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-2013/27

Application Mobile PayPass 1.0 (S1109398, release A) sur plateforme UpTeq NFC2.0.4_OFM sur composant ST33F1ME

Paris, le 29 mai 2013

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

[ORIGINAL SIGNE]

Patrick Pailloux

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-2013/27

Nom du produit (référence/version)

Carte Mobile PayPass 1.0 sur plateforme UpTeq NFC2.0.4_OFM sur composant ST33F1ME

(S1109398/T1020364, version B)

Nom de la TOE (référence/version)

Application Mobile PayPass 1.0 (S1109398, release A) sur plateforme UpTeq NFC2.0.4_OFM sur composant ST33F1ME

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

Gemalto

La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 Rousset, France

Commanditaire

Gemalto

La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat 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 Mobile PayPass 1.0 sur plateforme UpTeq NFC2.0.4_OFM sur composant ST33F1ME - Configuration Bridge AEPM (S1109398/T1020364, version B) » développée par Gemalto 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

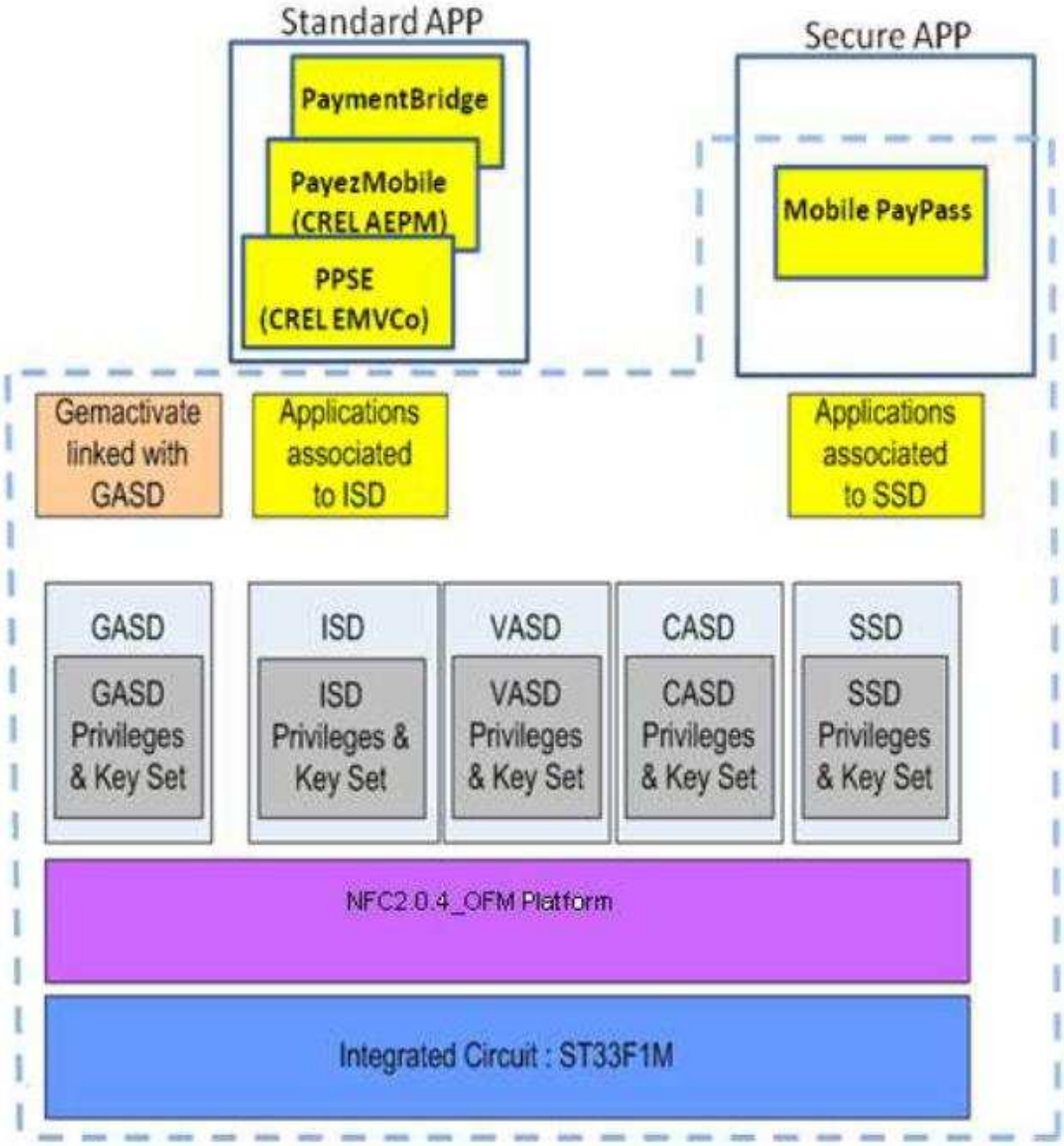
La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Architecture

