



PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de maintenance DCSSI-2006/06-M01

AdSignerWeb v3.1.801

Certificat de référence : DCSSI-2006/06

Paris, le 13 août 2009

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

Le contre-amiral Michel Benedittini,
directeur général adjoint
[ORIGINAL SIGNE]



Références

- a) [MAI] Procédure MAI/P/01 Continuité de l'assurance.
- b) [ST] Cible de sécurité – Module de signature client AdSignerWeb, référence : Dictao_ADOSI_CibleDeSecurite.doc, version 5.0 du 18/04/2006, DICTAO.
- c) [ST-Lite] Cible de sécurité – Lite – Module de signature client AdSignerWeb, référence : Dictao_ADOSI_CibleDeSecurite_Lite, version 5.0-Lite du 18/04/2006, DICTAO.
- d) [CER] Rapport de certification 2006/06 – AdSignerWeb v3.1.800, du 28 avril 2006, SGDN/DCSSI.
- e) [IAR] Rapport d'analyse d'impact AdSignerWeb, référence : dictao_adosi_iar01, version 1.4 du 19 juin 2009, DICTAO.
- f) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 2.0, April 1999, Management Committee of Agreement Group.
- g) [CCRA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.

Identification du produit maintenu

Le produit maintenu est le logiciel AdSignerWeb version 3.1.801 développé par la société Dictao.

Description des évolutions

Les modifications du produit AdSignerWeb consistent en des améliorations et des corrections de bugs dans la partie Applet et dans la partie ActiveX :

- modification de l'affichage de la politique de signature pour qu'elle apparaisse dans une nouvelle page Web ;
- correction d'un problème d'affichage de données à signer lié à une fonction ne tolérant pas des chaînes de caractères trop grandes (supérieures à 250 Ko) ;
- prise en compte du navigateur *Microsoft*® *Internet Explorer 7* dans l'environnement logiciel ;
- suppression du code PIN du cache, dans le cas de la JVM Sun, afin que le middleware le demande à chaque signature ;
- modification du filtrage des certificats au niveau du filtrage des clés (*keyUsage*) afin d'accepter des certificats qui n'ont que la « Non Répudiation » ;
- gestion de l'erreur générée dans le cas où l'utilisateur refuse de donner le code PIN au middleware ;
- correction d'un problème de décodage de la clé publique encodée en ASN1 dans le cas de clés de longueur 720 bits.

De plus, la société a changé de locaux. Les nouveaux locaux se situent à l'adresse suivante :

Dictao

152 avenue de Malakoff
75116 Paris
France

Ce déménagement a impliqué des évolutions dans le système d'information et l'environnement de développement de Dictao, ainsi que sur les procédures de support aux clients.

Fournitures impactées

Les fournitures impactées sont les suivantes :

- la cible de sécurité ;
- la liste de configuration ;
- le guide d'intégration ;
- la description du système d'information de Dictao ;
- la procédure de gestion des failles ;
- la procédure de maintenance corrective ;
- la procédure de test ;
- le plan de test ;
- le document de couverture de test ;
- le code source du produit.

Les fournitures référencées dans le rapport de certification [CER] et impactées par les évolutions décrites plus haut ont été mises à jour. La liste ci-dessous précise la nouvelle version de ces documents :

[ST]	Cible de sécurité – Module de signature client AdSignerWeb, version 5.32 du 30/01/2008, Référence : Dictao_ADOSI_CibleDeSecurite.doc, DICTAO.
[CONF]	Liste de configuration, version 8.01 du 30 janvier 2008, Référence : dictao_adosi_anx09, DICTAO.
[INSTALL]	Module de signature client AdSignerWeb version 3.1 – Guide d'intégration, version 5.01 du 30 janvier 2008, Référence : dictao_adosi_gu01, DICTAO.
[FLR]	Procedure de maintenance corrective, version 2.0 du 16/03/2007, Référence : dictao_smq_mco_prc02_maintenancorrective, DICTAO.

Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur**.

Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée, à la date de certification.

Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une ré-évaluation ou une surveillance de la nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Reconnaissance du certificat

Reconnaissance européenne (SOG-IS)

Le certificat initial a été émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance 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 :



Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², 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 :



Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, ref. CCIMB-2004-02-009, version 1.0, February 2004 ».

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

² Les pays signataires de l'accord 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.