PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/06

AdSignerWeb v3.1.800

Paris, le 28 avril 2006.

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[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 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 le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2006/06

AdSignerWeb v3.1.800

Développeur : Dictao

Critères Communs version 2.2

EAL3 Augmenté

(ADV_IMP.1*, ADV_LLD.1*, ALC_FLR.3, ALC_TAT.1*, AVA_VLA.2)
*appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS.

conforme au profil de protection :
« Application de création de signature électronique »
référence PP-ACSE version 1.0

Commanditaire : Dictao

Centre d'évaluation : Oppida

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)
Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle 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] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.
[2] En mai 2005, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, la Turquie, la République Tchèque, Singapour et l'Inde.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est l'application AdSignerWeb v3.1.800 développée par Dictao.

1.2. Développeur

Dictao

42 avenue de la Grande Armée
75017 Paris

www.dictao.com

1.3. Description du produit évalué

1.3.1. Architecture

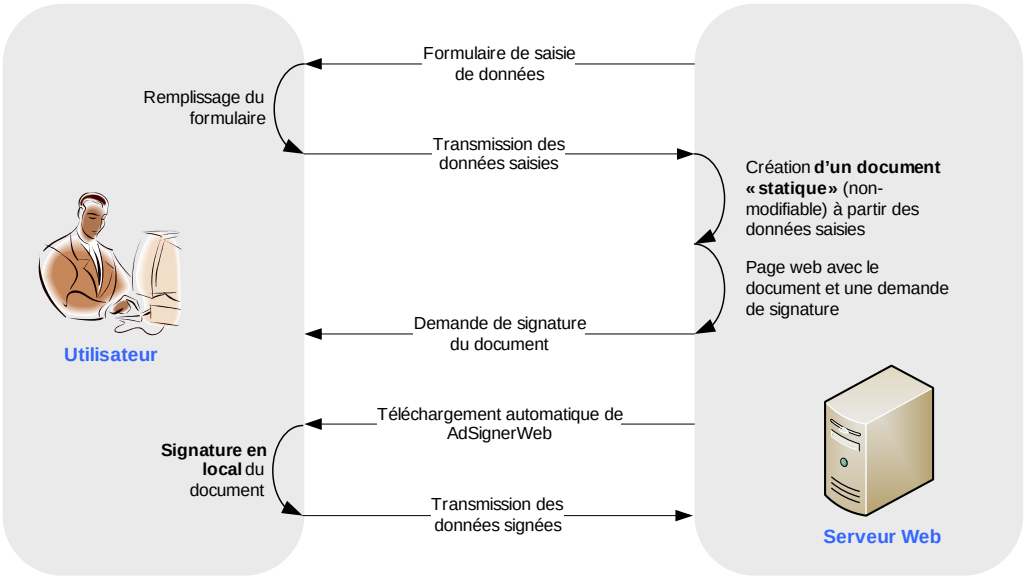
Le module AdSignerWeb permet de créer des signatures électroniques au format XAdES (version 1.1.1 ou 1.2.2) en s'appuyant sur un dispositif de création de signature externe (non évalué). Ce module peut signer des documents au format HTML et texte brut, et effectue lui-même l'interprétation du document HTML et son affichage.

Le module AdSignerWeb est destiné à être utilisé par une application de plus haut niveau, ci-après dénommée application web appelante, et devra s'appuyer sur un dispositif externe de création de signature (carte à puce, token USB ou module logiciel).

