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-2014/47

VMPA 1.4.2 – OT v1.0 sur plateforme NFC FlyBuy Platinum v2.0 sur composant ST33F1ME

Paris, le 7 octobre 2014

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

Guillaume POUPARD
[ORIGNIAL 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-2014/47

Nom du produit

VMPA 1.4.2 – OT v1.0 sur plateforme NFC FlyBuy Platinum V2 sur composant ST33F1ME

Référence/version du produit

VISA Mobile VMPA 1.4.2 v3

Identification hardware 0768910, identification card Manager GOP Ref V1.8.v

Conformité à un profil de protection

néant

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, 92705 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, 92705 Colombes Cedex, France

Centre d'évaluation

THALES (TCS – CNES)

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

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

Préface

La certification

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

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

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

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte « VMPA 1.4.2 – OT v1.0 sur plateforme NFC FlyBuy Platinum v2.0 sur composant ST33F1ME » développée par Oberthur Technologies et STMicroelectronics.

Ce produit est une carte (U)SIM[1] destinée à être insérée dans un téléphone portable disposant de la technologie NFC[2]. Il embarque l'application Mobile PayPass v1.0 qui met en œuvre la solution « Payez Mobile » spécifiée par l'Association Européenne Payez Mobile (AEPM). Cette application permet de réaliser des transactions de paiement sans contact (CMP, *Contactless Mobile Payment*) par radiofréquence.

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.

1.2.2. 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	Mobile VMPA 1.4.2 – OT v1.0 on NFC FlyBuy Platinum V2 on ST33F1ME	Oberthur Technologies
Référence interne de la TOE	Mobile VISA VMPA 1.4.2 – OT v1.0	
Identification Hardware	0768910	
Identification du *Card Manager*	GOP Ref V1.8.v	
Identification de l'applet	Version 03	
Label PVCS pour l'application	VMPA_OT_V01_00_03	
Label PVCS ROM	USIM_V31_NFC_V2_EAL4_CCD2_0768910	
Nom du circuit intégré	ST33F1ME	STMicroelectronics

[1] *Universal Subscriber Identity Module.*
[2] *Near Field Communication*, communication en champ proche.

La version certifiée du produit est identifiable par les éléments détaillés dans la [ST] :

- pour la plateforme :
  - le code article **07689A**, 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 **07 68 9A** 00 82 90 00 ;
  - la version du *Card Manager* en Java Card : « GOP Ref V1.8.v ». Cette valeur est obtenue, en codage ASCII, en réponse à la commande GET DATA 80 CA DF 6C 13 pour *Card Manager Release* (version du *Card Manager*) :
    DF 6C 10 **47 4F 50 20 52 65 66 20 56 31 2E 38 2E 76 2F** 00 ;
  - les données de production du produit **47 50 00 00 82 31 21 02 33 22** :
    - **47 50** = FAB_ID, identifiant de la fonderie du composant sous-jacent (ST Microelectronics) ;
    - **00 00** = IC_ID, identifiant du composant sous-jacent ;
    - **82 31** = OS_ID, identifiant du système d'exploitation ;
    - **21 02** = OS_Release_Date, date d'émission du système d'exploitation ;
    - **33 22** = 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 00 82 31 21 02 33 22** 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 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, SD) avec des privilèges de vérification de *Mandated DAP*. Ces informations sont obtenues via la commande GET STATUS (voir [ANSSI-CC-2012/39] et [GUIDES] pour le détail d'utilisation de cette commande) ;

