



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-2014/81

dragonFly version 3.2 sur composant SM33F1ME

Paris, le 28 novembre 2014

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

Guillaume POUPARD
[ORIGINAL SIGNE]



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 présumées 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.anssi@ssi.gouv.fr

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

| | | |
|---|---|--|
| Référence du rapport de certification | ANSSI-CC-2014/81 | |
| Nom du produit | dragonFly version 3.2 sur composant SM33F1ME | |
| Référence/version du produit | Version 3.2 Identification hardware 080503, Card Manager GOP Ref V16.3.0 | |
| Conformité à un profil de protection | [PP JCS-O] SUN Java Card System Protection Profile Open Configuration V2.6 [PP (U)SIM] (U)SIM Java Card Platform Protection Profile - Basic Configuration V2.0.2 | |
| 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 420 rue d'Estienne d'Orves CS 40008, 92 705 COLOMBES CEDEX, France | STMicroelectronics 190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 ROUSSET, France |
| 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 | 6 |
| 1.1. PRESENTATION DU PRODUIT | 6 |
| 1.2. DESCRIPTION DU PRODUIT | 6 |
| 1.2.1. <i>Identification du produit</i> | 7 |
| 1.2.2. <i>Services de sécurité</i> | 8 |
| 1.2.3. <i>Architecture</i> | 8 |
| 1.2.4. <i>Cycle de vie</i> | 10 |
| 1.2.5. <i>Configuration évaluée</i> | 12 |
| 2. L’EVALUATION | 13 |
| 2.1. REFERENTIELS D’EVALUATION | 13 |
| 2.2. TRAVAUX D’EVALUATION | 13 |
| 2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LE REFERENTIEL TECHNIQUE DE L’ANSSI..... | 13 |
| 2.4. ANALYSE DU GENERATEUR D’ALEAS..... | 14 |
| 3. LA CERTIFICATION | 15 |
| 3.1. CONCLUSION | 15 |
| 3.2. RESTRICTIONS D’USAGE..... | 15 |
| 3.3. RECONNAISSANCE DU CERTIFICAT | 16 |
| 3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> | 16 |
| 3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> | 16 |
| ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT..... | 17 |
| ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE | 18 |
| ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION | 20 |

1. Le produit

1.1. Présentation du produit

Le produit évalué est la plateforme (U)SIM Java Card intitulée « dragonFly version 3.2 sur composant SM33F1ME » dont la version du système d'exploitation natif est 080503 et la version du « *Card Manager*¹ » en Java Card est GOP Ref V16.3.0. Cette plateforme est développée par Oberthur Technologies et embarquée sur le microcontrôleur SM33F1ME développé et fabriqué par STMicroelectronics.

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, conformes au SWP (« *Single Wire Protocol* » – protocole fil unique) 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 sont « 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 (« *Over-The-Air* » - par les airs), sans manipulation physique du produit par l'utilisateur final.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué avec ses fonctionnalités de sécurité 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, ainsi qu'au profil de protection [PP JCS-O] comme le requiert le [PP (U)SIM]. Ces conformités sont du type « démontrable ».

¹ « *Card Manager* » est dénommé ISD (« *Issuer Security Domain* » – domaine de sécurité de l'émetteur) dans la terminologie GlobalPlatform.

1.2.1. Identification du produit

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

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

| Eléments de configuration | | Origine |
|---------------------------------------|--|-----------------------|
| Nom de la TOE | dragonFly version 3.2 sur composant SM33F1ME | Oberthur Technologies |
| Référence interne de la TOE | USIM V3.1 NFC FLYBuy V3.1 on DCN9 | |
| Identification du <i>Card Manager</i> | GOP Ref V16.3.0 | |
| Code article | 080503 | |
| Label PVCS ROM | DRAGONFLY_V3_2_DCN9_080503 | |
| Nom du circuit intégré | SM33F1ME | STMicroelectronics |

