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-2013/65

Application Mobile MasterCard PayPass V1 - M/Chip 4, version V01.00.04, sur plateforme NFC FlyBuy Platinum V2 sur composant ST33F1ME

Paris, le 24 décembre 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-2013/65

Nom du produit

Carte Mobile MasterCard PayPass – M/Chip 4 sur plateforme NFC FlyBuy Platinum V2 sur composant ST33F1ME

Référence/version du produit

MasterCard Mobile PayPass V1 – Version V01.00.04

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 3

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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Identification du produit 6
1.2.3. Services de sécurité 10
1.2.4. Architecture 11
1.2.5. Cycle de vie 12
1.2.6. Configuration évaluée 14

2. L'EVALUATION 15

2.1. REFERENTIELS D'EVALUATION 15
2.2. TRAVAUX D'EVALUATION 15
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 15
2.4. ANALYSE DU GENERATEUR D'ALEAS 15

3. LA CERTIFICATION 16

3.1. CONCLUSION 16
3.2. RESTRICTIONS D'USAGE 16
3.3. RECONNAISSANCE DU CERTIFICAT 17
3.3.1. Reconnaissance européenne (SOG-IS) 17
3.3.2. Reconnaissance internationale critères communs (CCRA) 17

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 18

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 19

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 21

1. Le produit

1.1. Présentation du produit

Le produit évalué est la « Carte Mobile MasterCard PayPass – M/Chip 4 sur plateforme NFC FlyBuy Platinum V2 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 MasterCard PayPass – M/Chip 4 on NFC FlyBuy Platinum V2 on ST33F1ME	Oberthur Technologies
Référence interne de la TOE	MasterCard Mobile PayPass V1 – Version V01.00.04	
Identification Hardware	0768910	
Identification du *Card Manager*	GOP Ref V1.8.v	
Identification de l'applet	0310051100071000	
Label PVCS pour l'application	MC_MOBILE_AEPMR3_APPLET_V01.00.04	
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] au chapitre « 2.3 TOE reference » :

- 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 00 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 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, 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 MasterCard obtenues en réponse à :
    - la commande SELECT 00 A4 04 00 07 :
      6F 1F 84 07 A0 00 00 00 04 10 10 A5 14 50 0A 4D 61 73 74 65 72 43 61 72 64 BF 0C 05 9F 4D 02 0B 0A ;
    - la commande GET DATA 80 CA 9F 7E 00 :
      9F 7F 30 **03 10 05 11 00 07 10 00** A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC AD AE AF B0 B1 B2 B3 B4 C1 C2 C3 C4 C5 C6 C7 CA CB CC CD CE CF D0 D1 D2 D3 D4 ;
  - l'identification de l'application par AID (« *Applet IDentifier* » – identifiant d'applet):
    - Package PayPassMobile : A0000000770100000210040<u>x</u>000051 ;
    - Applet PayPassMobile : A0000000770100000210040<u>x</u>000051 ;
    - Shared PIN package : A0000000770100000210000<u>x</u>000018 ;

    où « <u>x</u> » est une valeur comprise entre 0 et F utilisée pour attribuer un package à une banque. Il y a 16 AID prédéfinis dans la carte, le tableau suivant fournit les empreintes SHA1 et SHA2 en hexadécimal de celles-ci, considérées dans le cadre de cette évaluation, calculées à partir des fichiers IJC[1].

