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-2013/60

Services DESFIRE de NFC FlyBuy Platinum V3.0 version R9.32.4 sur le composant SM33F1ME

Paris, le 28 août 2013

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

Patrick Pailloux

[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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2013/60

Nom du produit

Services DESFIRE de NFC FlyBuy Platinum V3.0 version R9.32.4 sur le composant SM33F1ME

Référence/version du produit

Identification hardware 079424, Card Manager GOP Ref V11.3

Conformité à un profil de protection

Ce produit ne réclame pas la conformité à un profil de protection.

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'Estiennes 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'Estiennes 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 est la plateforme (U)SIM Java Card ouverte intitulée « NFC FlyBuy Platinum V3.0 version R9.32.4 sur le composant SM33F1ME avec la librairie MIFARE DESFIRE EV1 version 1.1 » dont la version du système d'exploitation natif est 079424 et la version du « *Card Manager*[1] » en Java Card est GOP Ref V11.3. Cette plateforme est développée par Oberthur Technologies et embarquée sur le microcontrôleur SM33F1ME développé et fabriqué par STMicroelectronics.
Les fonctions évaluées de ce produit sont les services de sécurité spécifiques au DESFIRE et décrit dans le paragraphe 1.2.3.

Cette plateforme (U)SIM Java Card peut 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.

Dans le cadre de la présente évaluation, la TOE (« *Target Of Evaluation* » – cible d'évaluation) est la plateforme seule comprenant uniquement l'implémentation de fonctions de sécurité liées au DESFIRE. Les logiciels applicatifs ne sont pas inclus dans le périmètre de l'évaluation.

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.

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

1.2.2. 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	Services DESFIRE de NFC FlyBuy Platinum V3.0 version R9.32.4 sur le composant SM33F1ME	Oberthur Technologies
Référence de la TOE	USIM V3.1 NFC FLYBuy Platinum V3.0 EAL4+ 768K on DCN9	
Code article	079424	
Identification du *Card Manager*	GOP Ref V11.3	
Label PVCS ROM	USIM_V31_NFC_FLYBUY_PLATINUM_079424	
Nom du circuit intégré	SM33F1ME	STMicroelectronics

La version certifiée du produit est identifiable par les éléments détaillés dans la [ST] au chapitre « 2.2 TOE reference » :

- le code article : **079424**.
  Cette valeur peut être lue dans la réponse ATR (« *Answer To Reset* » – réponse suite à réinitialisation) :
  3B 9F 96 80 3F C7 00 80 31 E0 73 FE 21 1B 64 **07 94 24** 00 82 90 00

- la version du « *Card Manager* » en Java Card : « GOP Ref V11.3 ».
  Cette valeur est obtenue, en codage ASCII, en réponse à la commande GET DATA 00 CA DF 6C 13 pour « *Card Manager Release* » (version du « *Card Manager* ») :
  DF 6C 10 **47 4F 50 20 52 65 66 20 56 3B 2E 33 2E 30 2F** 00
  (« GOP Ref V11.3 » en ASCII) ;

- les données de production du produit. 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 30 35 33 38** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 34 12 80 00 00 00 00 14 34 03 36 00 00 00 00
  correspondant à :
  - **47 50** = FAB_ID, identifiant de la fonderie du composant sous-jacent (ST Microelectronics) ;
  - **00 2B** = IC_ID, identifiant du composant sous-jacent (SM33F1ME);
  - **82 31** = OS_ID, identifiant du système d'exploitation ;
  - **30 35** = OS_Release_Date, date d'émission du système d'exploitation ;
  - **33 38** = OS_Release_Level, niveau d'émission du système d'exploitation dans les projets du développeur.

- 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).

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par la TOE, en plus de ceux fourni par le microcontrôleur (voir [ANSSI-CC-2013/13]), servent à protéger les données et les biens de l'application MIFARE DESFire. Ils sont détaillés dans la [ST] au chapitre « §7 TOE Summary Specification », et sont résumés ci-après :

- contrôle d'accès au code et données de l'application DESFire ;
- effacement des données utilisées par l'application DESFire.

