



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-2017/34-M01**

**ChipDoc P60 on JCOP 3 SECID P60 (OSA)
ICAO BAC avec AA et CA masqué sur
composant P6022J VB
(version 7b1101 et version 7b0301)**

Certificat de référence : ANSSI-CC-2017/34

Paris, le 9 octobre 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]



1. Références

[CER]	ChipDoc P60 on PCOP 3 SECID P60 (OSA) ICAO BAC avec AA et CA masqué sur le composant P6022J VB, 7 juin 2017, ANSSI-CC-2017/34.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	ChipDoc on OS-A PL5 – Impact Analysis Report for ChipDoc OS-A Platform Maintenance, 6 septembre 2017, référence : IAR – ChipDoc OS-A PL2->PL5.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CCRA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.

2. Identification du produit maintenu

Le produit « ChipDoc P60 on JCOP 3 SECID P60 (OSA) ICAO BAC avec AA et CA masqué sur composant P6022J VB, version v7b1 » a été initialement certifié sous la référence ANSSI-CC-2017/34 (référence [CER]).

Le produit objet de la présente maintenance est « ChipDoc P60 on JCOP 3 SECID P60 (OSA) ICAO BAC avec AA et CA masqué sur composant P6022J VB, version v7b1101 et version v7b0301 » développé par la société *NXP SEMICONDUCTORS GMBH*.

La version maintenue du produit est identifiable par les éléments suivants :

Commande	Donnée d'identification attendue	Interprétation des données
Get Data applet version 00 CB 00 03 00	00 07 11 01 ou 00 07 03 01	Applet version v7b1101 ou version v7b0301
Get Data IDENTIFY (platform) 80 CA 00 FE 02 DF 28 00	FE 39 FE 37 DF28 34	Données propriétaires et longueur des données
	01 0C 80 00 00 00 DC 0A 81 54 56 79 F4 50	Tag <i>EEPROM ID</i> Longueur <i>EEPROM ID</i> <i>EEPROM ID</i>
	02 08 02 00 00 00 00 00 00 00 ou 05 00 00 00 00 00 00 00	Tag <i>patch ID</i> Longueur <i>patch ID</i> <i>Patch ID</i>
	03 10 4A 78 48 79 79 79 30 30 30 35 38 36 30 34 30 30 (JxHyyy0005860400)	Tag <i>platform build ID</i> Longueur <i>platform build ID</i> <i>Platform build ID</i>
	04 08 6F6D AFA8 6B67 E7F6	Tag <i>custom mask ID</i> Longueur <i>custom mask ID</i> <i>Custom mask ID</i>
INSTALL [for load] 80 E6 02 00 0A 05 01 02 03 01 05 00 00 00 00 00	6D 00	Erreur signalant que l'instruction est invalide (la plate-forme est déjà fermée)

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- la plateforme est passée de la version de patch PL2 à la version de patch PL5 ;
- l'application est passée de la version v7b1 à la version v7b1101 ou v7b0301 pour corriger un bug dans le calcul de hash d'une fonction en dehors du périmètre d'évaluation ;
- le code source a été mis à jour pour avoir la possibilité d'avoir plusieurs systèmes de gestion de fichiers.

4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	ChipDoc v7b1 applet in ICAO configuration - Preparation and Operation Manual, revision 1.4, 16 juin 2017	[R-M01]
[ST]	Cibles de sécurité de référence: - ChipDoc P60 on JCOP 3 SECID P60 (OSA) ICAO BAC – Security Target JCOP 3 EMVP40 Security Target rev. 1.0 / 4 septembre 2017 ; Version publique : - ChipDoc P60 on JCOP 3 SECID P60 (OSA) ICAO BAC – Security Target Lite JCOP 3 EMVP40 Security Target rev. 1.0 / 28 septembre 2017.	[R-M01] [R-M01]
[CONF]	2017_09_19_CIL_CD_v7bxx01_ICAO_on_OSA_PL2_5.xlsx, 19 septembre 2017	[R-M01]

5. 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.

6. 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 réévaluation ou une surveillance de cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

7. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

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 CCRA [CCRA].

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 EAL 2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

² Les pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.



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@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.