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 certification ANSSI-CC-2016/60

DragonFly v4.0 sur composant SLE97CNFX1M50PE

Identification Hardware 412691
Card Manager GOP Ref V21.06.01

Paris, le 6 octobre 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

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

Référence du rapport de certification

ANSSI-CC-2016/60

Nom du produit

DragonFly v4.0 sur composant SLE97CNFX1M50PE

Référence/version du produit

Version 4.0, Identification Hardware 412691
Card Manager GOP Ref V21.06.01

Conformité à un profil de protection

(U)SIM Java Card Platform Protection Profile - Basic Configuration, version 2.0.2

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 4 augmenté
ALC_DVS.2, AVA_VAN.5

Développeurs

Oberthur Technologies	Infineon Technologies AG
420, rue d'Estienne d'Orves CS 40008, 92 705 Colombes Cedex, France	Am Campeon 1-12, 85579 Neubiberg, Allemagne

Commanditaire

Oberthur Technologies
420 rue d'Estienne d'Orves CS 40008, 92 705 COLOMBES CEDEX, France

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA **SOG-IS**

Le produit est reconnu au niveau EAL4.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la plateforme « DragonFly v4.0 sur composant SLE97CNFX1M50PE » dont l'identification matérielle est « 412691 » et la version du *Card Manager* en Java Card est « GOP Ref V21.06.01 ». Cette plateforme est développée par *OBERTHUR TECHNOLOGIES* et embarquée sur le microcontrôleur SLE97CNFX1M50PE, développé et fabriqué par *INFINEON TECHNOLOGIES AG*.

Le produit est une plateforme (U)SIM Java Card ouverte pouvant être insérée dans un téléphone portable ou tout autre équipement téléphonique. Le produit propose des communications sans contact (conforme au SWP[1]) et avec contact (conforme à l'ISO7816).

Le produit est destiné à héberger et exécuter une ou plusieurs applications (dites « applets » dans la terminologie Java). Ces applets peuvent revêtir un caractère sécuritaire différent (selon qu'elles soient « sensibles » ou « basiques ») et peuvent être chargées et instanciées avant ou après émission du produit. Dans ce second cas, ces opérations peuvent se faire via le réseau d'un opérateur de téléphonie mobile en mode OTA[2], sans manipulation physique du produit par l'utilisateur final.

Dans le cadre de la présente évaluation, la TOE[3] est la plateforme seule. Les logiciels applicatifs ne sont pas inclus dans le périmètre de l'évaluation, mais ont été pris en compte au titre de [OPEN].

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection [PP (U)SIM], en configuration basique, qui définit les besoins des opérateurs de téléphonie mobile et plus généralement des différents acteurs offrant des produits sans contact. Cette conformité est du type « démontrable ». Le profil de protection [PP (U)SIM] est lui-même conforme au profil de protection [PP JCS-O].

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

[1] *Single Wire Protocol* – protocole fil unique.
[2] *Over-The-Air* – par les airs.
[3] *Target Of Evaluation* – cible d'évaluation.

La version certifiée du produit est identifiable par les éléments suivants, détaillés dans la [ST] au chapitre 2.3 « *TOE Reference* » :

Eléments de configuration		Origine
Nom de la TOE	DragonFly v4.0	*OBERTHUR TECHNOLOGIES*
Référence interne de la TOE	USIM V4.0 NFC FlyBuy 4.0 on SLE97CNFX1M50PE	
Identification du *Card Manager*	GOP Ref V21.06.01	
Identification matérielle	412691	
Label PVCS ROM	USIM_V31_DF4_SLE97_REVB_V03	
Données de production	48 30 52 03 82 31 53 17 32 78	
Référence du circuit intégré	SLE97CNFX1M50PE with Mifare-compatible libraries	*INFINEON TECHNOLOGIES AG*

L'identification matérielle (ou code SAAAAR) « **412691 »** peut être lue dans la réponse ATR[1] : 3B 9F 96 80 3F C7 00 80 31 E0 73 FE 21 1F 64 **41 26 91** 00 82 90 00.

