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-2011/24

NFC FlyBuy sur S3FS91J

Paris, le 12 juillet 2011

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

Le vice-amiral Michel Benedittini,
directeur général adjoint
[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 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-2011/24

Nom du produit

NFC FlyBuy sur S3FS91J

Référence/version du produit

version du système d'exploitation en natif : 075895

version du *Card Manager* en Java Card : GOP Ref V1.5.o

Conformité à un profil de protection

[PP (U)SIM], version 2.0.2, certifié par l'ANSSI

(U)SIM Java Card Platform Protection Profile

Basic and SCWS Configurations

Evolutive Certification Scheme for (U)SIM cards

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

Oberthur Technologies

71-73 chemin des Hautes Pâtures, 92 726 NANTERRE CEDEX, France

Samsung Electronics Co. Ltd

San#24 Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do, 449-711, République de Corée

Commanditaire

Oberthur Technologies

71-73 chemin des Hautes Pâtures, 92 726 NANTERRE CEDEX, France

Centre d'évaluation

THALES - CEACI (T3S – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Tél : +33 (0)5 62 88 28 01 ou 18, mél : nathalie.feyt@thalesgroup.com

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 (U)SIM Java Card « NFC FlyBuy sur S3FS91J »**,** dont la version du système d'exploitation natif est 075895 et la version du *Card Manager*[1] en Java Card est GOP Ref V1.5.o. Cette plateforme est développée par Oberthur Technologies et Samsung Electronics Co. Ltd.

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 (*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 (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. Les logiciels applicatifs ne sont pas inclus dans le périmètre de l'évaluation.

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] configuration basic, 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 (voir [ST] au chapitre « 2.3 TOE REFERENCE » pour plus de détails) :

- la version du système d'exploitation natif : **075895**. Cette valeur peut être lue dans la réponse ATR (*Answer To Reset* – réponse suite à réinitialisation) et dont la valeur est 3B 9F 96 80 3F C7 00 80 31 E0 73 FE 21 1B 64 **07 58 95** 00 82 90 00 ;
- la version du *Card Manager* en Java Card : « GOP Ref V01.05.o ». Cette valeur est obtenue en codage ASCII via la commande Get Data pour « *Card Manager Release* » (version du *Card Manager*). La valeur lue doit être : DF 6C 0E **47 4F 50 20 52 65 66 20 56 31 2E 35 2E 6F** 90 00 ;
- les données de production du produit correspondant à (FAB_IC, IC_ID, OS_ID, OS_Release_Date, OS_Release_Level) comme spécifiées dans la [ST]. Ces informations sont obtenues via la commande Get Data pour « *Production Life cycle* » (cycle de vie de production). La valeur lue doit être 9F 7F 2A **42 50 01 13 82 31 B0 61 33 05** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 00, leur signification est :
  - **42 50 =** FAB_ID, identifiant de la fonderie du composant sous-jacent ;
  - **01 13** = IC_ID, identifiant du composant sous-jacent ;
  - **82 31** = OS_ID, identifiant du système d'exploitation ;
  - **B0 61** = OS_Release_Date, date d'émission du système d'exploitation (**B** correspond à l'année en hexadécimal après 2000, soit ici 2011 et 061 correspond au jour en hexadécimal dans l'année) ;
  - **33 05** = OS_Release_Level, niveau d'émission du système d'exploitation (**33** correspond à un numéro interne au développeur et le **5** correspond au dernier 5 du numéro de version (075895**)** du système d'exploitation natif) ;
- 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 « *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 pour protéger les données d'application et les biens concernent les applications et la gestion de ces applications (voir [ST] au « §2.5.10 TOE Security Features » et au « §8 TOE Summary Specification » pour plus de détails) :

- 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 les applications s'exécutant dans la plateforme ;
  - intégrité d'exécution du code d'application ;
- services de sécurité dédiés à la gestion de ces applications qui concernent :
  - le MNO (*Mobile Network Opérator* – opérateur du réseau mobile) 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 (*Bearer Independent Protocol* – protocole indépendant de la porteuse). Cependant, le MNO peut accorder ces privilèges à l'AP (*Application Provider* – fournisseur d'application) via la fonctionnalité GP « *Delegated Management* » (gestion déléguée) ;
  - les applications « basiques » pour lesquelles la plateforme n'impose aucune recommandation à l'exception de l'utilisation du « *Byte Code Verifier* » avant leur chargement ;
    - si le chargement s'effectue après l'émission de la carte (« *post-issuance* »), conformément à la configuration « *Mandated DAP* », toutes les applications basiques, une fois passées par le « *Byte Code Verifier* » 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 ;