Le produit est composé des éléments suivants :

- le microcontrôleur ST33F1ME ;
- un système JavaCard qui gère et exécute des applications. Il fournit également des interfaces de programmation (API) pour développer des applications conformes aux spécifications Java Card destinées à être chargées sur ce produit ;
- un package *Global Platform* qui fournit une interface de communication avec la carte à puce et permet de gérer des applications de façon sécurisée ;
- des API plateforme qui fournissent des mécanismes pour interagir avec des applications (U)SIM ;
- un environnement télécom comprenant l'authentification réseau des applications (non évalué) et des protocoles de communication ;
- l'application GemActivate qui permet l'activation de services post-émission[3] ;
- l'application sécuritaire Mobile PayPass v1.0 ;
- les applications standard (également dénommées applications basiques) PaymentBridge v1.0, PayezMobile v1.0 et PPSE v1.0.

[1] *Universal Subscriber Identity Module.*
[2] *Near Field Communication*, communication en champs proche.
[3] Chargement réalisé après la phase 7 du cycle de vie de la carte. Correspond au terme *post-issuance* en anglais.



Dans la figure précédente, les pointillés détourent la cible d'évaluation (TOE, *Target Of Evaluation*). La différence entre le produit et la TOE correspond aux applications standards PaymentBridge v1.0, PayezMobile v1.0 et PPSE v1.0 chargées sur cette carte à puce.
Bien que ces applications standards ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [NOTE.10]. En effet la conformité de ces trois applications standard a été vérifié conformément aux contraintes de développement d'applications décrites dans le rapport de certification [ANSSI-CC-2013/28].

1.2.2. Identification du produit

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

Le tableau suivant fournit les commandes et réponses permettant d'identifier les applications prises en compte dans le cadre de cette évaluation après avoir sélectionné leur AID. Les moyens d'identification des autres composants du produit sont fournis dans le rapport de certification [ANSSI-CC-2013/28].

Application (commande)	**Réponse en ASCII**	**Réponse en chaîne de caractère**
Mobile PayPass v1.0	4D 6F 62 69 6C 65 20 50 61 79 70 61 73 73 20 53 54 4D 30 30 38 20 76 65 72 73 69 6F 6E 20 4D 50 50 76 31 5F 41 45 50 4D 76 33 5F 31 5F 30 5F 62 30 30 32 36 5F 31 31 30 38 32 39 5F 32 31 30 32	Mobile Paypass STM008 version MPPv1_AEPMv3_1_0_b0026_110829_2102
PaymentBridge v1.0	50 61 79 6D 65 6E 74 20 42 72 69 64 67 65 20 53 54 4D 30 30 38 20 76 65 72 73 69 6F 6E 20 4D 50 50 76 31 5F 41 45 50 4D 76 33 5F 31 5F 30 5F 62 30 30 32 36 5F 31 31 30 38 32 39 5F 32 31 30 32	Payment Bridge STM008 version MPPv1_AEPMv3_1_0_b0026_110829_2102
PayezMobile v1.0	43 52 45 4C 20 50 61 79 65 7A 20 4D 6F 62 69 6C 65 20 76 65 72 73 69 6F 6E 20 4D 50 50 76 31 5F 41 45 50 4D 76 33 5F 31 5F 30 5F 62 30 30 32 36 5F 31 31 30 38 32 39 5F 32 31 30 32	CREL Payez Mobile version MPPv1_AEPMv3_1_0_b0026_110829_2102
PPSE v1.0	50 50 53 45 20 41 70 70 6C 69 63 61 74 69 6F 6E 20 4D 50 50 76 31 5F 41 45 50 4D 76 33 5F 31 5F 30 5F 62 30 30 32 37 5F 31 31 31 31 30 39 5F 31 35 35 33	PPSE Application MPPv1_AEPMv3_1_0_b0027_111109_1553

Le tableau suivant fournit les empreintes SHA1 et SHA2 en hexadécimal des applications considérées dans le cadre de cette évaluation, calculées à partir des fichiers IJC[1].