La version certifiée du produit est identifiable par les éléments détaillés dans la [ST] au chapitre « 2.3 TOE reference » pour la plateforme:

- le code article (ou code SAAAAR): **08 05 03**. Cette valeur peut être lue dans la réponse ATR (« Answer To Reset » – réponse suite à réinitialisation) : 3B 9F 96 80 3F C7 A0 80 31 E0 73 FE 21 1B 64 **08 05 03** 00 82 90 00 4F;
- la version du « Card Manager » en Java Card : « GOP Ref V16.3.0 ». Cette valeur est obtenue, en codage ASCII, en réponse à la commande GET DATA : 80 CA DF 6C 15 pour « Card Manager Release » (version du « Card Manager ») : DF 6C 12 **47 4F 50 20 52 65 66 20 56 31 36 2E 33 2E 30 2F** XX YY (X et Y dépendent de la personnalisation) ;
- les données de production du produit : **47 50 00 2B 82 31 33 40 33 47** correspondant à :
 - o **47 50** = FAB_ID, identifiant de la fonderie du composant sous-jacent (ST Microelectronics) ;
 - o **00 2B** = IC_ID, identifiant du composant sous-jacent ;
 - o **82 31** = OS_ID, identifiant du système d'exploitation ;
 - o **33 40** = OS_Release_Date, date d'émission du système d'exploitation ;
 - o **33 47** = 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 » (cycle de vie de production) : 9F 7F 2A **47 50 00 2B 82 31 33 40 33 47** 00 14 34 12 80 00 00 00 00 14 34 03 36 00 00 00 00 ;

- les données de configuration qui doivent correspondre à la configuration « Mandated DAP » (DAP obligatoire où DAP signifie « Data Authentication Pattern »), c'est-à-dire, entres autres (voir [GUIDES] pour plus de détails), la présence dans la TOE d'un seul « Security Domain » (domaine de sécurité) avec des privilèges de vérification de « Mandated DAP ». Ces informations sont obtenues via la commande GET STATUS (voir [ST] et [GUIDES] pour le détail d'utilisation de cette commande).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont détaillés dans la [ST] aux chapitres « §2.5.13 TOE Security Features » et « §8 TOE Summary Specification », et sont résumés ci-après :

- services de sécurité dédiés aux applications :
 - o confidentialité et intégrité des clés cryptographiques et des opérations associées ;
 - o confidentialité et intégrité des données d'authentification ;
 - o intégrité de l'exécution du code applicatif ;
- services de sécurité dédiés à la gestion de ces applications qui concernent :
 - o la délégation de privilèges : le MNO¹, en tant qu'émetteur de la carte², 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 fournisseur d'applications³ à l'aide de la fonctionnalité *GlobalPlatform* de délégation de cette gestion d'applications ;
 - o la vérification de la signature des applications à charger : la signature par une autorité de vérification VA⁴ (*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 ;
 - o la gestion de *Security Domain* (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 de la *Controlling Authority Security Domain* (CASD) 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 ;
 - o les services de sécurité DESFire : protection des données de l'application et du code DESFire en intégrité et en confidentialité ;
 - o la protection du chargement d'applications *post-issuance* ;
 - o l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

1.2.3. Architecture

La TOE est constituée des éléments suivants :

- un système Java Card, conforme au [PP JCS-O], qui gère et exécute les applications et qui fournit également les interfaces de programmation « Java Card 3.0.1 Classic Edition APIs » permettant de développer ces applications ;
- des packages *GlobalPlatform* (GP), 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 ;

¹ *Mobile Network Operator*, opérateur mobile.