- pour l'application :
  - les données d'identification de l'application Mobile VISA obtenues en réponse à :
    - la commande SELECT 00 A4 04 00 07 :
      6F 31 84 07 A0 **00 00 00 03 10 10** A5 26 9F 38 1B 9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 9F 4E 14 BF 0C 05 9F 4D 02 14 14 ;
    - la commande GET DATA 80 CA 9F 7E 04 :
      9F 7F 01 **03** ;
  - l'identification de l'application par AID (*Applet IDentifier* – identifiant d'applet):
    - Package VMPA_OT_V01_00_03_0X AID : A000000077 01008501 1000 00 0 x 0003 ;
    - Vmpa Applet Class AID : A000000077 01008501 1000 00 0 x 000356 ;
    - Multi-AccessApplet Class AID : A000000077 01008501 1000 00 0 x 00034D ;
    - Toolkit Applet Class AID : A000000077 01008501 1000 00 0 x 000354 ;

    où « x » est une valeur comprise entre 0 et F utilisée pour attribuer un package à une banque (*Bank ID*). Il y a 16 AID prédéfinis dans la carte, les empreintes SHA1 en hexadécimal de celles-ci considérées dans le cadre de cette évaluation et calculées à partir des fichiers IJC[1], sont fournies ci-dessous.

[1] Fichiers correspondant à des adaptations de fichiers CAP en vue de leur chargement en environnement mobile.

Ijc File Name	Hash value (SHA-1)
VMPA_OT_V01_00_03_00.ijc	E988C294CAF2AA77C56640ECDF06243ED679E356
VMPA_OT_V01_00_03_01.ijc	918A8D56A39A0ADAE6D63B3287DE6B3363829CBE
VMPA_OT_V01_00_03_02.ijc	DDF6FDFEBB30C124E1F8544CC58DF1AD60D3E0DB
VMPA_OT_V01_00_03_03.ijc	AD469F8AFDAEA5CF3D1125A3FABC6BAD11A5EACF
VMPA_OT_V01_00_03_04.ijc	BDE2BEF83708D8CB0CF1586D4DFC876D409C33F6
VMPA_OT_V01_00_03_05.ijc	1F44E84A0AC4D6CD70A394F55A6E47C7471EB259
VMPA_OT_V01_00_03_06.ijc	A3BD2CE79A3670AFEB98693AC2228D2C471E50B1
VMPA_OT_V01_00_03_07.ijc	17A329FFF250D9D1545D38FA2CF25811CCC089DC
VMPA_OT_V01_00_03_08.ijc	A0AF61F4419EBA71F295B28592F55B57DF80195B
VMPA_OT_V01_00_03_09.ijc	1EFF456CF40C0597D6CF07B14007ED6A2C954677
VMPA_OT_V01_00_03_0A.ijc	12364926B0048873F3DD05D23AF486D3184DFF5F
VMPA_OT_V01_00_03_0B.ijc	64B832A79332FD5F6434FD88238E9D55A829F27F
VMPA_OT_V01_00_03_0C.ijc	F081F4C8D33E16EBD827EC438F4073B3A7236730
VMPA_OT_V01_00_03_0D.ijc	1AC916C9559A1B1FB263A77F7BC74CAC3CC010AE
VMPA_OT_V01_00_03_0E.ijc	2AC5412DA0863D46793587781475BA9A6C18E3B9
VMPA_OT_V01_00_03_0F.ijc	FF42425F26DC6815D969C2F1AFEF275629205B23

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- ceux fournis par la plateforme (U)SIM précédemment certifiée, voir [ANSSI-CC-2012/39] ;
- ceux de l'application Mobile VISA VMPA 1.4.2 :
  - la communication hors ligne avec le terminal de paiement (POS, *Point Of Sale*) ;
  - l'authentification hors ligne ;
  - l'authentification en ligne et la communication avec la banque émettrice de la carte ;
  - la vérification et la gestion du code personnel ;
  - l'analyse de la gestion de risque transactionnel ;
  - la certification des transactions ;
  - le traitement de la remise à zéro des compteurs ;
  - le traitement de scripts reçus par OTA (*Over-The-Air*) ;
  - l'audit ;
  - la lecture et la mise à jour des journaux d'audit ;
  - la gestion du cycle de vie sans contact de l'application.