1.2.4. Architecture

La carte (U)SIM est composée des éléments suivants :

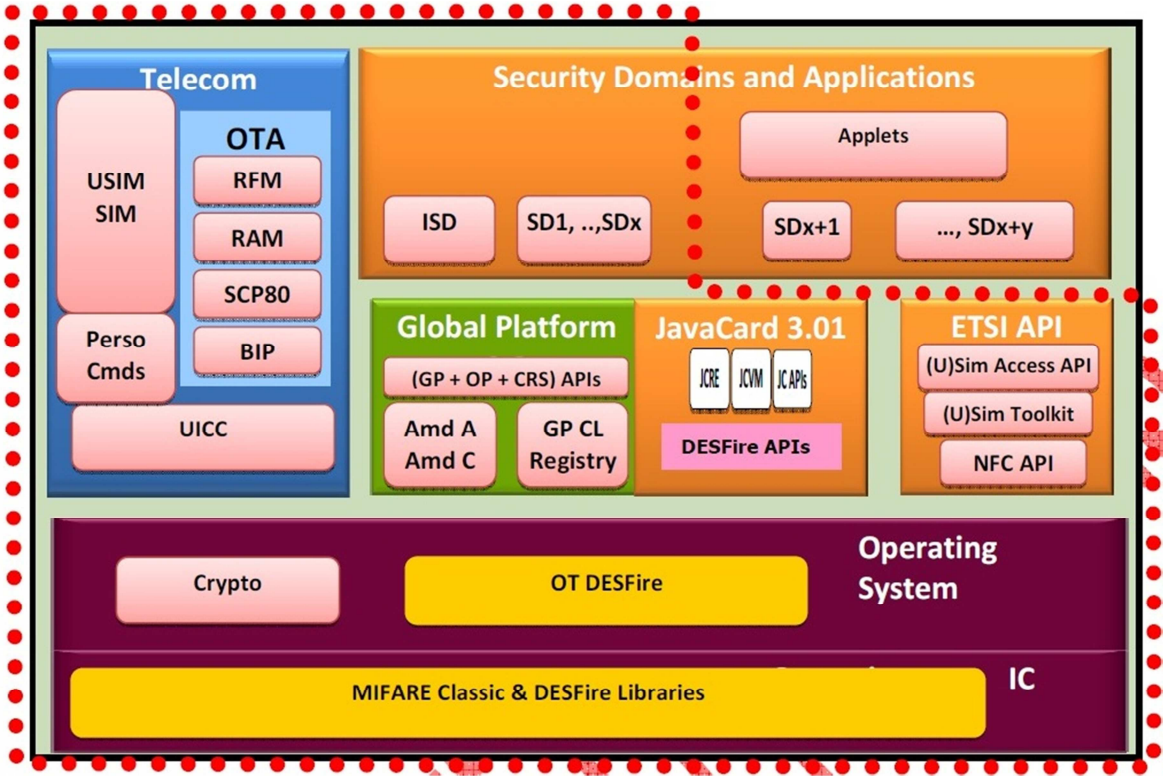
- un système Java Card qui gère et exécute les applications et qui fournit également les interfaces de programmation « Java Card 3.0.1 Classic Edition APIs » permettant de développer ces applications ;
- des packages *GlobalPlatform* (GP), conformes aux spécifications « GlobalPlatform Card Specification, version 2.2 », qui fournissent une interface commune et largement utilisée pour communiquer avec la carte et pour gérer de façon sécurisée les applications ;
- des interfaces de programmation « (U)SIM APIs », conformes aux spécifications « 3GPP TS 31.130 version 6.6.0 release 6 », qui fournissent des moyens pour interagir spécifiquement avec les applications (U)SIM ;
- 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, qui permet l'échange de données entre une carte (U)SIM d'un téléphone portable et des serveurs distants (remplaçant ainsi la technologie SMS) ;
- un système d'exploitation qui assure l'interface entre le matériel (composant) et le logiciel (applications) ;
- le composant SM33F1ME avec la librairie MIFARE DESFIRE EV1 (précédemment certifié, voir [ANSSI-CC-2013/13]).

La TSF (*TOE Security Function* – Fonctions de sécurité de la TOE) est constituée des éléments suivants :

- les fonctions de sécurité spécifiques au DESFire pour permettre l'intégrité et la confidentialité des données de l'application DESFire ainsi que la confidentialité du code de l'application DESFire ;
- le composant SM33F1ME avec la librairie MIFARE DESFire EV1 (précédemment certifié, voir [ANSSI-CC-2013/13]).