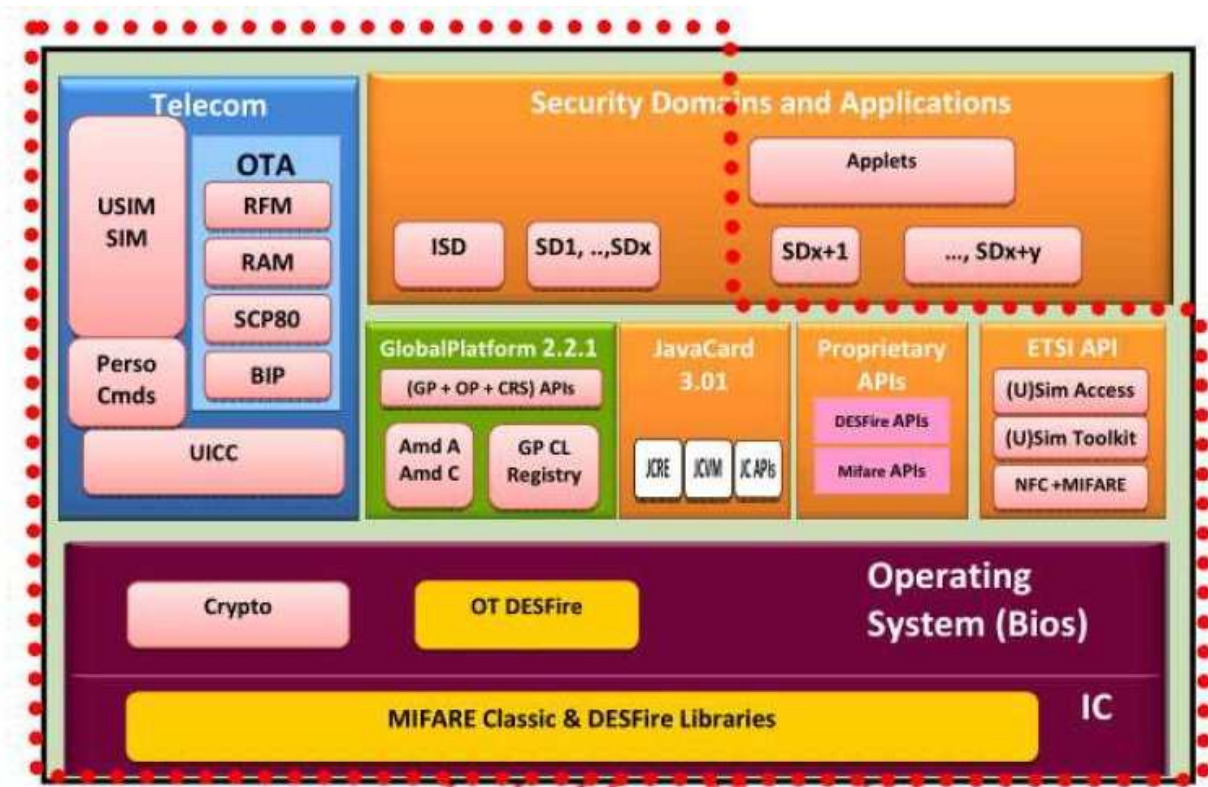
² *Card Issuer*.

³ *Application Provider* (AP).

⁴ *Verification Authority* (VA).