1.2.4. Architecture

Le produit est composé des éléments suivants :

- le microcontrôleur ST33F1M, revision E ;
- 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 aux applications une interface commune 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) ;
- les fonctionnalités (U)SIM qui fournissent toutes les fonctionnalités décrites dans les spécifications ETSI (*European Telecommunications Standards Institute*) 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) ;
- l'application PAP (*Payment Application Package*) correspondant à l'application Mobile VISA VMPA 1.4.2.

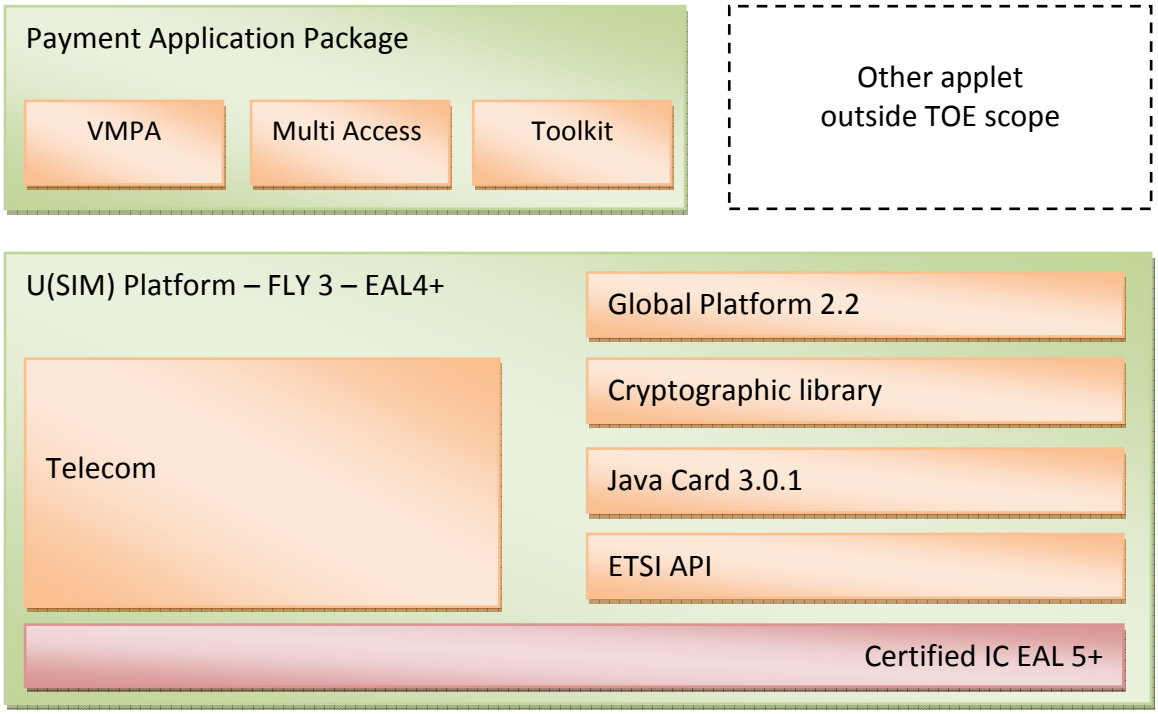

Figure 1 - Architecture et périmètre de la TOE

Le produit peut contenir d'autres applications qui ne font pas partie de la cible d'évaluation.