L'identification du *Card Manager* « **GOP Ref V21.06.01** » est obtenue, en codage ASCII, en réponse à la commande GET DATA « 80 CA DF 6C » pour *Card Manager Release*[2] : DF 6C 14 **47 4F 50 20 52 65 66 20 56 32 31 2E 30 36 2E 30 31** 2F XX YY 90 00 (X et Y dépendent de la personnalisation).

Les données de production du produit « **48 30 52 03 82 31 53 17 32 78** » correspondent à :
- **48 30** = FAB_ID, identifiant de la fonderie du composant sous-jacent ;
- **52 03** = IC_ID, identifiant du composant sous-jacent ;
- **82 31** = OS_ID, identifiant du système d'exploitation ;
- **53 17** = OS_Release_Date, date d'émission du système d'exploitation ;
- **32 78** = OS_Release_Level, niveau d'émission du système d'exploitation dans les projets du développeur.

Ces données sont obtenues en réponse à la commande GET DATA « 80 CA 9F 7F 2D » pour *Production Life Cycle*[3] : 9F 7F 2A **48 30 52 03 82 31 53 17 32 78**.

Les données de configuration, qui doivent correspondre à la configuration *Mandated DAP*[4], sont obtenues via la commande GET STATUS (voir [ST] et [GUIDES] pour le détail d'utilisation de cette commande). Cette configuration correspond notamment à la présence dans la TOE d'un SD[5] avec des privilèges de vérification de *Mandated DAP*, (voir [GUIDES] pour plus de détails).

La principale différence entre le produit et la TOE (la plateforme) correspond à l'application chargée pré-émission sur cette carte à puce : « MIFARE4Mobile 2.X framework Package ».

Cette application est présente dans la configuration du produit à la disposition de l'évaluateur et est identifiée par les éléments ci-après.

[1] *Answer To Reset* – réponse suite à réinitialisation.
[2] Version du *Card Manager*.
[3] Cycle de vie de production.
[4] DAP obligatoire, où DAP signifie *Data Authentication Pattern.*
[5] *Security Domain* – Domaine de sécurité.

Packages	AID[1].	Version
MIFARE4Mobile 2.X framework Package	A0 00 00 03 96 4D 34 4D 10 07	1.0.7
M4M – Interface - Wallet	A0 00 00 03 96 4D 34 4D 70	2.2.0
M4M – Interface – Parser	A0 00 00 03 96 4D 34 4D 60	1.0.0
M4M – Interface – User Verifier	A0 00 00 03 96 4D 34 4D 40	1.0.0

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont détaillés dans la [ST] au chapitre 2.5.14 « *TOE Security Features* » et au chapitre 8 « *TOE Summary Specification* ». Ils sont résumés ci-après :

- services de sécurité dédiés aux applications :
  - confidentialité et intégrité des clés cryptographiques et des opérations associées ;
  - confidentialité et intégrité des données d'authentification ;
  - confidentialité et intégrité des données d'application entre applications ;
  - intégrité de l'exécution du code applicatif. La JCVM[2] et la propriété d'isolation des applications garantissent l'exécution correcte et sécurisée des applications sensibles, même avec la présence d'application basique sur la TOE,
- services de sécurité dédiés à la gestion de ces applications qui concernent :
  - la délégation de privilèges : le MNO[3], en tant qu'émetteur de la carte (*Card Issuer*), correspond initialement à l'unique entité autorisée à gérer les applications de la carte (chargement, instanciation, suppression) au travers d'un canal de communication sécurisé avec la carte en phase 7 (phase d'utilisation de la carte, voir chapitre 1.2.4). Cependant le MNO peut céder ce privilège à un AP[4] à l'aide de la fonctionnalité *GlobalPlatform* de délégation de cette gestion d'applications ;
  - la vérification de la signature des applications à charger : la signature par une VA[5] (*Mandated* DAP) de chaque application à charger est vérifiée par la carte (par le représentant du VA sur la carte) avant la finalisation du processus de chargement de l'application considérée et de son instanciation ;
  - la gestion de SD : les fournisseurs d'applications disposent de jeux de clés spécifiques et connus d'eux seuls associés à leurs SD. La confidentialité de ces jeux de clés est assurée par l'utilisation des services du CASD[6] pour leur chargement. Ces clés leur permettent de s'authentifier auprès de ces SD et d'établir un canal de confiance entre la TOE et un équipement externe ;
  - les services de sécurité DESFire : protection des données de la librairie et du code DESFire en intégrité et en confidentialité ;
  - la protection du chargement d'applications post-émission (le chargement d'applications s'effectue après la livraison du produit à l'utilisateur final) ;
  - l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