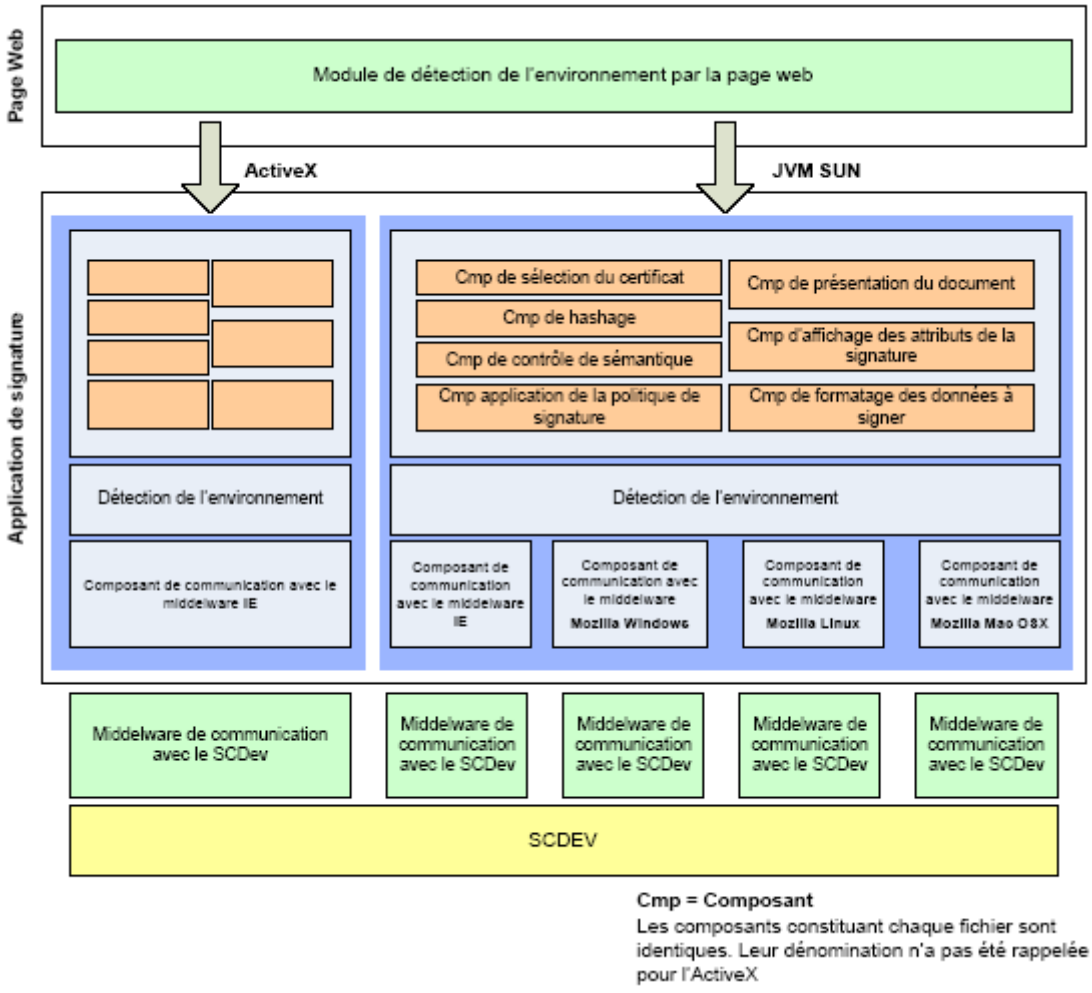
AdSignerWeb est composé de deux fichiers:

- un ActiveX (fichier .cab) qui s'exécute en environnement Windows et Internet Explorer ;
- une applet Java dédiée à la machine virtuelle Java (JVM) de Sun (fichier .jar) qui s'exécute sous de nombreux types de systèmes d'exploitation et navigateurs à condition que la JVM de Sun soit installée sur la machine hôte.

Ces deux fichiers effectuent les mêmes opérations sur des environnements d'exécution différents. C'est l'application web appelante qui détecte l'environnement et donc détermine à quel élément (fichier) faire appel. Ces deux fichiers sont stockés sur un serveur et chargés sur le poste client lorsque cela est nécessaire (le chargement des fichiers n'a pas été évalué).



La figure ci-dessous présente une vue schématique d'AdSignerWeb et de son architecture interne.