- les applications « sensibles » qui doivent subir une évaluation [CC] en composition sur la présente plate-forme[1] ;
  - si le chargement s'effectue après l'émission de la carte («*post-issuance*»), conformément à la configuration «*Mandated DAP*», toutes les applications sensibles sont signées par la VA (*Validation Authority* - autorité de validation). La vérification par la carte de cette signature sera un préalable à 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 de ces applications sensibles à charger ;
- les AP qui personnalisent leurs applications et leurs SD (*Security Domain* - domaine de sécurité) dans la carte de façon confidentielle ; pour ce faire, les AP disposent de jeux de clés correspondant à leurs SD leur permettant de s'authentifier puis d'établir un canal de confiance avec la TOE.

[1] Comme pour toute évaluation, le cycle de vie de construction de la (future) TOE fera partie du périmètre de l'évaluation, en particulier, l'adéquation des mesures organisationnelles pour protéger la TOE en construction.

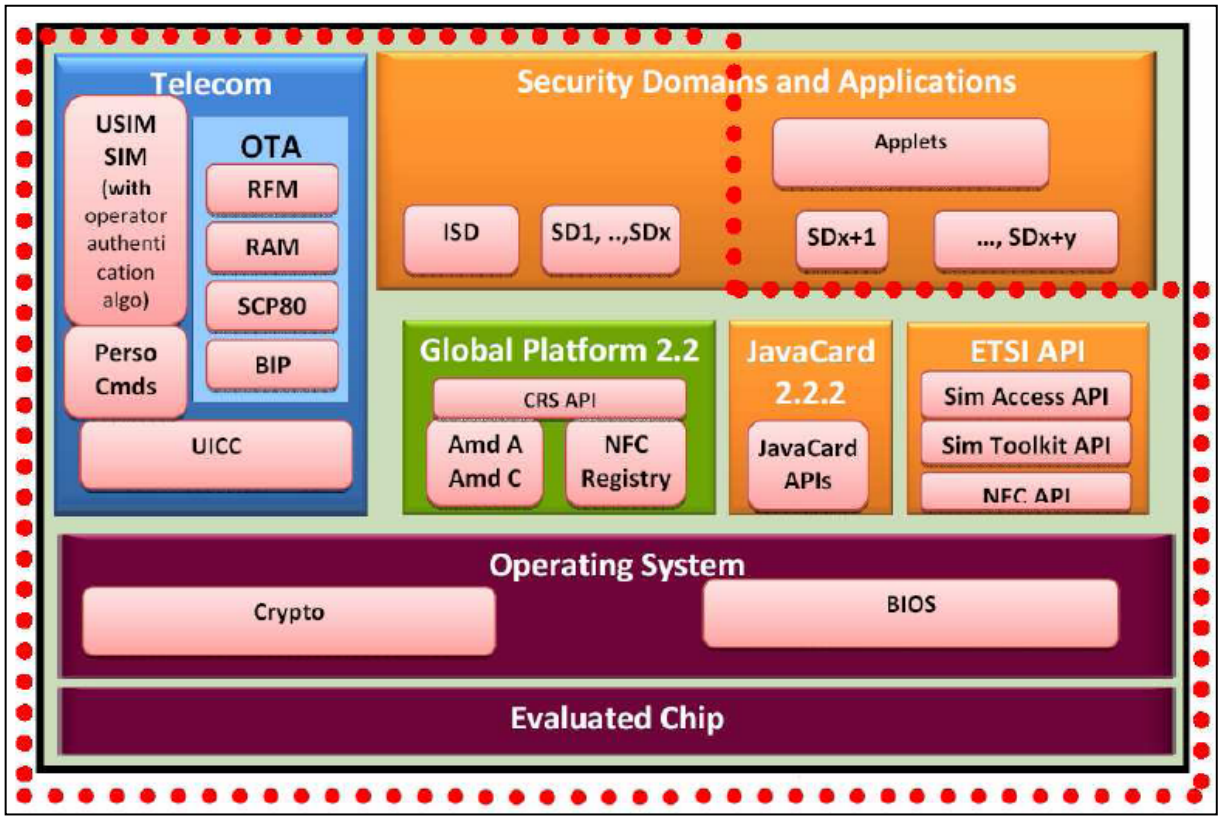
1.2.3. Architecture

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 », 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 ;
- un système d'exploitation qui assure l'interface entre le matériel (composant) et le logiciel (applications), en particulier, il comprend la VM (*Virtual Machine* – machine virtuelle) et des interfaces de programmation (OS APIs) ;
- des fonctionnalités (U)SIM qui fournissent toutes les fonctionnalités décrites dans les spécifications ETSI comme les commandes UICC, l'authentification au réseau, les commandes OTA (*Over The Air* – par les airs), etc. ;
- le protocole BIP ;
- le composant S3FS91J (précédemment certifié, cf. [ANSSI-CC-2009/57]).