[1] *Application Identifier.*
[2] *Java Card Virtual Machine* - virtuelle machine Java Card.
[3] *Mobile Network Operator* – opérateur mobile.
[4] *Application Provider* - fournisseur d'applications.
[5] *Verification Authority* - autorité de vérification.
[6] *Controlling Authority Security Domain* – domaine de sécurité de l'autorité de direction.

1.2.4. Architecture

La TOE est constituée des éléments suivants :

- des packages *GlobalPlatform*, conformes aux spécifications *GlobalPlatform Card Specification*, version 2.2.1, qui fournissent une interface commune et largement utilisée pour communiquer avec la carte et pour gérer de façon sécurisée les applications ;
- un système Java Card, conforme au [PP JCS-O], qui inclut la JCVM, le JCRE[1], la JCAPI[2]. Il gère et exécute les applications, appelées « applets ». Il fournit également les API pour développer ces applets conformément aux spécifications Java Card, Classic Edition, version 3.0.4 ;
- des fonctionnalités (U)SIM conformes aux spécifications ETSI et 3GPP, qui fournissent des moyens pour interagir spécifiquement avec les applications (U)SIM ;
- des commandes de personnalisation, qui fournissent un ensemble de commandes propriétaires pour la personnalisation ;
- le protocole BIP[3], technologie OTA, qui permet l'échange de données entre une carte (U)SIM d'un téléphone portable et des serveurs distants (remplaçant ainsi la technologie SMS). Cette technologie n'offre pas de service de sécurité ;
- des Mifare APIs : l'application native DESFire, la technologie Mifare Classic, MIFARE4Mobile v2.1 ;
- Cipurse API, qui supporte CIPURSE Server Crypto API révision 2.0. Il n'offre pas de fonction de sécurité dans la présente évaluation ;
- Calypso API qui supporte Calypso révision 3.2 développée par Calypso Network Association ;
- un système d'exploitation qui assure l'interface entre le matériel (composant) et le logiciel (applications) ;
- le composant SLE97CNFX1M50PE (précédemment certifié, voir [CER-IC]).

Le produit inclut une application chargé en pré-émission : « MIFARE4Mobile 2.X framework Package » et aucune application connue chargée en post-émission.
Bien que cette application standard ne soit pas incluse dans le périmètre de l'évaluation, elle a été prise en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, cette application standard a été vérifiée conformément aux contraintes de développements d'applications décrites dans les guides [GUIDE_Sec].

La figure 1 illustre les principaux éléments de la TOE. Les pointillés en rouge indiquent les parties évaluées en tant que TSF[4].

[1] *Java Card Runtime Environment* – environnement d'exécution Java Card.
[2] *Java Card Application Programming Interface* – Interface de programmation d'applications Java Card.
[3] *Bearer Independent Protocol* – protocole indépendant de la porteuse.
[4] *TOE Security Function.*

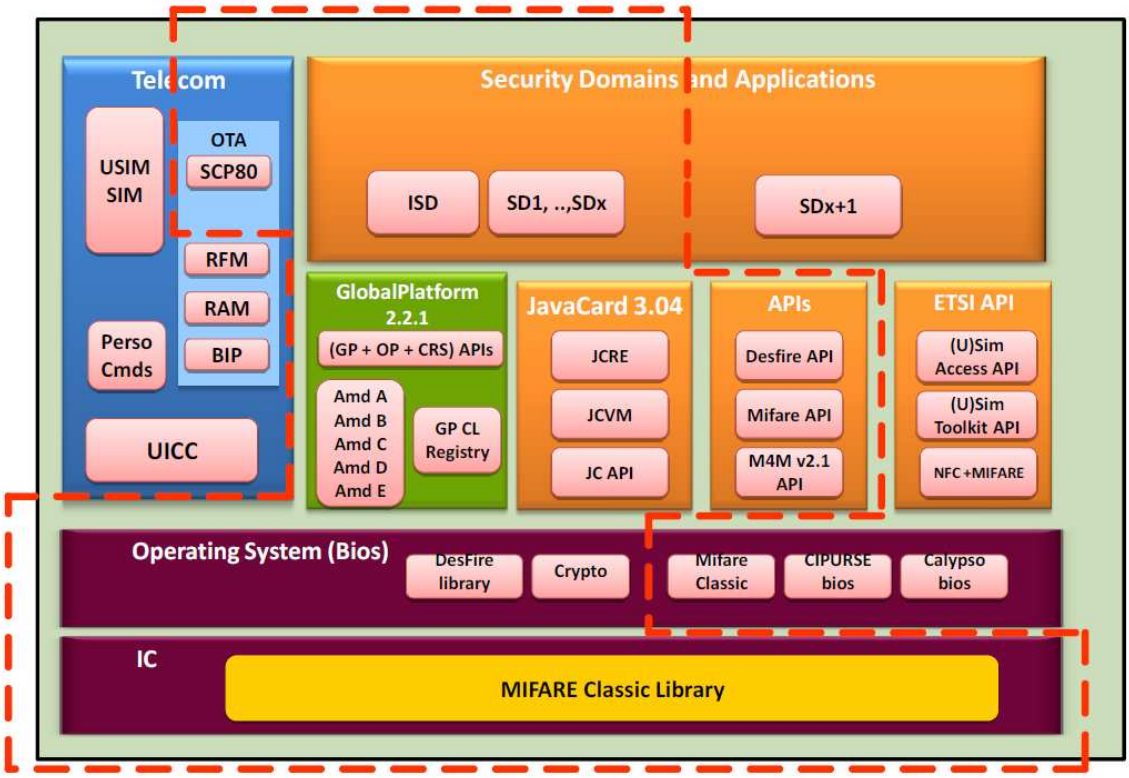

Figure 1 : Architecture de la TOE (*Target of Evaluation*)

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit par la figure 2.