1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

Phase	Description	Acteur	Guide
Spécification	Spécification du produit	Dictao	
Développement	Développement du produit	Dictao	
Tests	Tests et recette	Dictao	
Livraison	Livraison du produit et de sa documentation	Dictao	Procédure de livraison
Intégration	Intégration du produit dans une application web	Développeur de l'application web	Guide d'intégration Procédure de gestion d'anomalie
Installation sur le serveur	Installation sur le serveur web du produit et de l'application web et administration	Développeur ou administrateur de l'application web	Guide d'administration Procédure de gestion d'anomalie
Utilisation	Téléchargement sur la machine hôte puis signature	Utilisateur final	Guide d'utilisation qui doit être retransmis par l'intégrateur

1.3.3. Périmètre et limites du produit évalué

Le produit évalué comprend les éléments suivants :

- un composant de contrôle de l'invariance de la sémantique du document pour les formats html restreint et texte brut encodé en base 64 ;
- un composant de présentation de documents html et texte brut encodé en base 64 ;
- un composant d'application de la politique de signature ;
- un composant de sélection du certificat ;
- un composant d'affichage des attributs de la signature ;
- un composant de formatage des données à signer au format XML XAdES version 1.1.1 ou 1.2.2 ;
- un composant de hachage (SHA-1 et SHA-256) ;
- un composant de détection d'environnement ;
- un composant de communication avec le dispositif de création de signature incluant une vérification de signature PKCS#1.

Les éléments suivants ne font donc pas partie du périmètre d'évaluation :

- la plateforme hôte composée de la machine hôte, du système d'exploitation, du navigateur Internet ;
- le dispositif de création de signature et son interface de communication ;
- l'application web appelante.

AdSignerWeb a été évalué sur les configurations suivantes :

Sur ordinateur personnel (PC) :

	Internet Explorer v6.0 SP2 JRE v1.5.0_06	Mozilla v1.7.12 JRE v1.5.0_06	Firefox v1.5 JRE v1.5.0_06
Windows XP	❑ Module ActiveX ❑ Module Java Sun	❑ Module Java Sun	❑ Module Java Sun
Windows Server 2003	❑ Module ActiveX		
Fedora Core 4 (Linux 2.6.12)		❑ Module Java Sun	❑ Module Java Sun

Les dispositifs de création de signature utilisés sont soit celui du navigateur soit la carte à puce Cyberflex Access e-gate 32K USB de Axalto (sur environnement Windows XP / Internet Explorer).

Sur MAC :

	Mozilla v1.7.12 JRE v1.3.1	Firefox v1.5 JRE v1.4.2
MAC OS X (10.3)	❑ Module Java Sun	❑ Module Java Sun

Le dispositif de création de signature utilisé est celui du navigateur.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et aux interprétations suivantes :

- RI # 86 – Role of Sponsor ;
- RI # 137 – Rules governing binding should be specifiable ;
- RI # 146 – C&P elements include characteristics ;
- RI # 192 – Sequencing of sub-activities ;
- RI # 220 – FCS_CKM/COP dependency on FDP_ITC.1 ;
- RI # 227 – CC Part2 F.12 user notes ;
- RI # 228 – Inconsistency between FDP_ITC and FDP_ETC ;
- RI # 232 – FDP_ROL statement ;
- RI # 243 – Must Test Setup And Cleanup Code Run Unprivileged?.

2.2. Commanditaire

Dictao

42 avenue de la Grande Armée
75017 Paris

www.dictao.com

2.3. Centre d'évaluation

Oppida

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

Téléphone : +33 (0)1 30 14 19 00

Adresse électronique : cesti@oppida.fr

2.4. Rapport technique d'évaluation

L'évaluation s'est déroulée du 13 avril 2005 au 25 avril 2006.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.5. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation. Cette cible de sécurité est conforme au profil de protection « Application de création de signature électronique » [PP].

La cible de sécurité contient une exigence fonctionnelle de sécurité explicitement énoncée FDP_MRU.1 Mandatory rules.

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite

2.6. Evaluation du produit

2.6.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL3[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL3	Methodically tested and checked
+ ADV_LLD.1[2]	Descriptive low-level design
+ ADV_IMP.1[2]	Subset of the implementation of the TSF
+ ALC_FLR.3	Systematic flaw remediation
+ ALC_TAT.1[2]	Well-defined development tools
+ AVA_VLA.2	Independent vulnerability analysis

2.6.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

Dictao

42 avenue de la Grande Armée
75017 Paris

www.dictao.com

[1] Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].
[2] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

Les mesures de sécurité analysées par l'évaluateur permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation lors du développement.

