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-CC-2011/32

Worldline Signer One
sur poste de travail

Paris, le 15 novembre 2011

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

[Original signé]

Patrick Pailloux

SÉCURITÉ Ti 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-CC-2011/32

Nom du produit

Worldline Signer One sur poste de travail

Référence/version du produit

Version poste de travail v1.1.1

Conformité à un profil de protection

[PP-ACSE_CCV3.1], version v1.7

Profil de protection Application de création de signature électronique

Critères d'évaluation et version

CC version 3.1 révision 3

Niveau d'évaluation

EAL3 Augmenté

ALC_FLR.3 et AVA_VAN.3

Développeur(s)

Atos Worldline

ZI A Rue de la pointe, 59113 Seclin
France

Commanditaire

Atos Worldline

River Ouest, 80 quai Voltaire, 95877 Bezons
France

Centre d'évaluation

OPPIDA

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

Accords de reconnaissance applicables

CCRA

SOG-IS

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 un logiciel de signature de documents sur poste de travail bureautique. Le produit, nommé « Worldline Signer One sur poste de travail » en version 1.1.1, est développé par Atos Worldline.

Ce produit est destiné à être utilisé par des utilisateurs humains pour la création de signature électronique de documents. Elle permet à ces utilisateurs, sur leur poste de travail personnel de signer électroniquement un ou plusieurs document. Dans le cas où plusieurs documents sont signés dans un mode dit « parapheur électronique », le produit permet de ne saisir qu'une seule fois le code confidentiel pour signer l'ensemble des documents.

1.2. Description du produit

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

La cible de sécurité est strictement conforme au profil de protection [PP-ACSE_CCV3.1].

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version du produit est identifiable sur la page de l'écran principal de signature en cliquant sur le bouton d'aide en bas de la fenêtre. La version certifiée est la version v1.1.1 pour poste de travail
Ces éléments sont aussi disponibles dans le bordereau de livraison du produit.
Ils peuvent aussi être vérifiés sur les sites internet du développeur aux adresses suivantes :

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

Un lien pointe vers une page de suivi des versions.
Le produit évalué est référencé sous l'intitulé « Worldline Signer One plateforme PC : 1.1.1 » et la liste des empreintes (SHA256) des modules est fournie dans le fichier « condensat-1.1.2.txt ».

1.2.2. Services de sécurité

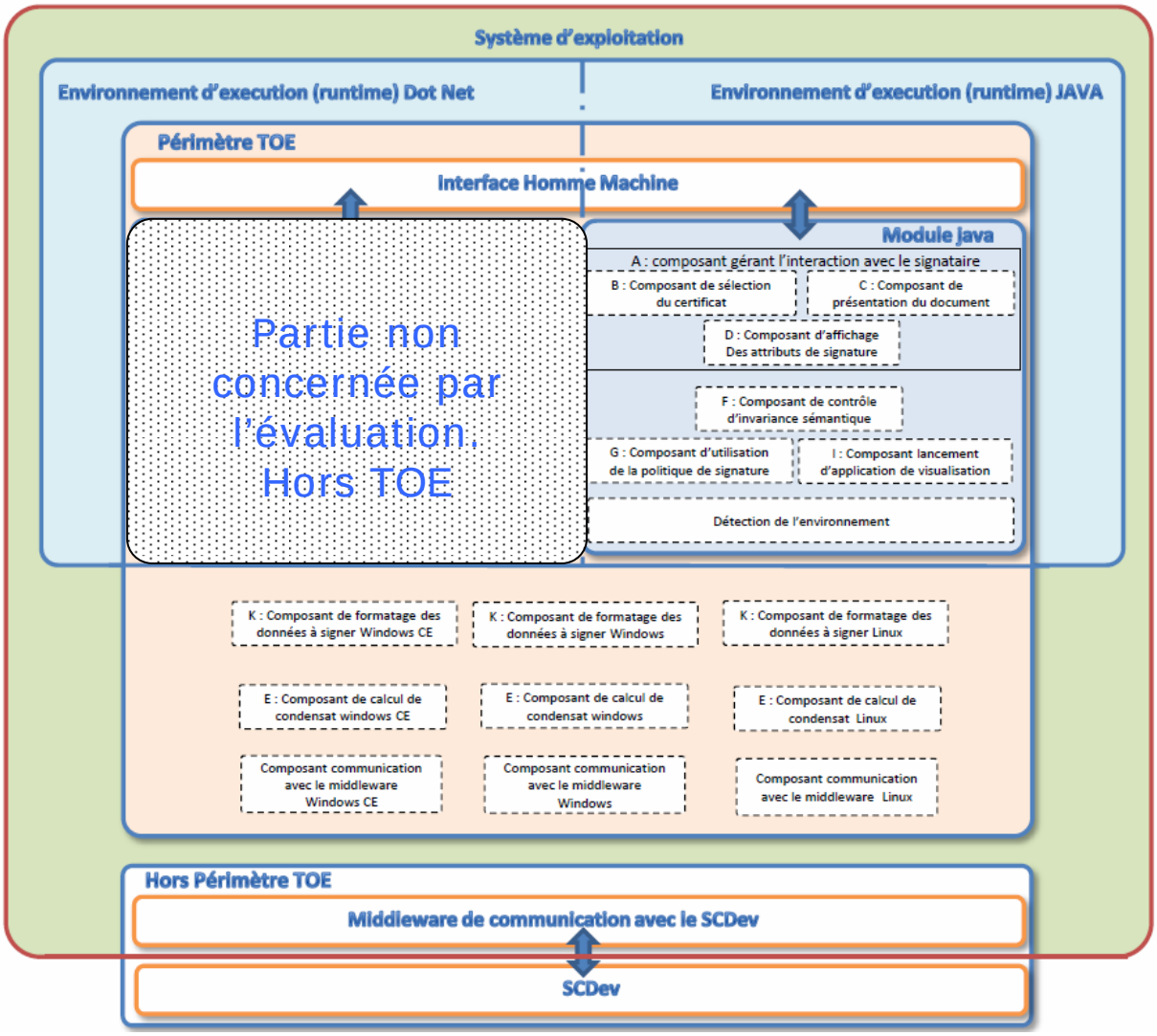
Les principaux services de sécurité fournis par le produit sont :

