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 maintenance ANSSI-CC-2010/26-M01

Applet ID One Classic v1.01.1 en configuration CNS, Classic ou CIE masquée sur Cosmo v7.0-a Standard et Basic sur composants Atmel

Certificat de référence : ANSSI-CC-2010/26

Paris, le 18 juillet 2011

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Références

[MAI] : Procédure MAI/P/01 Continuité de l'assurance ;
[ST] : IDOne ClassIC Card - SECURITY TARGET 3; reference FQR 1104711 / Edition 3 ;
[CER] : Rapport de certification ANSSI-CC-2010/26 du 20 05 2011 ;
[ANA-CRY] : Evaluation report - Project: ERATO – cryptographic rating; reference ERA_ER, version 1; Thales-CEACI ;
[SOG-IS] : « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee;
[CC RA] : Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000 ;
[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.

Identification du produit maintenu

Le produit maintenu est l'applet, d'Oberthur Technologies, ID One Classic v1.01.1 en configuration CNS, Classic ou CIE masquée sur la plateforme, d'Oberthur Technologies, Cosmo v7.0-a Standard et Basic sur composants Atmel Secure Microcontroller Solutions.

Comme indiqué dans [CER], la partie applet du produit est identifiable par la commande GET DATA avec le tag "DF65" :

La valeur retournée doit être "DF65 04 **1011 1D 00**".
La valeur **1011** correspond à la version de l'application ID One CIE, soit 1.01.1 ici
La valeur **1D** indique une configuration CIE (elle serait de 06 pour une configuration ID One Classic et de 19 pour CNS) ;
La valeur **00** indique que le CHV manager n'est pas utilisé.

Description des évolutions

Le produit n'a pas évolué.

L'objet de ce rapport de maintenance est de prendre en compte la cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF-CRY] qui a été faite pour ce produit. Cette cotation a été réalisée par le CESTI ayant effectué l'évaluation du produit initial. Cette cotation est l'une des conditions nécessaires pour permettre à l'ANSSI de délivrer un certificat de conformité aux exigences de l'article 3.I du décret 2001-272 du 30 mars 2001 relatif à la signature électronique, pour ce produit en tant que dispositif sécurisé de création de signature électronique.

Les résultats obtenus à l'issue de la cotation ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu aux conclusions suivantes :

- les mécanismes sont reconnus conformes au référentiel technique [REF-CRY] avec les recommandations suivantes :
    - le logiciel distant doit contrôler la longueur des données transmises à la carte en entrée de la commande de signature PSO CDS, cette longueur doit être cohérente avec la longueur du hash transmis ;
    - la taille du module RSA doit être de 2048 bits (maximum supporté par le produit) et son utilisation ne doit pas dépasser l'année 2020.

Fournitures impactées

Aucune livraison précédente n'est impactée par les modifications décrites ci-dessus. Toutefois, le rapport d'analyse [ANA-CRY] mentionne les guides à mettre à jour si une évolution du produit est envisagée.

Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact **mineur** du point de vu du référentiel des Critères Communs version 3.1 qui a été utilisé pour la certification du produit initial. Les évolutions décrites plus haut découlent uniquement des exigences du référentiel [REF-CRY].

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

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 ».

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 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 :

Reconnaissance internationale critères communs (CCRA)

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

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

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 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.