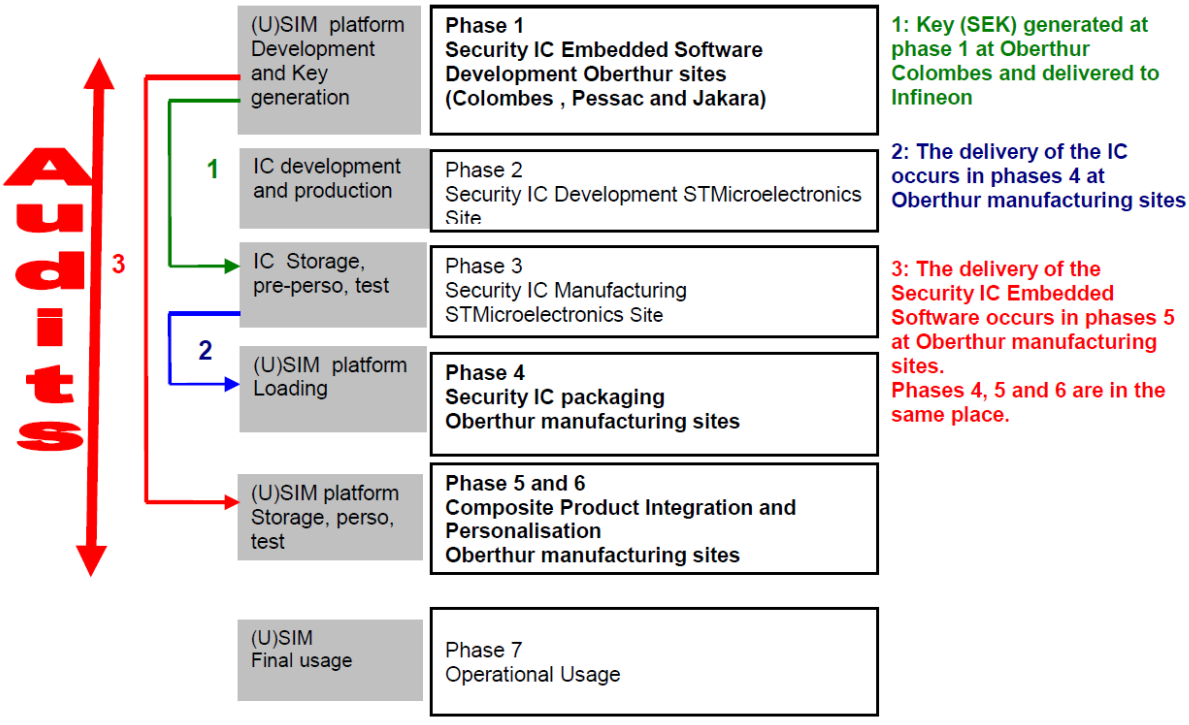

Figure 2 : Cycle de vie du produit

Les phases 1 et 2 correspondent au développement du produit :

- développement du logiciel embarqué : le logiciel dédié au composant (*firmware*), le système d'exploitation, le système Java Card, l'applet (U)SIM, l'applet *Card Manager* et d'autres parties logicielles de la plateforme ;
- développement du composant.

Les phases 3 et 4 correspondent à la fabrication et au conditionnement (*packaging)* du composant.
La phase 5 correspond au chargement du logiciel embarqué (hormis le *firmware* qui est déjà masqué en phase 3) dans le composant.
La phase 6 correspond à la personnalisation du produit.
La phase 7 correspond à la phase opérationnelle du produit.
Les phases 1 à 6 correspondent donc à la construction de la TOE. Elles ont été prises en compte dans la présente évaluation, avec, pour les phases 2 et 3, une réutilisation des résultats de l'évaluation du composant SLE97CNFX1M50PE (voir [CER-IC]). Le point de livraison, ou d'émission de la carte, est en sortie de la phase 6.

Le produit a été développé sur les sites suivants :

Oberthur Technologies – Colombes (pour la phase 1)
420 rue d'Estienne d'Orves, CS 40008
92705 Colombes, France

Oberthur Technologies – Pessac (pour la phase 1)
Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus - Porte 2
33600 Pessac, France

Oberthur Technologies – Jakarta (pour la phase 1)
The Landmark Centre Tower A, 18th floor
Jl. Jend. Sudirman No. 1
Jakarta 12910, Indonésie

Oberthur Technologies –Rabat (pour la phase 1)
OBERTHUR TECHNOLOGIES
Bâtiment 4 – Plateau 202
11, Complexe de Technopolis
11100 Sala Al Jadida, Maroc

Le produit a été conditionné, intégré et personnalisé sur les sites suivants :

Oberthur Technologies – Vitré (pour les phases 4, 5 et 6)
Avenue d'Helmstedt, BP 90308
35503 Vitré Cedex, France

Oberthur Technologies – Shenzen (pour les phases 4, 5 et 6)
4F, Great wall technology building, No 2, KeFa Rd
Science and Technology park, Nanshan district
Shenzhen, 518057, République Populaire de Chine

Les sites de développement et de fabrication du microcontrôleur sont identifiés dans le rapport de certification du composant (voir [CER-IC]).