- vérifier la conformité de la politique de signature (validité dans le temps, authentification de l'émetteur de la politique, intégrité de la politique, conformité sémantique) ;
- donner les informations permettant de filtrer les certificats de signature autorisés (autorité émettrice, gamme de certificat) ;
- donner les informations sur les attributs de signature à inclure ainsi ;
- lister les formats de documents autorisés pour signature par la TOE, ainsi que les modules de visualisation à utiliser pour chacun des formats listés ;
- indiquer l'algorithme de signature à mettre en œuvre ;
- indiquer le format de signature final en réponse par la TOE ;

- limiter le nombre de signatures autorisées lors de l'appel de l'outil.

1.2.3. Architecture

Le produit est constitué de différents modules représentés sur la figure ci-dessous.



En partant du haut vers le bas, nous distinguons sur ce schéma :

- l'interface homme-machine ;
- le module java, pour poste bureautique, qui constitue le cœur du logiciel ;
- les composants de mise en forme des données à signer, de calcul de condensat et de communication avec le middleware ;
- le middleware de communication avec le dispositif de création de signature, dépendant du couple système d'exploitation / navigateur ;
- le dispositif de création de signature.

Les interfaces et les modules exécutables font partie de la cible d'évaluation.
Le middleware et le dispositif de création de signature ne font pas partie de la cible d'évaluation.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

Étape	Lieu
Développement	ATOS Worldline Seclin
Compilation	ATOS Worldline Rennes
Installation	Chez l'utilisateur
Administration	Chez l'utilisateur
Utilisation	Chez l'utilisateur

Le produit a été développé sur les sites suivants :

ATOS Worldline Rennes

2 allée Ermengarde d'Anjou, ZA Atalante Champeaux
35000 Rennes
France

ATOS Worldline Seclin

ZI A Rue de la Pointe
59113 Seclin
France

1.2.5. Configuration évaluée

Pour l'évaluation, le produit a été installé et testé sur la plate-forme suivante :

- CPU : Intel Pentium 4 2.8 GHz / RAM : 512 Mo / Disque dur : 80 Go ;
- lecteur de carte à puce requis ;
- Worldline Signer One sur poste de travail dans les configations identifiées dans le tableau ci-dessous.

	Internet Explorer JRE 5	**FireFox JRE 5**
Windows XP SP3	Module Java. v1.1.1	Module Java. v1.1.1
Windows Seven	Module Java. v1.1.1	Module Java. v1.1.1
Ubuntu 10.04	-	Module Java. v1.1.1

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1, révision 3 [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 9 septembre 2011, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée par l'ANSSI conformément à ses référentiels techniques [REF-CRY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu à la conclusion suivante :
Les mécanismes analysés sont conformes aux exigences du référentiel cryptographique de l'ANSSI (Cf. [REF-CRY]).

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

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. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Worldline Signer One pour poste de travail », version v1.1.1, soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL3 augmentée de ALC_FLR.3 et AVA_VAN.3.

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 se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

Ce certificat fait l'objet d'une reconnaissance internationale

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**3**	Implementation representation CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**1**	Testing: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité Outil de signature Worldline Signer Pro 0ne référence WLS.AUD.0001.12.AV, version v6.0 du 27 mai 2011 éditée par Atos Worldline
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation, Projet WLSO référence OPPIDA/CESTI/WORLDLINE_SIGNER_ONE/RTE/1.1, version v1.2 du 9 septembre 2011 édité par Oppida
[ANA-CRY]	Cotation Cryptographique WLSO, référence 124/ANSSI/ACE, version du 18 janvier 2011 édité par ANSSI
[CONF]	Livraison 1.0.0 référence WLS.D.FDL.0001.10 SV Livraison 1.0.0, version v1.0.0 du 22 novembre 2010, édité par Atos Worldline
[GUIDES]	Guide d'installation du produit : - Guide préparatoire référence WLS.AUD.0013, version v5.0 du 31 mai 2011 édité par Atos Worldline Guide d'utilisation du produit : - Guide utilisateur référence WLS.AUD.0016, version v3.0 du 21 février 2011 édité par Atos Worldline
[PP-ACSE_CCV 3.1]	Protection Profile - Profil de protection Application de création de signature électronique, version v1.7 du 2 mars 2011. Certifié par l'ANSSI sous la référenceANSSI-CC-PP-2008/05-M01.

Annexe 3. Références liées 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.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr