



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-2018/32-M01**

**Plateforme ouverte Java Card MultiApp V4.1  
en configuration ouverte masquée sur le  
composant S3FT9MH  
Release Date 28/09/2018**

**Certificat de référence : ANSSI-CC-2018/32**

*Paris, le 4 avril 2019*

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

Guillaume POUPARD  
[ORIGINAL SIGNE]



## 1. Références

[CER]	Plateforme ouverte JavaCard MultiApp V4.1 en configuration ouverte masquée sur le composant S3FT9MH, 3 août 2018, ANSSI-CC-2018/32.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[IAR]	Impact analysis report – MultiApp V4.1 JavaCard Platform, version 1.0, 22 novembre 2018.
[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 « Plateforme ouverte Java Card MultiApp V4.1 en configuration ouverte masquée sur le composant S3FT9MH » a été initialement certifié sous la référence ANSSI-CC-2018/32 (référence [CER]).

Le produit objet de la présente maintenance est la « Plateforme ouverte Java Card MultiApp V4.1 en configuration ouverte masquée sur le composant S3FT9MH, OS Release Date 28/09/2018 » développée par la société *GEMALTO* et par *SAMSUNG ELECTRONICS CO.*.

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

Eléments de configuration	
Nom de la TOE	MultiApp V4.1 Platform
Référence interne de la TOE	MULTIAPPV41_CODE_EIR18_LBL01 Checkpoint 1.57
Données de production du produit	'42 50 16 11 19 81 82 71 04 01' avec '42 50' = <i>IC Fabricator</i> (Samsung) '16 11' = <i>IC Type</i> (S3FT9MH) '19 81' = <i>OS ID</i> (identifiant de la plateforme) '82 71' = <i>OS Release Date</i> (28/09/2018) '04 01' = <i>OS Release Level</i> (v4.1)

## 3. Description des évolutions

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

- amélioration fonctionnelle des protocoles sans contact type A & B ;
- correction fonctionnelle de la fonction HMAC.

## 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]	MultiApp V4.1- AGD_PRE document – Javacard Platform, référence D1424307, version 1.1 du 04/03/2019, <i>GEMALTO</i> .	[R-M01]
	MultiApp V4.1 : AGD_OPE document – Javacard Platform, référence D1424308, version 1.5 du 16/03/2018, <i>GEMALTO</i> .	[CER]
	Global Dispatcher Personalization Applet – User Guide, référence D1390286D du 30/05/2017, <i>GEMALTO</i> .	[CER]
	Rules for applications on Multiapp certified product, référence D1390963, version 1.2 de novembre 2017, <i>GEMALTO</i> .	[CER]
	Guidance for secure application development on Multiapp platforms, référence : D1390326, version A01 de février 2016, <i>GEMALTO</i> .	[CER]
	Verification process of Gemalto non sensitive applet, référence D1390670, version A01 de février 2016, <i>GEMALTO</i> .	[CER]
	Verification process of Third Party non sensitive applet, référence D1390671, version A01 de février 2016, <i>GEMALTO</i> .	[CER]
[ST]	<p>Cibles de sécurité de référence:</p> <ul style="list-style-type: none"> <li>- MultiApp V4.1 : JCS Security Target, référence D1417544, version 1.13 du 4 mars 2019, <i>GEMALTO</i>.</li> </ul> <p>Version publique :</p> <ul style="list-style-type: none"> <li>- MultiApp V4.1 : JCS Security Target Lite, référence D1417544, version 1.13p du 4 mars 2019, <i>GEMALTO</i>.</li> </ul>	[R-M01]
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>- MultiApp V4.1 : ALC LIS document – Javacard platform, référence D1449828, version 1.10 du 26 février 2019, <i>GEMALTO</i> ;</li> <li>- LIS_MAV41_PLT_Code_1.57, version 1.57, <i>GEMALTO</i>.</li> </ul>	[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.

Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

## 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].

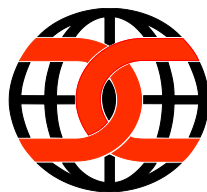
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord<sup>1</sup>, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et 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 signataires<sup>2</sup>, des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC\_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



---

<sup>1</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.org](http://www.sogis.org).

<sup>2</sup> Les pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://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](mailto:certification@ssi.gouv.fr)

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