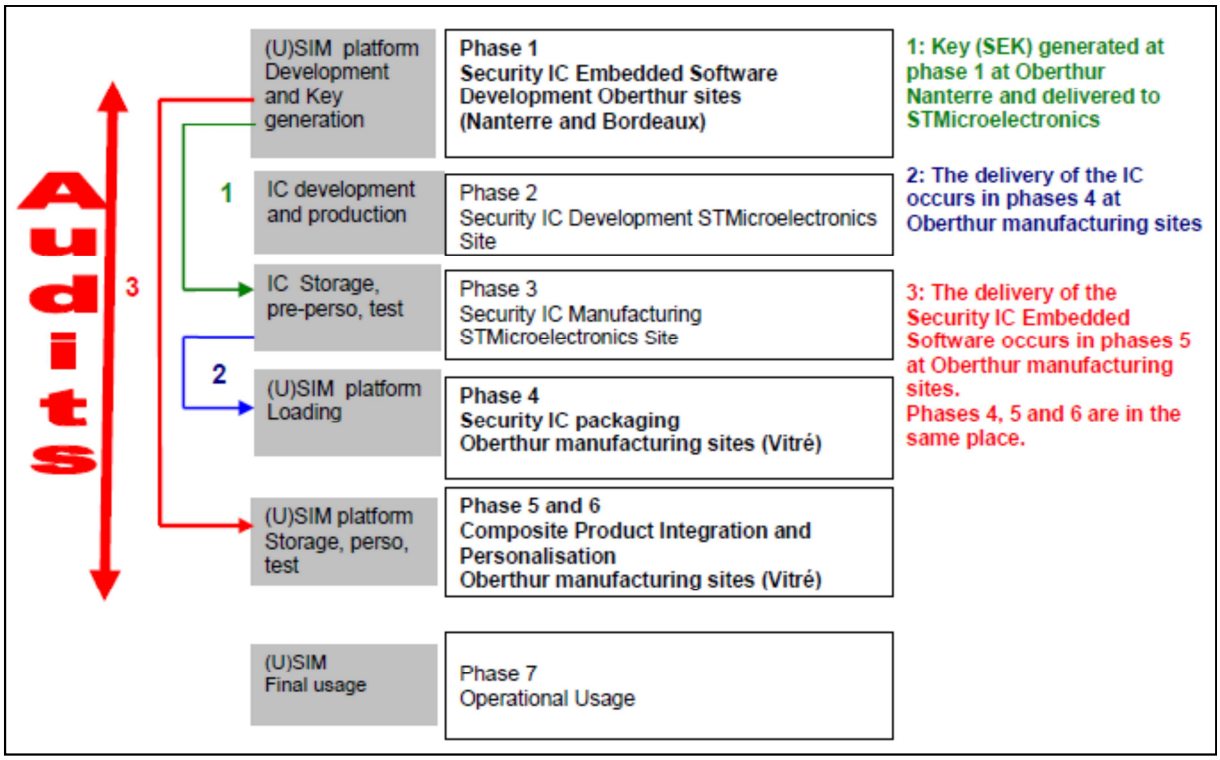
Le produit peut héberger d'autres applets chargées en phase « *pre-issuance* » dont les identifiants seront fournis au chapitre « §1.2.5 Configuration évaluée ».

La figure suivante illustre les principaux éléments de la TOE. Les éléments en pointillés délimitent le périmètre d'évaluation (la TOE), les deux blocs jaune : « OT DESFire » et « MIFARE Classic & DESFire libraries » sont les fonctions évaluées dans le cadre de l'évaluation.



1.2.5. 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 – Nanterre (pour la phase 1)**

  71-73, rue des Hautes Pâtures
  92726 Nanterre
  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

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

1.2.6. Configuration évaluée

Le certificat porte sur la configuration identifiable par les éléments donnés précédemment (voir « §1.2.2 Identification du produit »).