L'évaluateur a analysé le plan de gestion de configuration fourni par le développeur qui précise l'utilisation du système de gestion de configuration. Le système permet de maintenir notamment la liste de configuration [CONF] qui identifie tous les éléments gérés par le système.

L'évaluateur a également vérifié que :

- le produit évalué est identifié de façon unique ;
- cette identification est indiquée sur le produit ;
- les éléments constitutifs du produit évalué sont identifiés de façon unique ;
- les éléments constitutifs du produit évalué sont gérés par un système de gestion de configuration ;
- le système garantit que seules des modifications autorisées sont appliquées au éléments constitutifs.

Des procédures de correction d'anomalies [FLR] décrivent la manière dont toute anomalie découverte sera suivie et corrigée, ainsi que la diffusion des informations et corrections relatives à ces anomalies, tant que le produit est maintenu par le développeur. Ces procédures ont été évaluées, bien que le respect de ces procédures ne puisse pas être déterminé au moment de l'évaluation. Les utilisateurs considérés dans le cadre du composant ALC_FLR.3 correspondent aux intégrateurs et administrateurs.

La vérification de l'application des procédures analysées a été effectuée lors d'une visite du site de développement, avenue de la Grande Armée, à Paris. (cf Annexe 1)

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_CAP.3	Authorisation controls	Réussite
ACM_SCP.1	TOE CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.1	Identification of security measures	Réussite
ALC_FLR.3	Systematic flaw remediation	Réussite
ALC_TAT.1[1]	Well-defined development tools	Réussite

2.6.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP), conception de haut-niveau (HLD), conception de bas-niveau (LLD)[1], implémentation (IMP)[1].

[1] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS.

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :
- Cryptographic operation (FCS_COP.1) ;
- Export of user data with security attributes (FDP_ETC.2) ;
- Subset information flow control (FDP_IFC.1) ;
- Simple security attributes (FDP_IFF.1) ;
- Import of user data without security attributes (FDP_ITC.1) ;
- Import of user data with security attributes (FDP_ITC.2) ;
- Advanced rollback (FDP_ROL.2) ;
- User identification before any action (FIA_UID.2) ;
- Management of security attributes (FMT_MSA.1) ;
- Static attribute initialisation (FMT_MSA.3) ;
- Management of TOE security functions data (FMT_MTD.1) ;
- Specification of management functions (FMT_SMF.1) ;
- Security management roles (FMT_SMR.1) ;
- Inter-TSF basic TSF data consistency (FPT_TDC.1).

Une exigence fonctionnelle supplémentaire a été définie:
- FDP_MRU.1 Mandatory rules.

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_FSP.1	Informal functional specification	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1[1]	Descriptive low-level design	Réussite
ADV_IMP.1[1]	Subset of the implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.6.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du produit entre le développeur et l'intégrateur du produit.

L'installation du produit correspond à la phase d'intégration dans une application web et d'installation sur un serveur web. Les procédures analysées [INSTALL] permettent d'obtenir la configuration évaluée du produit.

Pour les tâches d'évaluation liées aux procédures de livraison [DEL] et d'installation [INSTALL], les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		**Verdicts**
ADO_DEL.1	Delivery procedures	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

[1] Appliqué à la partie de la cible d'évaluation répondant aux exigences fonctionnelles de la classe FCS

2.6.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les développeurs de l'application web et les administrateurs de celle-ci et comme utilisateurs les signataires.
L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		**Verdicts**
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.6.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.
L'évaluateur a réalisé ses tests fonctionnels indépendants sur les plates-formes indiquées au paragraphe 1.3.3 page 9.

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		**Verdicts**
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.6.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [INSTALL] [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Aucune fonction n'a fait l'objet d'une estimation du niveau de résistance intrinsèque.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests sur les plates-formes indiquées au paragraphe 1.3.3 page 9.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de niveau élémentaire.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.1	Examination of guidance	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.2	Independent vulnerability analysis	Réussite

2.6.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques (listés dans la cible de sécurité [ST]) a été analysée par la DCSSI. Les mécanismes analysés atteignent le niveau de robustesse standard tel que défini dans le référentiel cryptographique de la DCSSI [CRY].

