 février 2011*
[GUIDES]	*Worldline Signer Server, Manuel utilisateur. Référence : WLSign.AUD.0004 version v1.0 Date : 1er mars 2011.*

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 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 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité V.1, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, V1.20 du 26.1.2010