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

Identifiant banque	Package	SHA1	SHA2
00	PayPass Mobile	5B2E292A08C5289C2AE0283564FA211E1AC55065	DC427C7B5E9902ADAC6591987BFEF9765C856BCD43983EB1C2A37C6F93649AE3
	Shared PIN	1C1E92FC63D14D6FF08D80344696D9EEA0D59DC2	EF563D926F4A21AB8985B889FB8663937C9B6A9BA7982490A7D1ACD9AB217E96
01	PayPass Mobile	6931590D5F132539F7B070FE041687E112D7D810	64A01144BF8F27BF509BAA1A3AC50E3D905D37C451816870D1934F46A5630758
	Shared PIN	50DB0CD873BE5BEAADE33FF0F57DDC979EE6A829	909CED7CF65F3C970D96DE81CB3C2A48A579EC57518C578138A495044714DBB1
02	PayPass Mobile	0303B43145C718A8A50A458F49CB924A7E7AB75C	39EDF9D9D4F1B3AB97185470E552331CF7D5E6A96778D191C482B61AAA7FAC5C
	Shared PIN	03CB686880FB22B1BC1EB1F9F8D3D89F33C0BC63	F4F0E3B5A643C7F7AF44F85C2B4EB5CF7C0D9381FDB85E97927277B21D152429
03	PayPass Mobile	C697EBB0C941A9CD625C1D40FCC16D0D7FCD4233	CABF03BF1AE61C51817448AE92E4B8F12349C6CB05F4AA86AAD286E08C4281B0
	Shared PIN	D16E13DD6DC62FB076C8D9DCF78595735C43D142	FF0BF56A3CE7CB0E1AC0B8CDACA5551670974C7578B02C0C832396F58AFCCBB6
04	PayPass Mobile	89B856DE2D2B2339F321F9A2A26E822CAA4F73B9	F6C1E2524204A20BE1EB590F8D46E2CB71D957735D880FFEC32EE0B9F7D05BB2
	Shared PIN	83DB700EC59D7885B7E989E6A1FE36E41FA2C8D4	631A16E014C351149FA0A2A361112E36A4A2E2BA6D37F7C3F2A98A4CDF7DAE9E
05	PayPass Mobile	807A7B11A7CB04709507FE5BE7EC926643EB0A5B	A23964C5CD75CD8F6969EFF9B6583B8AE1A6CA356AD6A458E9692A1DA96EFA68
	Shared PIN	2F50140BD0B49524049857B1C9204F0CD4067137	D4F5D5C16508C3275CC2E85DBCF85DB87B437C179A1AF191125FE4670DC19627
06	PayPass Mobile	DCF750B700972867471CA1EA945DC8B48563491C	BD6356DEDE9D7A826C68E776D44AFFADFEAD4EF65E86E5D32550D6AD102809EA
	Shared PIN	6AE3D94579452B0F84A3E85E1A1CFC78D32E670E	44FBB36DD308E3891281CD478C6AEC41283E6D04EBC0BF08541D1607AFF29544
07	PayPass Mobile	9E2A9B8316BE8256C14917EBED663768E0266E1B	D7F43BE46FEA3FBF10A47672F49ED55AACC093BEB5A1FB6996021EB82314F493
	Shared PIN	15C87D5390553D525B254D55B9AE8200506AB04F	307BFB190918541E97C31673E93612DDD0DB829C8D192634F172272E918DDD98