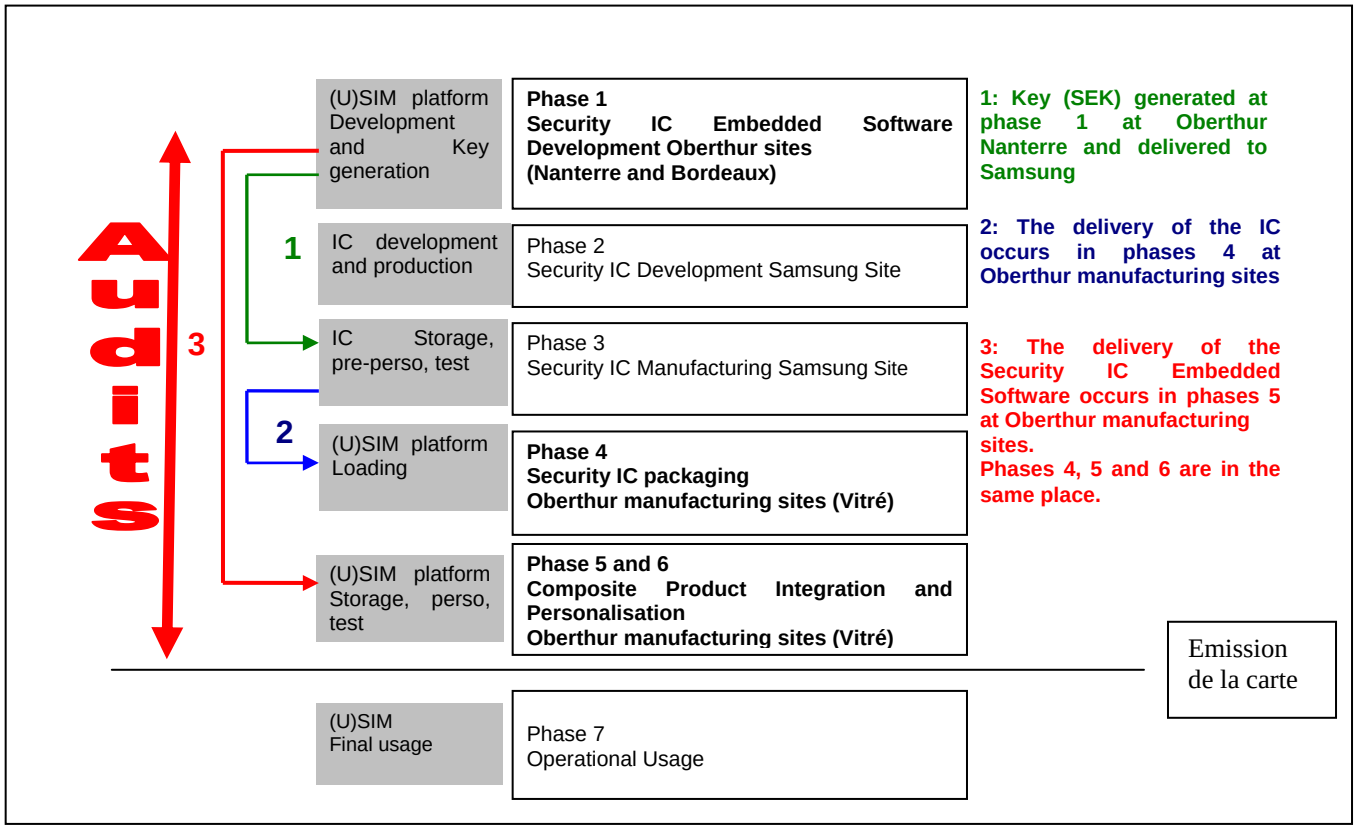
Le produit peut héberger d'autres applets chargées en phase *pre-issuance* mais l'évaluation sécuritaire de ces applets ne fait pas partie du périmètre de l'évaluation de la présente TOE (voir « §1.2.5 Configuration évaluée » plus bas pour plus de détails).