De plus, le produit testé par l'évaluateur était configuré de la façon suivante (du point de vue du contenu de la carte – « *Card Content* ») :

- domaine de sécurité de l'émetteur (« *Issuer Security Domain - Card Manager* ») :
  - A0 00 00 01 51 00 00 00 ;
- autres domaines de sécurité (« *Security Domains* ») et applications :
  - *CAT-TP* : A0 00 00 00 77 01 00 00 14 00 00 FE 00 00 01 00 ;

    - *« Remote Management » (for CAT-TP)* : A0 00 00 00 77 01 00 00 14 00 00 FE 00 00 03 00;
- autres fichiers exécutables chargés dans le produit en phase « *pre-issuance* » sous la forme de packages Java Card, ils sont identifiés ci-après soit par leur nom Java Card soit par leur AID (« *Applet Identifier* » – identifiant d'applet) :
    - *« Card Manager »* : A0 00 00 01 51 53 50 ;
    - CAT-TP *« Applet Utility »* : A0 00 00 00 77 01 00 00 14 10 00 00 00 00 00 02;
    - CAT-TP: A0 00 00 00 77 01 00 00 14 10 00 00 00 00 00 01 ;
    - CAT-TP *« Remote Management »* : A0 00 00 00 77 01 00 00 14 10 00 00 00 00 00 03 ;
- autres fichiers packages natifs intégrés dans le code mais pour lesquels la commande « *Get Status* » du produit ne renvoie pas d'éléments d'identification.

Dans son évaluation, l'évaluateur a pris en compte la présence de tous ces composants logiciels.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
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 [CC 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 » 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 de l'évaluation de la version précédente du produit certifié (voir [ANSSI-CC-2012/39]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 9 août 2013, 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 le produit « Services DESFIRE de NFC FlyBuy Platinum V3.0 version R9.32.4 sur le composant SM33F1ME, Identification hardware 079424, Card Manager GOP Ref V11.3 » 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.

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 [AGD_OPE] ;
  - 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 :
  - 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 ;
  - si le chargement s'effectue avant l'émission de la carte (« *pre-issuance* »), 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 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'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. 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. 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**	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									
	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 FLY3Bis – DESFIRE services of NFC FLYBuy Platinum V3.0 on SM33F1M, référence FQR 110 6469, issue 2.2. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target-Lite FLY3Bis – DESFIRE services of NFC FLYBuy Platinum V3.0 on SM33F1M, référence FQR 110 6326, issue 2.1.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – Project FLY3Bis, référence Fly3b_ETR, révision 2.0, 9 août 2013. Pour le besoin des évaluations en composition avec cette plateforme un rapport technique pour la composition a été validé : - Evaluation Technical Report Lite – Project FLY3Bis, référence Fly3b_ETR Lite_v2.0, révision 2.0, 19 août 2013.
[CONF]	Liste de configuration - NFC FlyBuy Platinum v3.0 – Configuration List, référence FQR 110 6557, issue 2.
[GUIDES]	Guide de préparation du produit : - NFC FlyBuy Platinum v3.0 AGD_PRE Delivery Acceptance, référence FQR 110 6560, issue 1. Guide d'opération du produit : - NFC FlyBuy Platinum v3.0 APPLICATION MANAGEMENT GUIDE, référence FQR 110 6443, ISSUE 1 ; - [AGD_OPE] : NFC FlyBuy - Application Security recommandations, référence FQR 110 5886, version 2 ; - NFC FlyBuy Platinum APPLICATION DEVELOPMENT GUIDE, référence FQR 110 5885, version 1.1. Guide d'utilisation du produit : - NFC FlyBuy Platinum v3.0 référence FQR 110 6576, issue 1. - NFC FlyBuy Platinum v3.0, DesFireST APIs User Guide référence FQR 110 6444, issue 1.
[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.*
[ANSSI-CC-2012/39]	NFC FLYBUY PLATINUM V2 sur composant ST33F1ME. *Certifié par l'ANSSI sous la référence ANSSI-CC-2012/39.*

[ANSSI-CC-2013/13]	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 DESFireTM EV1. *Certifié par l'ANSSI sous la référence ANSSI-CC-2013/13.*

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, 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.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[JIWG AP]	Joint Interpretation Library - Application of attack potential to smart-cards, version 2.9, janvier 2013.
[COMP]	Joint Interpretation Library – 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, May 2000.
[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.