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

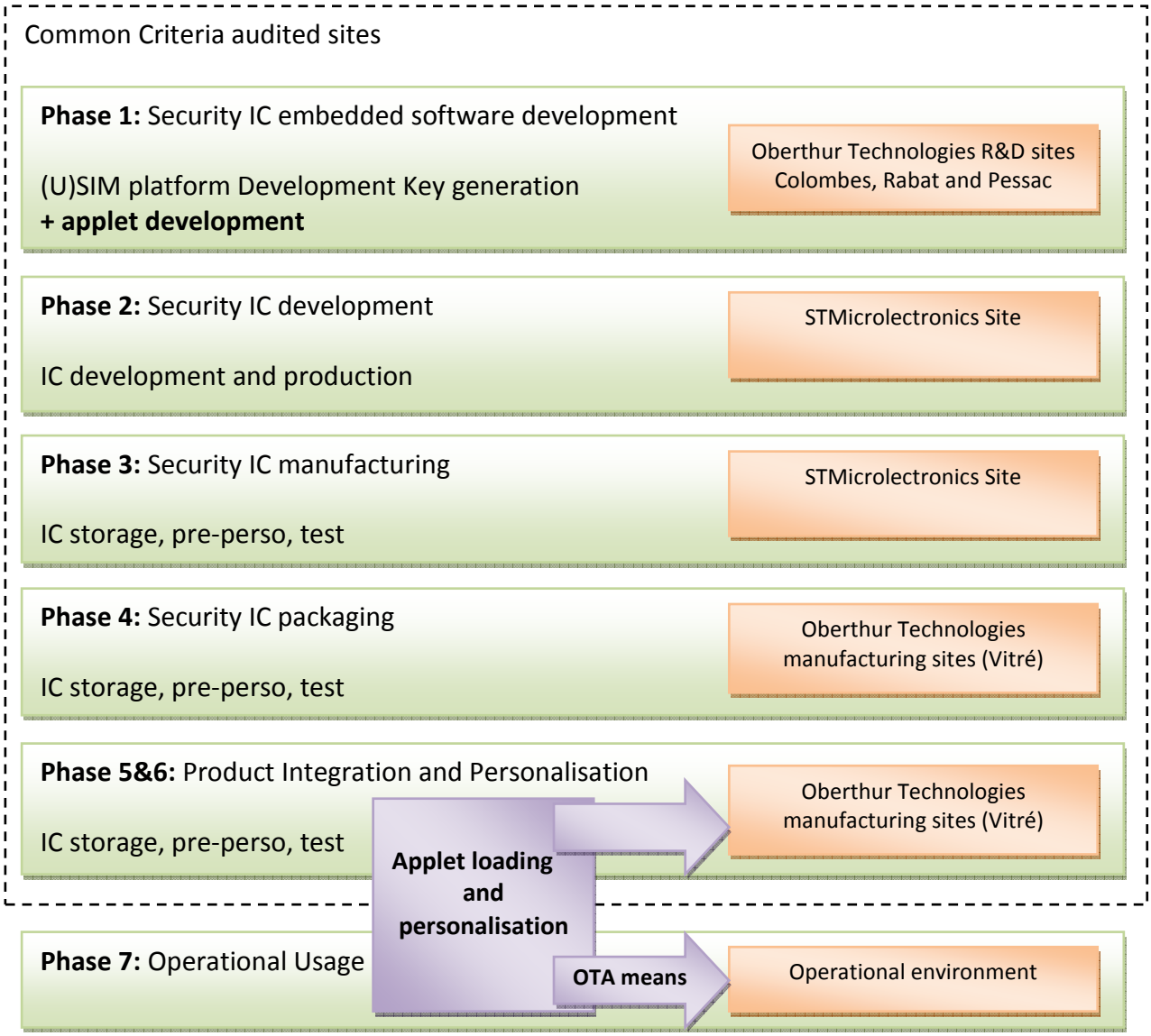

Figure 2 – Cycle de vie de la TOE

Le produit a été développé sur les sites suivant :

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

  420 rue d'Estienne d'Orves
  92700 Colombes
  France

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

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

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

  Batiment 4 – Plateau 202
  11, Complexe de Technopolis
  11100 Sala Al Jadida
  Maroc

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 production du microcontrôleur et de la plateforme sont identifiés dans le rapport de certification [ANSSI-CC-2012/39].

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 (*Mobile Network Operator* – opérateur du réseau mobile, il peut également assumer le rôle 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 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 (*Validation Authority* – autorité de validation).

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

1.2.6. Configuration évaluée

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

La configuration ouverte du produit a été évaluée conformément à [NOTE.10]. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 ne remet pas en cause le présent rapport de certification.