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit les rôles suivants :

- le fabriquant du composant ;
- l'intégrateur et le personnalisateur de la carte ;
- le MNO[1] qui, en tant qu'émetteur de la carte, est initialement la seule entité autorisée à gérer les applications (chargement, instanciation, suppression), ce qu'il fait au travers d'un canal de communication sécurisé établi avec la carte, en utilisant des SMS[2] ou via le BIP. Cependant, le MNO peut accorder ces privilèges à l'AP via la fonctionnalité GP *Delegated Management*[3] ;
- l'AP qui personnalise ses applications et ses SD dans la carte de façon confidentielle. Pour ce faire, l'AP dispose de jeux de clés correspondant à ses SD leur permettant de s'authentifier puis d'établir un canal de confiance avec la TOE.
- le *Key Escrow*[4] qui est en charge du stockage sécurisé du jeu de clés initial de l'AP, clés générées par le personnalisateur de la TOE ;
- le CA[5] qui est en charge de sécuriser la création et la personnalisation des clés de l'AP) ;
- le VA qui est en charge de la vérification de la signature des applications (*Mandated* DAP) durant la procédure de chargement.

Des applications peuvent être chargées en phase 7. Ces chargements doivent être protégés conformément à [GUIDES].

Le guide [GUIDE-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.
Par ailleurs, les guides [GUIDE_Basic] et [GUIDE_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte. Le guide [GUIDE-OPE] décrit aussi les règles de vérification qui doivent être appliquées par l'autorité de vérification.

L'évaluateur a considéré comme utilisateur du produit son détenteur final.

1.2.6. Configuration évaluée

Le certificat porte sur la configuration identifiable par les éléments d'identification donnés précédemment (voir chapitre 1.2.2 Identification du produit).

La configuration évaluée correspond à celle décrite dans la cible de sécurité [ST], à l'exception du mode « *Amendment B* » qui n'est pas désactivé.

La configuration ouverte du produit a été évaluée conformément à [OPEN]. Ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de

[1] *Mobile Network Operator* - opérateur du réseau mobile, il peut également assumer le rôle d'émetteur de la carte ou d'administrateur des serveurs OTA.
[2] *Short Message Service* – service de message court.
[3] Gestion déléguée.
[4] Dépositaire de clés.
[5] *Controlling Authority* – autorité de contrôle.

certification et réalisé selon les processus évalués ne remet pas en cause le présent rapport de certification.
L'application « MIFARE4Mobile 2.X framework Package », identifiée en section 1.2.2, a été vérifiée conformément aux contraintes décrites dans [GUIDES].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à la note d'application [OPEN].
Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « Infineon Technologies Smart Card IC (Security Controller) M5072 G11 with optional RSA v1.03.006, EC v1.03.006 and Toolbox v1.03.006 with specific IC dedicated software from Infineon Technologies AG » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP-0035]. Ce microcontrôleur a été certifié le 28 octobre 2014 sous la référence BSI-DSZ-CC-0946-2014 (voir [CER-IC]). Le niveau de résistance du microcontrôleur a été confirmé le 23 novembre 2015 dans le cadre du processus de surveillance (voir [SUR-IC]).

L'évaluation s'appuie en partie sur les résultats d'évaluation du produit « dragonFly version 3.2 sur composant SM33F1ME » certifié le 28 novembre 2014 sous la référence ANSSI-CC-2014/81 (voir [CER]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 11 août 2016, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).
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.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « DragonFly v4.0 sur composant SLE97CNFX1M50PE, identification matérielle 412691, version du *Card Manager* GOP Ref V21.06.01 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Cette plateforme répond aux caractéristiques de plateforme ouverte cloisonnante définie dans la note [OPEN]. En conséquence, tout chargement de nouvelles applications conformes aux contraintes exposées ci-après ne remet pas en question le présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment celles relatives aux applications qui stipulent que :