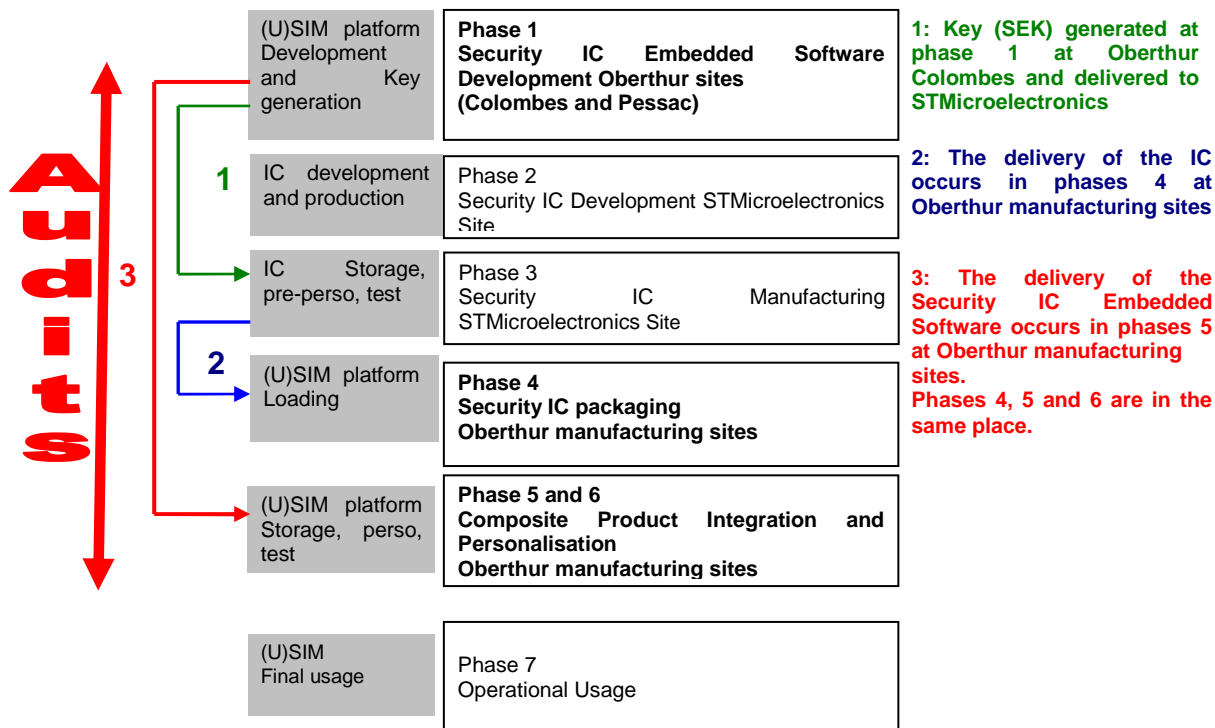
- des interfaces de programmation « (U)SIM API », conformes aux spécifications « 3GPP TS 43.019 », qui fournissent des moyens pour interagir spécifiquement avec les applications (U)SIM ;
- un système d’exploitation qui assure l’interface entre le matériel (composant) et le logiciel (applications) ;
- des fonctionnalités (U)SIM qui fournissent toutes les fonctionnalités décrites dans les spécifications ETSI comme l’authentification au réseau, les commandes OTA par exemple ;
- le protocole BIP (« *Bearer Independent Protocol* » – protocole indépendant de la porteuse), technologie OTA, permet l’échange de données entre une carte (U)SIM d’un téléphone portable et des serveurs distants (remplaçant ainsi la technologie SMS) ;
- des fonctions de sécurité propres au DESFire ;
- le composant SM33F1ME (précédemment certifié, voir [ANSSI-CC-2013/13]).

La figure suivante illustre les principaux éléments de la TOE :



1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



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 SM33F1ME (voir [ANSSI-CC-2013/13]). 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 suivant :

- **Oberthur Technologies – Colombes (pour la phase 1)**

420 rue d'Estienne d'Orves
CS 40008
92705 Colombes
France

- **Oberthur Technologies – Bordeaux (pour la phase 1)**

Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus - Porte 2
33600 Pessac
France

Le produit a été conditionné, intégré et personnalisé sur le site suivant :

- **Oberthur Technologies – Vitré (pour les phases 4, 5 et 6)**

La Haye Robert - Avenue d'Helmesdt – BP 36
35503 Vitre Cedex
France

- **Oberthur Technologies – Shenzen (pour les phases 4, 5 et 6)**

East of 3rd Floor, Great Wall Technology Building No.1
No.2 Kefa Roas, Science and Technology Park
Nanshan District, Shenzhen 518057
Chine

Les sites de développement et de fabrication du microcontrôleur sont identifiés dans le rapport de certification du composant (voir [ANSSI-CC-2013/13]).