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (Art. 8 du décret 2002-535)

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation résumés ci-dessous et suivre les recommandations se trouvant dans les guides fournis [INSTALL] [GUIDES] :

- la machine hôte sur laquelle le produit s'exécute doit être non hostile ;
- le dispositif de création de signature électronique doit authentifier le signataire et générer la signature correspondant au certificat sélectionné ;
- l'ensemble des composants logiciels et/ou matériels assurant l'interface entre le produit et le dispositif de création de signature électronique doit garantir l'intégrité et l'exclusivité de la communication ;
- le signataire doit être présent entre l'instant où il manifeste son intention de signer et celui où il entre les données d'authentification permettant d'activer la clé de signature ;
- les administrateurs de l'application web appelante doivent s'assurer de l'authenticité des politiques de signature avant qu'elles ne soient utilisées par le produit ;
- le développeur de l'application web appelante intégrant le produit et son administrateur sont de confiance, formés à l'utilisation du produit et disposent des moyens nécessaires à la réalisation de leur activité ;
- l'environnement du produit doit fournir à l'application web appelante et/ou à son administrateur les moyens de contrôler l'intégrité des services et des paramètres du produit ;
- la communication entre la machine hôte sur laquelle s'exécute le produit et le serveur depuis lequel sont chargés l'application web appelante et le produit doit garantir la protection en intégrité des paramètres transmis au produit ;
- le serveur sur lequel sont stockés le produit et l'application web appelante doit être protégé de manière à garantir leur intégrité.

3.3. Reconnaissance européenne (SOG-IS)

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

3.4. Reconnaissance internationale (CC RA)

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

Annexe 1. Visite du site de développement de la société Dictao

Le site au 42 avenue de la Grande Armée de la société Dictao situé à Paris, a fait l'objet d'une visite par l'évaluateur le 17 février 2006 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le produit AdSignerWeb v3.1.800.

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ACM_CAP.3 ;
- ALC_DVS.1 ;
- ADO_DEL.1;
- ALC_FLR.3.

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 2. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 3. Références documentaires du produit évalué

[PP]	• Profil de protection « Application de création de signature électronique» Réf. : PP-ACSE version 1.0
[CONF]	• Liste de configuration Réf. : dictao_adosi_anx09 version 7.0 du 20/04/2006
[GUIDES]	• Module de signature client AdSignerWeb version 3.1 - Guide d'administration Réf. : dictao_adosi_gu04 version 5.0 du 18/03/2006 • Module de signature client AdSignerWeb version 3.1 - Guide d'utilisation Réf. : dictao_adosi_gu02 version 3.0 du 07/02/2006
[INSTALL]	• Module de signature client AdSignerWeb version 3.1- Guide d'intégration Réf. : dictao_adosi_gu01 version 4.5
[DEL]	• Module de signature client AdSignerWeb - Procédure de livraison Réf. : dictao_adosi_gu03 version 6.0 du 09/03/2006
[FLR]	• Procédure de Maintien en Condition Opérationnelle Réf. : dictao_smq_mco_prc01 version 2.0 du 26/01/2006
[RTE]	• OPPIDA/CESTI/ADOSI/RTE/1.1
[ST]	• Cible de sécurité - Module de signature client AdSignerWeb Réf. : Dictao_ADOSI_CibleDeSecurite.doc version 5.0 • Cible de sécurité - Lite - Module de signature client AdSignerWeb Réf. : Dictao_ADOSI_CibleDeSecurite_Lite du 18/04/2006
[Visite]	• Rapport de visite d’audit Réf. : OPPIDA/CESTI/ADOSI/DOC.001/2.0

Annexe 4. 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, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[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 2.0, April 1999, Management Committee of Agreement Group.
[CRY]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.02 du 19/11/04.

Toute correspondance relative à ce rapport doit être adressée au :

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

certification.dcssi@sgdn.pm.gouv.fr