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, (U)SIM applet, 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 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 précédente du composant (cf. [ANSSI-CC-2009/57]). Le point de livraison, ou d'émission de la carte, est en sortie de la phase 6.

Le produit a été développé sur le site 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 packagé, 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 (cf. [ANSSI-CC-2009/57]).

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 (il peut également assumer le rôle d'émetteur de la carte ou d'administrateur des serveurs OTA) ;
- l'AP ;
- le AD (*Application Developper* – 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.

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 plus haut (cf. « §1.2.1 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 (« *Executable Load Files* »), ils sont identifiés ci-après soit par leur nom Java Card soit par leur AID (*Applet IDentifier* – identifiant d'applet) :
  - Packages natifs intégrés dans le code :
    - Java.lang: A0 00 00 00 62 00 01
    - Java.io: A0 00 00 00 62 00 02
    - Java.rmi: A0 00 00 00 62 00 03
    - Javacard.framework: A0 00 00 00 62 01 01
    - Javacard.framework.service: A0 00 00 00 62 01 01 01
    - Javacard.security: A0 00 00 00 62 01 02
    - Javacardx.crypto: A0 00 00 00 62 02 01
    - Sim.access: A0 00 00 00 09 00 03 FF FF FF FF 89 10 71 00 01
    - Sim.toolkit: A0 00 00 00 09 00 03 FF FF FF FF 89 10 71 00 02
    - uicc/access: A0 00 00 00 09 00 05 FF FF FF FF 89 11 00 00 00
    - uicc/toolkit: A0 00 00 00 09 00 05 FF FF FF FF 89 12 00 00 00
    - uicc/system: A0 00 00 00 09 00 05 FF FF FF FF 89 13 00 00 00
    - uicc/usim/access: A0 00 00 00 87 10 05 FF FF FF FF 89 13 10 00 00
    - uicc/usim/toolkit: A0 00 00 00 87 10 05 FF FF FF FF 89 13 20 00 00
    - uicc/access/fileadministration: A0 00 00 00 09 00 05 FF FF FF FF 89 11 01 00 00
    - uicc/isim/access: A0 00 00 00 87 10 05 FF FF FF FF 89 14 10 00 00
    - com/gemplus/javacard/treeManagement: A0 00 00 00 09 00 02 FF 32 FF 20 89 BF FF BA 02
  - Packages Java Card chargés :
    - *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 RemoteMgt: A0 00 00 00 77 01 00 00 14 10 00 00 00 00 00 03

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 3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM] et à la note [ANSSI-CC-NOTE.10].

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 [CC AP] ont été appliqués.

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 « Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [BSI-PP-0035]. Ce microcontrôleur a été certifié par l'ANSSI (cf. [ANSSI-CC-2009/57])

Le niveau de résistance du microcontrôleur a été confirmé le 23 décembre 2010 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 juillet 2011, 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

Le produit évalué offre les services cryptographiques suivants :
- Random number generation ;
- Hash algorithms ;
- Secure channel protocol SCP 80 ;
- Secret elements ;
- Key generation ;
- Signature, cryptogram and verification ;
- Encryption and decryption ;
- Card content management ;
- Secure channel.

Ces services ne peuvent cependant pas être analysés d'un point de vue cryptographique car ils ne concourent pas à la sécurité propre du produit ; leur résistance dépend de leur emploi par l'application embarquée ultérieurement sur le produit.

La cotation des mécanismes cryptographiques a été réalisée par l'ANSSI conformément à son référentiel technique [REF-CRY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu aux conclusions suivantes :