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

- le fabricant du composant ;
- l'intégrateur et le personnalisateur de la carte ;
- le MNO (« *Mobile Network Operator* » – opérateur du réseau mobile, il peut également assumer le rôle d'émetteur de la carte ou d'administrateur des serveurs OTA) 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 (« *Short Message Service* » – service de message court) ou via le BIP. Cependant, le MNO peut accorder ces privilèges à l'AP (« *Application Provider* » – fournisseur d'application) via la fonctionnalité GP « *Delegated Management* » (gestion déléguée) ;
- 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.
- l'AD (*Application Developer* – développeur d'applications) ;
- le « *Key Escrow* » (dépositaire de clés, il est en charge du stockage sécurisé du jeu de clés initial de l'AP, clés générées par le personnalisateur de la TOE) ;
- le CA (« *Controlling Authority* » – autorité de contrôle, il est en charge de sécuriser la création et la personnalisation des clés de l'AP) ;
- le VA (« *Validation Authority* » - autorité de validation).

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

1.2.5. Configuration évaluée

Le certificat porte sur la configuration identifiable par les éléments d'identification donnés précédemment (voir « §1.2.1 Identification du produit »).

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 certification et réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.

La configuration évaluée ne comporte aucune application hors TOE.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM] et à la note [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 SM33F1ME certifié au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP0035]. Ce microcontrôleur a été certifié le 6 mars 2013 sous la référence [ANSSI-CC-2013/13].

Par ailleurs, cette évaluation a également pris en compte les résultats des évaluations des versions précédentes du produit certifié (voir [ANSSI-CC-2012/39], [ANSSI-CC-2013/60] et [ANSSI-CC-2014-35]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 27 octobre 2014, 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 le référentiel technique 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 visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [ANSSI-CC-2013/13]).

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 la plateforme (U)SIM Java Card intitulée « dragonFly version 3.2 sur composant SM33F1ME », dont la version du système d'exploitation natif est 080503 et la version du « *Card Manager*¹ » en Java Card est GOP Ref V16.3.0, soumise 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 :
 - o respecter dans leurs implémentations les recommandations se trouvant dans le guide [AGD_OPE] ;
 - o respecter les [GUIDES] suivant la sensibilité de ces applications ;
- les applications « basiques » 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 :
 - o si le chargement s'effectue après l'émission de la carte (« *post-issuance* »), conformément à la configuration « *Mandated DAP* », toutes les applications doivent être signées (typiquement, par une VA (*Validation Authority* - autorité de validation comme définie dans [ST]), 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 [AGD_OPE_App_Mngt] décrit la procédure ;
 - o si le chargement s'effectue avant l'émission de la carte (« *pre-issuance* »), les [GUIDES] indiquent les mesures organisationnelles à mettre en place, en

¹ « *Card Manager* » est dénommé ISD (« *Issuer Security Domain* » – domaine de sécurité de l'émetteur) dans la terminologie GlobalPlatform.

particulier pour s'assurer de l'intégrité et de l'authenticité des applications basiques à charger.

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'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 :



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 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 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, 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 | 1 | Security architecture description |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 | 4 | 4 | Complete functional specification |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 | 1 | 1 | Implementation representation of the TSF |
| | ADV_INT | | | | | 2 | 3 | 3 | | | |
| | ADV_SPM | | | | | | 1 | 1 | | | |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 | 3 | 3 | Basic modular design |
| AGD Guides d'utilisation | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Operational user guidance |
| | AGD_PRE | 1 | 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 | 4 | Production support, acceptance procedures and automation |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 | 4 | 4 | Problem tracking CM coverage |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Delivery procedures |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 | 2 | 2 | Sufficiency of security measures |
| | ALC_FLR | | | | | | | | | | |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 | 1 | 1 | Developer defined life-cycle model |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 | 1 | 1 | Well-defined development tools |
| ASE Evaluation de la cible de sécurité | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Conformance claims |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Extended components definition |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | ST introduction |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Security objectives |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Derived security requirements |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security problem definition |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | TOE summary specification |
| ATE Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | Analysis of coverage |
| | ATE_DPT | | | 1 | 1 | 3 | 3 | 4 | 1 | 1 | Testing: basic design |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | Functional testing |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | Independent testing: sample |
| AVA Estimation des vulnérabilités | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 | 5 | 5 | Advanced methodical vulnerability analysis |