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 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 de la plateforme « NFC FlyBuy Platinum V2 sur composant ST33F1ME » au niveau EAL4 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PPUSIMB]. Cette plateforme a été certifiée sous la référence [ANSSI-CC-2012/39].
Le niveau de résistance de la plateforme a été confirmé le 1er avril 2014 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 18 mars 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 les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF-CRY] 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-2011/07]).

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 « VMPA 1.4.2 – OT v1.0 sur plateforme NFC FlyBuy Platinum v2.0 sur composant ST33F1ME » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 0 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 :

- toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doivent respecter les contraintes de développement de la plateforme (guides [AGD-Dev_Basic] et [AGD-Dev_Sec] selon la sensibilité de l'application considérées ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doit être activée conformément aux indications de [TECH_LOAD] ;
- le chargement des applications *pre-issuance* doit être protégé conformément au guide [ORG_LOAD] ;
- la protection du chargement de toutes les applications chargées *pre-issuance* doit être activée conformément aux indications de [TECH_LOAD].

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 ALCHEMY, VMPA 1.4.2 – OT v1.0 sur plateforme NFC FlyBuy Platinum v2.0 sur composant ST33F1ME », référence FQR 110 6752, Issue 3.0. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Security target - lite ALCHEMY, VMPA 1.4.2 – OT v1.0 sur plateforme NFC FlyBuy Platinum v2.0 sur composant ST33F1ME », référence FQR 110 6951, Issue 1.0.
[RTE]	Rapport technique d'évaluation : - « Evaluation technical report - Project: ALCHEMY », référence ACY_ETR, revision 1.0, 18 mars 2014.
[CONF]	- « Alchemy Configuration list », référence FQR 900 0154, Edition 1.
[GUIDES]	Guides de préparation du produit : - [TECH_LOAD] : USIM V3.1 NFC V2 EAL4+ 768K on CCD2 - AGD_PRE - Delivery Acceptance, référence FQR 110 5884, version 6, Oberthur Technologies ; - [TECH_LOAD] : ALCHEMY PERSONALIZATION MANUAL, référence FQR 900 0141, version 2, Oberthur Technologies ; Guides opérationnel du produit : - [AGD-Dev_Sec] : NFC FlyBuy - Application Security recommandations, référence FQR 110 5886, version 2, Oberthur Technologies ; - [AGD-Dev_Basic] : USIM V3.1 NFC V2 EAL4+ 768K on CCD2 - (APPLICATION DEVELOPMENT GUIDE), référence FQR 110 5885, version 1, Oberthur Technologies ; - [AGD-OPE_VA] : USIM V3.1 NFC V2 EAL4+ 768K on CCD2 - (APPLICATION MANAGEMENT GUIDE), référence FQR 110 5887, version 4, Oberthur Technologies ; - [ORG_LOAD] : ALCHEMY AGD_OPE, référence FQR 900 0140, version 2, Oberthur Technologies.
[PP JCS-O]	SUN Java Card System Protection Profile - Open Configuration, version 2.6, 19 avril 2010. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03.*
[PPUSIMB]	(U)SIM Java Card Platform Protection Profile - Basic and SCWS Configurations (Basic configuration), référence PU-2009-RT-79, version 2.0.2, 17 juin 2010. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/04.*

[ANSSI-CC-2011/07]	Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E avec la bibliothèque cryptographique optionnelle NesLib v3.0. *Certifiés par l'ANSSI sous la référence ANSSI-CC- 2011/07.* *Surveillés par l'ANSSI sous la référence ANSSI-CC-2011/07-S01.*
[ANSSI-CC-2012/39]	NFC FLYBUY PLATINUM V2 sur composant ST33F1ME. *Certifié par l'ANSSI sous la référence ANSSI-CC-2012/39.*
[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.*

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.
[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.
[NOTE.10]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 February 2013.
[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-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.

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