08	PayPass Mobile	43442FF85C47696A39823F5DE41187EC8E389B3A	BE3216EEB0633A43883324BEFA0AA17AB1E26B44449B71A1E55390A302ABD00B
	Shared PIN	675DD86A0CB2D4ECD0F741B395AC86357CE5028B	4EF5073EAF02D9311685687E2877740A88C8FC180F1EFD1B0EBE6DEBDCE1A88F
09	PayPass Mobile	D9161FAEA3258BECC00AAFFD4B53DE0D4EC15836	FC97BEB25B72B6E20C12FBFC5A78035D856315A5F0863B5C0A58238FA0AFE8D4
	Shared PIN	22FFF693C6DD0949FB283214188ED61C5E72FB2A	1848FC7324230EBAED3B4B9C26EC825E952C9AC26B5A3C96E3DF860871C3B73B
0A	PayPass Mobile	130B991D15275C6627A6336E341588BBE93870BC	3F3B77DC9146FE1074973B8FEBE34EA46C0C765DFBEA45B644DFCE15E0ADD38B
	Shared PIN	1346B5D1F3B1C5EDEDB1861A0F42E04B7AC043F0	7D04D0A242AE734E6EAE5D53FFFCE48AC9BEE1F416A3A900FF3B981FA95FDDE8
0B	PayPass Mobile	1BC2671DDC75E00E4366F50B858129FC4484EAEA	4D7F6E1C60945F3F774866497A968456AF3BC35AAF6EBF5EF6D29384278962A8
	Shared PIN	BD0F2D1C9720573137B8D41023591B9C81FA8AA4	688C18CAC7F8FEDB1887E6FCFC9F2CA8B761721BF30421B540BB3CA8162CD9B3
0C	PayPass Mobile	803DF131808D98CD390D53B723C332A9504CAAC9	259B966B0937C3F1A670BB3609E24A31B38C853674C320606BCEE8AD296B9740
	Shared PIN	2A6038C4F755C2C8AE3F4B30BF98CD67B684E1C5	F251F364D155A0A0C4B546C0A848088F8FA9C78D576E924D0A86B8719E4FDE0C
0D	PayPass Mobile	6B95CD8383E4393B97E2D36E890B3E611CA3D0FC	B56D12214AF98A3DEF8343BB4635A6C05D913AF53960CA85FB69D8ECDF57A05B
	Shared PIN	F188ACDF0DD7051D0A295585657E304633254625	45E3AB0193021E8953327FA84F127E1D6468B3B10AB9B0315848C4164517A08E
0E	PayPass Mobile	CC0B88C2C39E5743F504D2A8638FE9E7F8046681	D26CF97BF8B019D1AA7EA33685721D8C7BC6F45D9BB8B8DFF8F48AC46B08FAB8
	Shared PIN	7D1532466C408E2257B2DA6794955E184AFC3F0E	268B67F425E5E310A9897BF71BE4AEFAAEFC54D33D5D9C8EAED22728CD9EA0E2
0F	PayPass Mobile	44880B19A49111514C4E112AEC5793BF97A2B03D	8A307C39E08E3BB9E426F7BC15F4C132115B8E1FCF5E91ABD0FEFA2DD0C48826
	Shared PIN	D49648273700C6A0D438027FFB7A7A359D211A6A	2A69A6D8B0ABE0E13A5977CDC80D999E944041745D0CA38168E731D4217B43F9

1.2.3. Services de sécurité

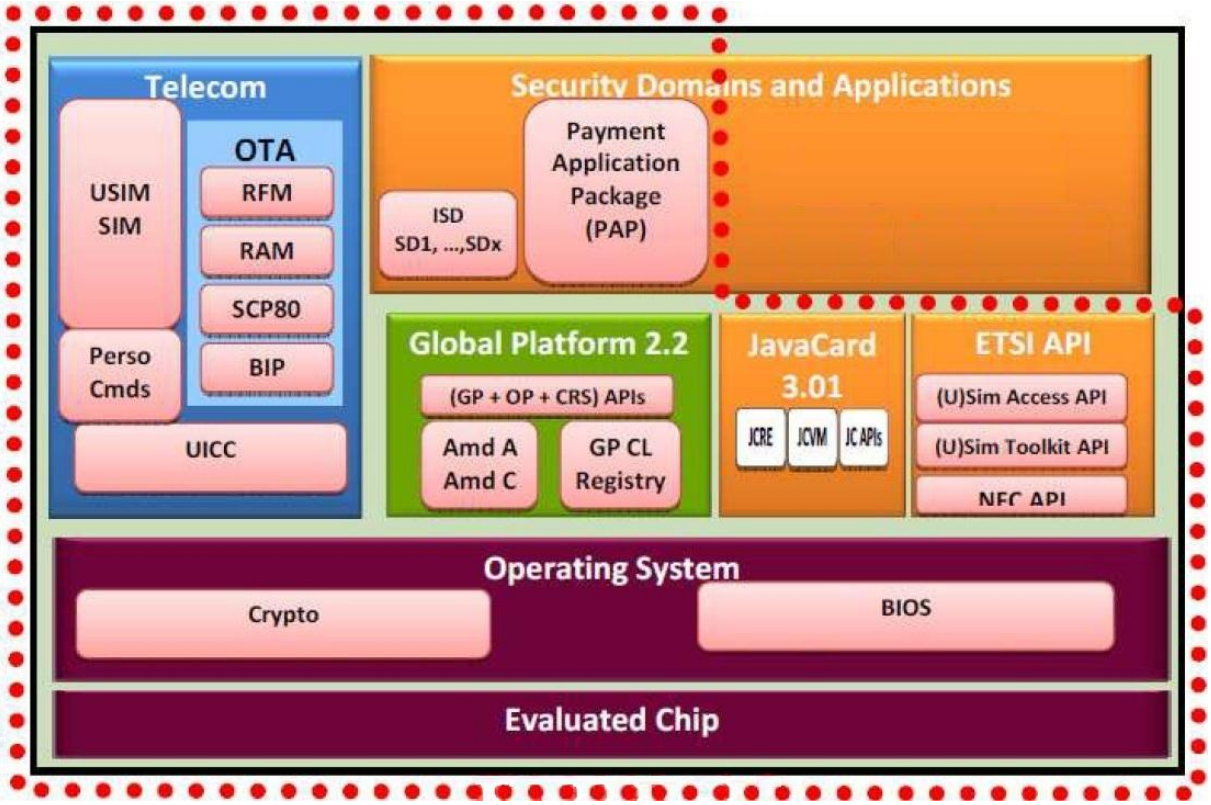
Les principaux services de sécurité fournis par le produit sont :

