



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-2011/45-M01

**SafeNet eToken (Smartcard or USB token)
version 9.1.2 - Athena IDProtect/OS755 Java
Card on Inside Secure AT90SC25672RCT-USB
Microcontroller embedding IDSign applet**

Certificat de référence : ANSSI-CC-2011/45

Paris, le 16 juillet 2013

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

[Original signé]

Patrick Pailloux



1. Références

- [MAI] Procédure MAI/P/01 Continuité de l'assurance ;
- [ST] SafeNet eToken - Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB embedding IDSign applet – Security Target, 19 juillet 2011, version 2.1 ;
- [ST_Lite] SafeNet eToken - Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB embedding IDSign applet – Security Target Lite, 19 juillet 2011, version 2.1 ;
- [CER] SafeNet eToken version 9.1.2 - Athena IDProtect/OS755 Java Card on Inside Secure AT90SC25672RCT-USB Microcontroller embedding IDSign applet, 22 Septembre 2011, référence ANSSI-CC-2011/45 ;
- [IAR] SafeNet eToken - Common Criteria EAL4+ - Addition of Fulfillment Site - Impact Analysis Report, 6 Mars 2013, référence 002-010838-001 révision A ;
- [SOG-IS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, Janvier 2010, Management Committee ;
- [CC RA] Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, Mai 2000.

2. Identification du produit maintenu

Le produit maintenu est la carte ou token USB « SafeNet eToken version 9.1.2 - Athena IDProtect/OS755 Java Card on Inside Secure AT90SC25672RCT-USB Microcontroller embedding IDSign applet », développé par les sociétés Athena Smartcard Solutions et Inside Secure.

Ce produit a été initialement certifié sous la référence ANSSI-CC-2011/45 (référence [CER]).

3. Description des évolutions

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

- le site de SafeNet à Rotterdam (Pays-Bas) a été ajouté en tant que site de chargement de patch ;
- le site d'Athena à Edimbourg (Ecosse), où a été développé l'OS, a été fermé et remplacé par un nouveau site à Livingston (Ecosse).

4. Fournitures impactées

Suite à cette maintenance, les fournitures suivantes ont été mises à jour depuis le certificat initial :

[CONF]	Listes de configuration du produit: <ul style="list-style-type: none">- Borealis_Extended - Documents Configuration List, Version 3.1, 30 Mai 2013 ;- Configuration List of Evidence Provided to Thales - Common Criteria Lab for Rotterdam Site Certification, 6 Juin 2013, référence 002-010845-001, révision B.
--------	---

[ST]	<p>Cible de sécurité de référence:</p> <ul style="list-style-type: none">- SafeNet eToken 9.1.2 - Athena IDProtect/OS755 Java Card on Inside Secure AT90SC25672RCT-USB Microcontroller embedding IDSign Digital Signature applet - Security Target, 15 Mai 2013, référence ST-IDDS-01, version 3.2. <p>Cible de sécurité publique:</p> <ul style="list-style-type: none">- SafeNet eToken 9.1.2 - Athena IDProtect/OS755 Java Card on Inside Secure AT90SC25672RCT-USB Microcontroller embedding IDSign Digital Signature applet - Public Security Target, 15 Mai 2013, référence SafeNet eToken 9.1.2 – Public Security Target, version 3.2.
------	---

5. Conclusions

Les évolutions listées au chapitre 3 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.

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 la 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, juin 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 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.