	SHA1	**SHA2**
Mobile PayPass v1.0	68 B4 FF D2 56 63 96 17 F1 F1 69 18 16 76 B0 BC 41 10 9C 0D	83 3C C6 27 3E EB 56 CB D8 9D 7A C5 CA 91 D7 1C F2 2B 60 B1 6B 8E FA 38 CA 2E 75 11 00 86 89 E5
PaymentBridge v1.0	E7 CF D6 59 4F AD C7 39 72 D4 AF 87 9C 4C 8B 26 8A 2E 3D 62	44 3D 61 E3 CA 76 DC D2 CE 09 03 2B 08 C8 58 82 B7 5D 3D B9 A9 61 20 F0 68 E8 2D 85 2F E5 4C BD
PayezMobile v1.0:	40 84 B8 5A 74 4D 56 F6 D6 78 81 EF 28 03 19 DC D8 0D 52 59	82 22 0A 10 17 76 F8 CC 15 16 F3 2C 6B 39 B1 35 9A 7E 44 E1 B1 9F C3 03 4A 8E 5A 70 96 9E 1D 3D
PPSE v1.0	86 E7 AC 1E 72 6C 07 40 87 DA 0E 24 1C E9 85 4F 3D CE 53 DF	14 24 77 60 81 38 69 1A 70 99 C5 4D 80 5E DF 73 A2 AA 91 9F C4 17 A0 BA E1 47 C8 39 55 54 84 DF

1.2.3. Services de sécurité

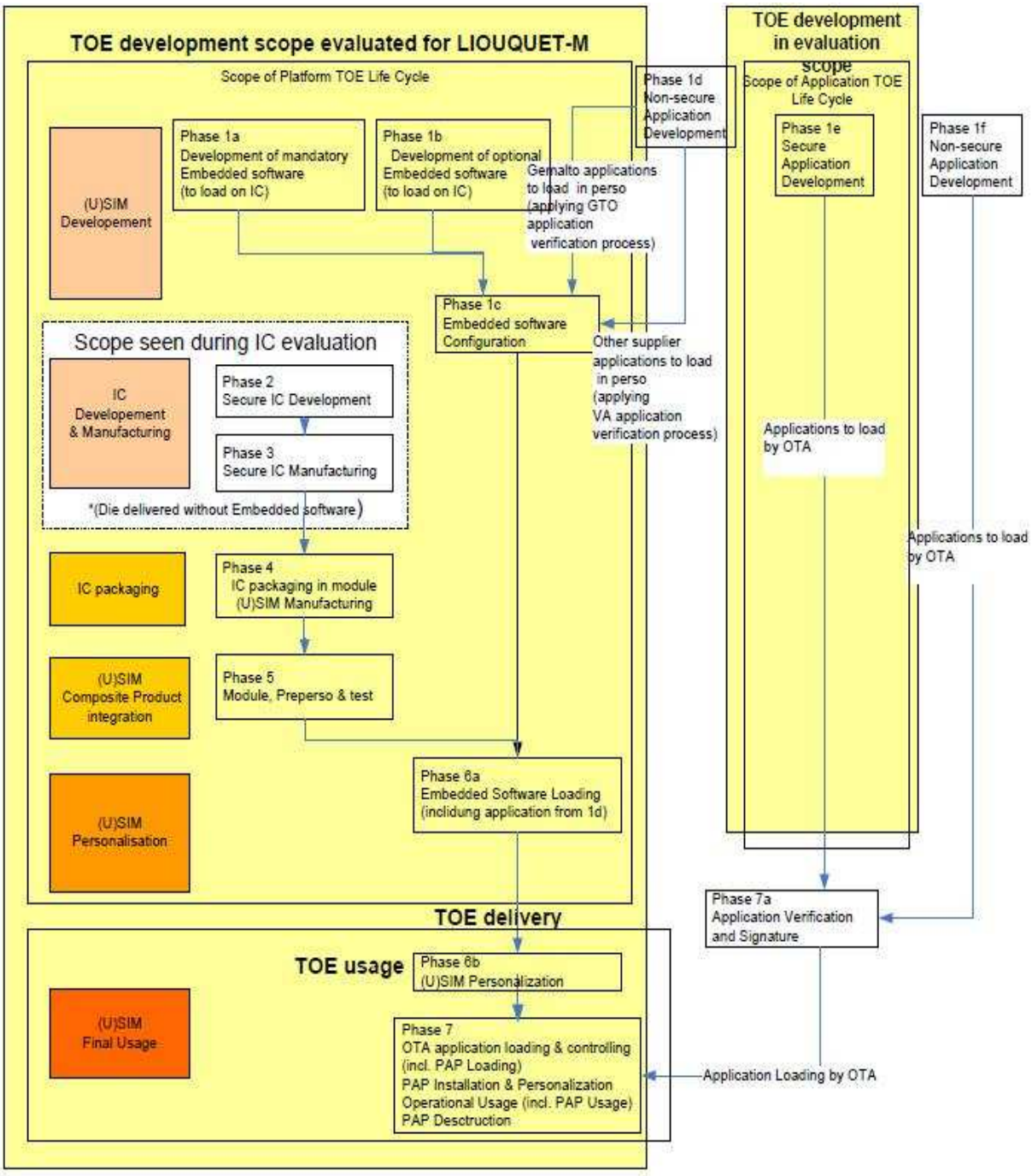
Les principaux services de sécurité fournis par le produit sont :