- les mécanismes sont reconnus conformes au référentiel technique [REF-CRY] avec les exceptions et recommandations suivantes :
  - lorsque des éléments sensibles sont échangés au cours d'une session de communication sécurisée, il est nécessaire d'utiliser le niveau de sécurité le plus haut du canal de communication sécurisé (protection en intégrité et confidentialité) car le chiffrement seul des données sensibles par l'algorithme de chiffrement Triple-DES ECB utilisé avec une clé statique et le choix du « *padding* » laissé à l'application appelante n'est pas reconnu conforme au référentiel [REF-CRY]. Ce choix d'implémentation, objet de la présente remarque, provient des spécifications ETSI TS-102 225 de la cible de sécurité [ST] auxquelles le développeur est contraint de se conformer ;
  - le SCP 80 propose plusieurs mécanismes cryptographiques pour protéger les communications d'un canal sécurisé ; parmi ces mécanismes, ceux reconnus conformes au référentiel [REF-CRY] sont :
    - ISO 9797, Algo 3 et 4 pour l'intégrité ;
    - triple-DES CBC avec clés de 112 ou 168 bits pour la confidentialité.
  - les mécanismes mis en œuvre par le produit pour assurer la fonction de chargement sécurisé des applications (signature DAP), conformément aux spécifications GlobalPlatform auxquelles le développeur est contraint de se conformer, ne sont pas reconnus conformes au référentiel [REF-CRY] ; en effet, ceux-ci reposent sur l'utilisation de RSA avec des clés de 1024 bits et l'emploi de la fonction SHA-1 ; toutefois, à la date de la certification, l'évaluateur n'a pas pu mettre en évidence une vulnérabilité exploitable pour le niveau AVA_VAN visé. Néanmoins, l'ANSSI attire l'attention de l'utilisateur sur le fait que ce verdict de l'évaluateur reflète l'état de l'art actuel dans le domaine des attaques ; cet état de l'art évolue avec le temps, notamment du fait des avancées dans le domaine de la cryptographie. Dans son référentiel technique [REF-CRY], qui dicte l'ensemble des règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, la règle « RègleFact-1 », relative à RSA, indique : « la taille minimale du module est de 2048 bits, pour une utilisation ne devant pas dépasser l'année 2020. »

2.4. Analyse du générateur d'aléas

Ce générateur a fait l'objet d'une analyse par l'ANSSI, qui l'a reconnu conforme à son référentiel technique [REF-CRY].

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 « NFC FlyBuy sur S3FS91J », dont la version du système d'exploitation en natif est 075895 et la version du *Card Manager* en Java Card est GOP Ref V1.5.o, soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

3.2. Restrictions d'usage

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

Ce certificat donne une appréciation de la résistance de la plateforme « NFC FlyBuy sur S3FS91J », dont la version du système d'exploitation en natif est 075895 et la version du *Card Manager* en Java Card est GOP Ref V1.5.o, à des attaques génériques du fait de l'absence d'application spécifique embarquée. Ces attaques ont été menées, entre autres, avec le chargement d'applets malveillantes conçues pour les besoins de test par l'évaluateur.

Cette plateforme répond aux caractéristiques de plateforme ouverte cloisonnante définie dans la note [ANSSI-CC-NOTE.10]. 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].

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 the 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 – FLY, référence FQR 110 5322, version 2, Oberthur Technologies. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite – NFC FlyBuy, référence FQR 110 5730, version 1, Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report – Project : FLY, référence FLY_ETR, version 4, Thales-CEACI. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation technical report Lite – Project : FLY, référence FLY_ETR Lite, version 1, Thales-CEACI.
[ANA-CRY]	référence du rapport d'analyse cryptographique de l'ANSSI : - Cotation de mécanismes cryptographiques – Projet FLY, référence 1659/ANSSI/ACE du 29/06/2011, ANSSI
[CONF]	Liste de configuration du produit: - USIM V3.1 Secure PKI on S3FS91J (OX75) - Configuration List, référence FQR 110 5685, version 2 Oberthur Technologies.
[GUIDES]	Guide de préparation du produit : - USIM V3.1 Secure PKI on S3FS91x - AGD_PRE - Delivery Acceptance référence FQR 110 5367, version 2, Oberthur Technologies. Guides d'opération du produit : - USIM V3.1 SECURE PKI ON S3FS91J-OX75 - (APPLICATION DEVELOPMENT GUIDE) référence FQR 110 5569, version 2, Oberthur Technologies. - USIM V3.1 Secure PKI on S3FS91x - (APPLICATION MANAGEMENT GUIDE) référence FQR 110 5570, version 3, Oberthur Technologies. - USIM V3.1 Secure PKI on S3FS91x - Application Security recommandations,

	référence FQR 110 5370, version 3, Oberthur Technologies.
[BSI-PP-0035]	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]	Java Card System Protection Profile - Open Configuration, version 2.6, 19 April 2010. *Profil de protection certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03.*
[PP (U)SIM]	(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations Evolutive Certification Scheme for (U)SIM cards *Profil de protection certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/04*
[ANSSI-CC-NOTE.10]	« Note d'application - Certification d'applications sur "plateformes ouvertes cloisonnantes" », référence ANSSI-CC-NOTE/10.0, voir ssi.gouv.fr
[ANSSI-CC-2009/57]	Certificat ANSSI délivré le 18 mars 2010 sous le titre : « Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7 »

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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[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.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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-CRY]	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, voir www.ssi.gouv.fr