- les développeurs d'applications « sensibles » doivent :
  - respecter dans leurs implémentations les recommandations se trouvant dans le guide [GUIDE_Sec] ;
  - respecter les [GUIDES] suivant la sensibilité de ces applications,
- les applications « basiques » et « sensibles » doivent être contrôlées par le *Byte Code Verifier* avant leur chargement (pas d'autre exigence imposée par la plateforme) ;
- le chargement de ces applications doit être protégé :
  - si le chargement s'effectue post-émission, conformément à la configuration *Mandated* DAP, toutes les applications doivent être signées (typiquement, par une VA), ce qui assure leur authenticité et leur intégrité jusqu'au chargement dans la carte. La vérification par la carte de ces signatures sera un préalable pour leur chargement effectif dans la carte. Le guide [GUIDE_OPE] décrit la procédure qui doit être suivie, notamment par les autorités de vérification ;
  - si le chargement s'effectue avant l'émission de la carte (pré-émission), les [GUIDES] indiquent les mesures organisationnelles à mettre en place, en particulier pour s'assurer de l'intégrité et de l'authenticité des applications basiques ou sensibles à charger,
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications de [GUIDE_OPE] ;
- le chargement des applications pré-émission doit être protégé conformément au guide [GUIDE_OPE].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est 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[1], 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 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs.

Pour les évaluations enregistrées avant septembre 2014, ou bien pour les réévaluations enregistré avant le 8 septembre 2017, 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 CCRA 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, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR								3	Systematic flaw remediation
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target - DragonFly V4.0, référence FQR 401 4748, version 3, 02/2016. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite - DragonFly V4.0, référence FQR 401 4747, version 1, 02/2016.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report Project : dragonFly v4.0, référence DGF4-0_ETR, version 3.0, 11/08/2016.
[CONF]	Liste de configuration du produit : DragonFly v4.0 rev B on IO266G - Configuration List, référence FQR 401 6044, version 2, 21/03/2016.
[GUIDES]	Guide d'installation du produit : - Pre-Production Process of Secured Platforms, référence I CRD13 2 CRD012 05, Oberthur Technologies ; - Delivery Procedure on Secured Platform, référence I CRD13 2 CRD015 04, Oberthur Technologies ; - NFC FlyBuy Platinum v3.0 - Production Life Cycle, référence FQR 110 6561, issue 1, Oberthur Technologies. Guide d'utilisation du produit, [GUIDE_OPE] : - dragonFly v4.0 Application Management Guide, référence FQR 401 4751, version 5, 23/02/2016 ; - dragonFly V4.0 - rev B – Mobile platform user guide, reference FQR 4015820, issue 4, 23/02/2015, Oberthur Technologies. Guide pour le développement d'application basique, [GUIDE_Basic] : - dragonFly v4.0 Application Development Guide, référence FQR 401 4750, version 1, 09/03/2015 ; - dragonFly v4.0 Application Management Guide, référence FQR 401 4751, version 5, 23/02/2016. Guide pour le développement d'application sensible, [GUIDE_Sec] : - dragonFly v4.0 Application Security Recommendations, référence FQR 401 4749, version 2, 17/12/2015 ; - dragonFly v4.0 Application Management Guide, référence FQR 401 4751, version 5, 23/02/2016.
[CER]	Rapport de certification ANSSI-CC-2014/81, dragonFly 3.2 sur composant SM33F1ME. *Certifié par l'ANSSI le 28 novembre 2014.*

[CER-IC]	Certification Report BSI-DSZ-CC-0946-2014 for Infineon Technologies Smart Card IC (Security Controller) M5072 G11 with optional RSA v1.03.006, EC v1.03.0006 and Toolbox v1.03.006 with specific IC dedicated software from Infineon Technologies AG. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 28 octobre 2014.*
[SUR-IC]	Certification Report BSI-DSZ-CC-0946-V2-2015 for Infineon Technologies Smart Card IC (Security Controller) M5072 G11 with optional RSA v1.03.006, EC v1.03.0006 and Toolbox v1.03.006 with specific IC dedicated software from Infineon Technologies AG. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 11 novembre 2015.*
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[PP JCS-O]	SUN Java Card System Protection Profile - Open Configuration, version 3.0. *Profil de protection certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01.*
[PP (U)SIM]	(U)SIM Java Card Platform Protection Profile - Basic Configuration, version 2.0.2. *Profil de protection certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/04.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001 ; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002 ; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, janvier 2012.
[OPEN]	Certification of "Open" smart card products, version 1.1 (for trial use), 4 février 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.