Annexe 2. Références documentaires du produit évalué

| | |
|----------|--|
| [ST] | <p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - Security target dragonFly v3.2, référence FQR 110 6788, issue 2.0, Oberthur Technologies. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Security Target-Lite dragonfly v3.2, référence FQR 110 6787, issue 2.0, Oberthur Technologies. |
| [RTE] | <p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation technical report - Project: DragonFly, référence DragonFLY_ETR, version 3.0, 27 octobre 2014, THALES (TCS – CNES). |
| [CONF] | <p>Liste de configuration</p> <ul style="list-style-type: none"> - dragonFly v3.2 - Configuration List, référence FQR 115 0003, issue 2, Oberthur Technologies. |
| [GUIDES] | <p>Guide de préparation du produit :</p> <ul style="list-style-type: none"> - Pre-Production Process of Secured Platforms référence I CRD13 2 CRD012 01, Oberthur Technologies ; - Delivery Procedure on Secured Platform référence I CRD13 2 CRD015 01, Oberthur Technologies ; - NFC FlyBuy Platinum v3.0 - Production Life Cycle, référence FQR 110 6561, issue 1 Oberthur Technologies. <p>Guides d'opération du produit :</p> <ul style="list-style-type: none"> - [AGD_OPE] : dragonFly v3.1 - Application Security recommandations, référence FQR 110 6719, version 4, Oberthur Technologies. - dragonFly v3.1 (APPLICATION DEVELOPMENT GUIDE), référence FQR 110 6718, version 1, Oberthur Technologies. - [AGD_OPE_App_Mngt] : dragonFly v3.1 (APPLICATION MANAGEMENT GUIDE), référence FQR 110 6717, issue 1, Oberthur Technologies. - Guidance for implementation of MIFARE DESFire on SM33F1ME, référence FQR 110 7071, issue 1, Oberthur Technologies. |

| | |
|--------------------|---|
| | <p>Guides d'utilisation du produit :</p> <ul style="list-style-type: none"> - DesFireST APIs User Guide référence FQR 110 6576, issue 1. |
| [PP0035] | <p>Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i></p> |
| [PP JCS-O] | <p>SUN Java Card System Protection Profile - Open Configuration, version 2.6, <i>Profil de protection certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03.</i></p> |
| [PP (U)SIM] | <p>(U)SIM Java Card Platform Protection Profile - Basic Configuration, version 2.0.2, <i>Profil de protection certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/04.</i></p> |
| [ANSSI-CC-2012/39] | <p>NFC FLYBUY PLATINUM V2 sur composant ST33F1ME. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-2012/39.</i></p> |
| [ANSSI-CC-2013/60] | <p>Services DESFIRE de NFC FlyBuy Platinum V3.0 version R9.32.4 sur le composant SM33F1ME. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-2013/60</i></p> |
| [ANSSI-CC-2013/13] | <p>ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384, SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512, SL33F1M/1M0/896/768/640/512, SP33F1M, With dedicated software revision D, Optional cryptographic library Neslib 3.0 or 3.2, Optional MIFARE DESFire™ EV1. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-2013/13.</i></p> |

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, DCSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004. |
| [JIWG IC] * | Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009. |
| [JIWG AP] * | Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013. |
| [COMP] * | Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012. |
| [CC RA] | Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 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 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr . |
| [OPEN] | Certification of « Open » smart card products, version 1.1 (for trial use), 4 February 2013. |

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