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

Correctif du rapport de certification ANSSI-CC-2013/42

Plateforme jTOP INFv#46 masquée sur composants Infineon SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM avec fonctionnalités MRTD

Certificat de référence : ANSSI-CC-2013/42

Paris, le 28 juillet 2015

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Rapport de certification ANSSI-CC-2013/42 émis par l'ANSSI le 27 juin 2013.
[ST-CER]	Cible de sécurité : – JTOP INF#v46 (SLJ 52 Gxx yyy zL) – Security Target for MRTD, 24 avril 2013, référence CP-2011-RT-751-v.46-0.97, version 0.97 ; – Java Card Open Platform – Security Target-LITE, 18 mai 2013, référence PU-2011-RT-751-v46-1.0-LITE, version 1.0.
[R-M01]	Rapport de maintenance ANSSI-CC-2013/42-M01 émis le 10 avril 2015.
[ST-M01]	Cibles de sécurité : – jTOP INFv#46 (SLJ 52 Gxx yyy zL) – Security Target for MRTD, 12 décembre 2014, référence CP-2011-RT-484-46, version 1.1 ; – Java Card Open Platform for MRTD Security Target LITE, 02 avril 2015, référence PU-2011-RT-484-46-LITE, version 1.1.
[REF]	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 (RGS_B_1), voir www.ssi.gouv.fr.
[X931]	ANSI X9.31 Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), 1998.

2. Identification du produit

Le produit « Plateforme jTOP INFv#46 masquée sur composants Infineon SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM avec fonctionnalités MRTD » a été initialement certifié sous la référence ANSSI-CC-2013/55 (référence [CER]).

Il a déjà fait l'objet d'une maintenance sous la référence ANSSI-CC-2013/42-M01 (référence [R-M01]).

3. Correctif du rapport

Le correctif porte sur la substitution de la phrase de la section **2.4. Analyse du générateur d'aléas** du rapport de certification [CER] :

« Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique » ;

par la phrase :

« Par ailleurs, la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique suivant l'implémentation du standard [X931] ».

4. Correctif des fournitures

Les cibles de sécurité [ST-CER] et [ST-M01] sont substituées par les cibles de sécurité suivantes qui ne mentionnent plus le référentiel [REF] :

- cible de sécurité de référence : jTOP INFv#46 (SLJ 52 Gxx yyy zL) – Security Target for MRTD, 20 juillet 2015, référence CP-2011-RT-484-46, version 1.2 ;
- cible de sécurité publique : Java Card Open Platform for MRTD Security Target-LITE, 20 juillet 2015, référence PU-2011-RT-484-46-LITE, version 1.2.

De plus, les documents suivants ont été mis à jour afin d'identifier la nouvelle version de la cible de sécurité de référence :

- Liste de configuration : Configuration ITEMS, product jTop INFv#46.03, 20 juillet 2015, référence ARGES_CONFIGURATION_ITEMS_20150720.TXT ;
- jTOP INFv#46 (SLJ 52 Gxx yyy zL) - Operational User Guidance, 20 juillet 2015, référence CP-2011-RT-732-46, version 1.5 ;
- jTOP INFv#46 (SLJ 52 Gxx yyy zL) – Preparative Procedures, 20 juillet 2015, référence CP-2011-RT-731-46, version 1.2.