



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-PP-2010/03-M01**

**« Java Card Protection Profile – Open
Configuration »
(version 3.0 du 18 mai 2012)**

Certificat de référence : ANSSI-CC-PP-2010/03

Paris, le 29 mai 2012

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

Patrick Pailloux
[ORIGINAL SIGNE]



Références

- a) [MAI] Procédure MAI/P/01 Continuité de l'assurance.
- b) [CER] Rapport de certification ANSSI-CC-PP-2010/03 du profil de protection « Java Card™ System Open Configuration, version 2.6 » du 25 juin 2010.
- c) [IAR] « Java Card System Protection Profile – Open Configuration – Impact Analysis Report », référence CP-2012-RT-214, version 1.0 du 18 mai 2012.
- d) [NOTE.10] « Note d'application - Certification d'applications sur “plateformes ouvertes cloisonnées” », référence ANSSI-CC-NOTE/10.0, voir www.ssi.gouv.fr.
- e) [SOG-IS] « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, du 8 janvier 2010.
- f) [CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, mai 2000.

Identification du produit maintenu

Le profil de protection maintenu [PP] est le profil de protection pour « Java Card™ System Open Configuration » rédigé par Trusted Labs SAS pour le compte de Oracle Inc. qui avait été certifié sous la référence b.

Description des évolutions

La mise à jour de ce PP rend optionnelle l'utilisation du RMI (*Remote Method Invocation*) et prend en compte les conditions d'évaluation de produits ouverts établies par la note [NOTE10].

Les modifications suivantes ont également été réalisées :

- Sun Microsystems est remplacé par Oracle Inc ;
- la référence du JCBV (*JavaCard Byte Code verifier*) a été mise à jour ;
- des corrections typographiques ont été apportées au profil de protection.

Fournitures impactées

[PP]	Java Card System Protection Profile Open Configuration, version 3.0, 18 may 2012.
------	---

Conclusions

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

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'accord¹, 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].

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 :



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.

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.