- ceux fournis par la plateforme (U)SIM précédemment certifiée, voir [ANSSI-CC-2012/39] ;
- ceux de l'application Mobile MasterCard PayPass V1 :
  - 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 :

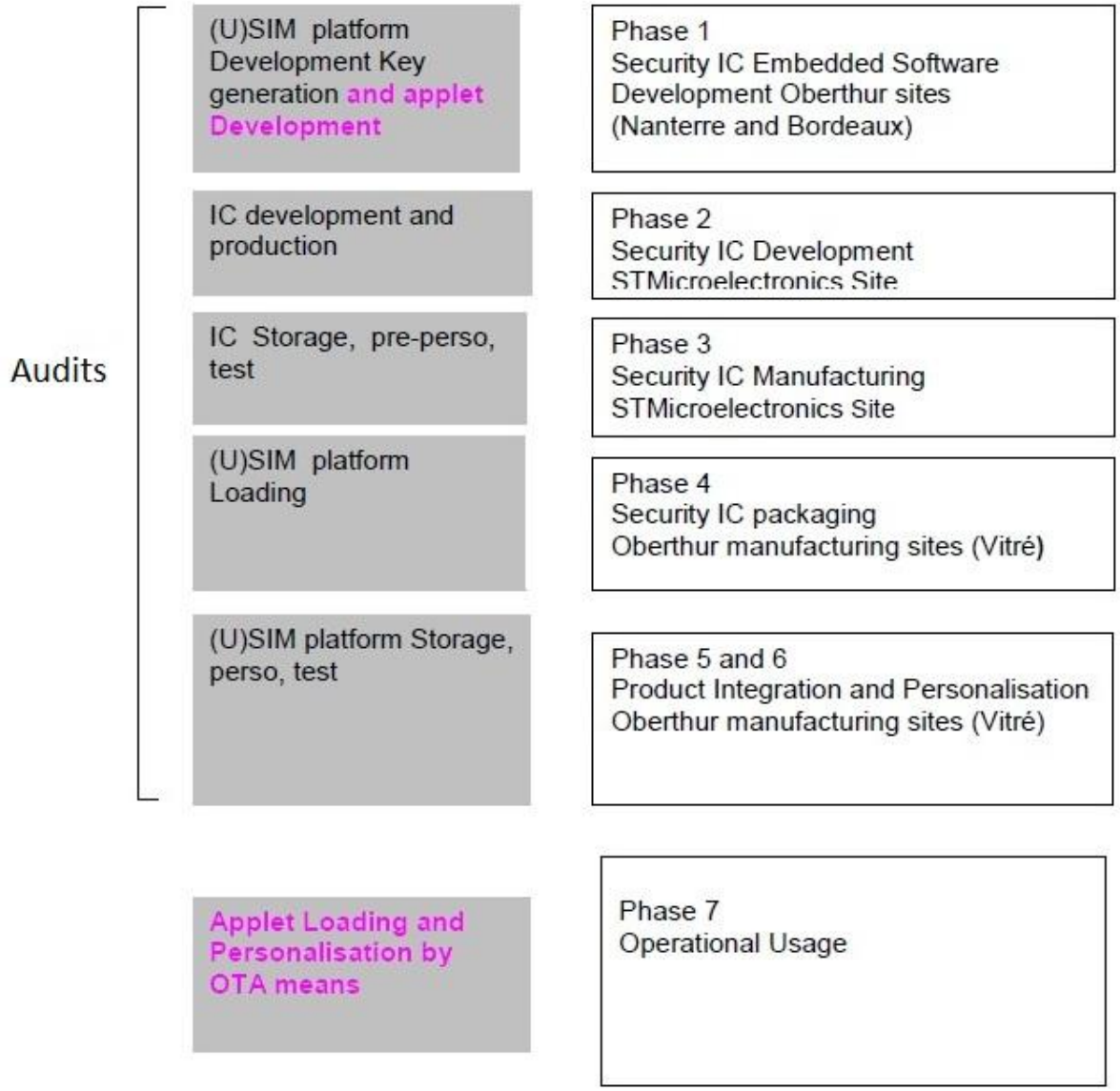
- le microcontrôleur ST33F1M, revision E ;
- un système Java Card, conforme au [PP JCS-O], qui gère et exécute les applications et qui fournit également les interfaces de programmation « Java Card 3.0.1 Classic Edition APIs » permettant de développer ces applications ;
- des packages *GlobalPlatform* (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 MasterCard PayPass –M/Chip 4.



Dans la figure précédente, les pointillés délimitent la cible d'évaluation (TOE, *Target Of Evaluation*). La différence entre le produit et la TOE correspond au fait que 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 :



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 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 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

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 sur la plateforme déjà certifiée 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 rapport technique d'évaluation [RTE], remis à l'ANSSI le 06 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 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 «Carte Mobile MasterCard PayPass – M/Chip 4 sur plateforme NFC FlyBuy Platinum V2 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 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 JUBA, Mobile MasterCard PayPass – M/Chip 4 on NFC FlyBuy Platinum », référence FQR 110 6389, Issue 1.0. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Security target - lite JUBA, Mobile MasterCard PayPass – M/Chip 4 on NFC FlyBuy Platinum », référence FQR 110 6672, Issue 1.0.
[RTE]	Rapport technique d'évaluation : - « Evaluation technical report - Project: JUBA », référence JUB_ETR, revision 2.0, 06 août 2013.
[CONF]	- « Configuration list for AEPMR3 Applet CC », référence FQR 110 6633, Edition 2 ; - « Card configuration for certification », référence FQR 110 6555, Edition 2.
[GUIDES]	Guide de préparation du produit : - USIM V3.1 NFC V2 EAL4+ 768K on CCD2 - AGD_PRE - Delivery Acceptance, référence FQR 110 5884, version 6, Oberthur Technologies ; Guides opérationnel du produit : - [AGD_OPE] : NFC FlyBuy - Application Security recommandations, référence FQR 110 5886, version 2, Oberthur Technologies ; - USIM V3.1 NFC V2 EAL4+ 768K on CCD2 - (APPLICATION DEVELOPMENT GUIDE), référence FQR 110 5885, version 1, Oberthur Technologies ; - USIM V3.1 NFC V2 EAL4+ 768K on CCD2 - (APPLICATION MANAGEMENT GUIDE), référence FQR 110 5887, version 3, 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, 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.
[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, janvier 2012.
[NOTE.10]	« Note d'application - Certification d'applications sur "plateformes ouvertes cloisonnantes" », référence ANSSI-CC-NOTE/10.0, voir www.ssi.gouv.fr.
[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.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, référence CCDB-2009-03-002 version 3.0, revision 1, mars 2009.