- ceux fournis par la plateforme (U)SIM précédemment certifiée, voir [ANSSI-CC-2013/28] ;
- ceux de l'application Mobile PayPass v1.0 :
  - 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 ;
  - gestion de risque transactionnel ;
  - la certification des transactions ;
  - le traitement de la remise à zéro des compteurs ;
  - le traitement de scripts reçus par OTA ;
  - 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] Fichiers correspondant à des adaptations de fichiers CAP en vue de leur chargement en environnement mobile.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Les sites de développement et de production du microcontrôleur et de la plateforme sont identifiés dans le rapport de certification [ANSSI-CC-2013/28].

Les applications Mobile PayPass v1.0, PaymentBridge v1.0, PayezMobile v1.0 et PPSE v1.0 ont été développées sur les sites suivants :

Sites Gemalto de développement de l'application

La Vigie
Avenue du Jujubier
ZI Athelia IV
13705 La Ciotat Cedex
France

6, rue de la Verrerie
92197 Meudon Cedex
France

12 Ayar Rajah Crescent
Singapour 139941
Singapour

Les applications standards PaymentBridge, PayezMobile and PPSE peuvent être chargées de deux façons sur cette carte :

- pré-émission[1] (i.e. avant diffusion de la carte à l'utilisateur final) conformément aux processus audités de Gemalto identifiés dans le rapport de certification [ANSSI-CC-2013/28] ;
- ou post-émission à travers le réseau de l'opérateur mobile (chargement via le réseau de communication[2]). Le responsable du processus de chargement doit alors se référer au chapitre 1.2.2 du présent rapport de certification pour vérifier, avant signature de l'application et diffusion aux cartes (U)SIM, que l'application à charger correspond à l'une de celles ayant été vérifiées au cours de cette évaluation.

1.2.5. Configuration évaluée

Le certificat porte sur les configurations suivantes du produit :

- « Carte Mobile PayPass 1.0 sur plateforme UpTeq NFC2.0.4_OFM sur composant ST33F1ME - **Configuration Bridge AEPM**,
  référence S1109398A/ S1121881B Bridge AEPM configuration », qui contient l'application sécuritaire Mobile Paypass v1.0 et les applications standards PaymentBridge v1.0, PayezMobile v1.0 et PPSE v1.0 ;
- « Carte Mobile PayPass 1.0 sur plateforme UpTeq NFC2.0.4_OFM sur composant ST33F1ME - **Configuration Mastercard EMVCo**,
  référence S1109398A/ S1121881B Mastercard EMVCo configuration », qui contient l'application sécuritaire Mobile Paypass v1.0 et l'application standard PPSE v1.0 ;
- « Carte Mobile PayPass 1.0 sur plateforme UpTeq NFC2.0.4_OFM sur composant ST33F1ME - **Configuration AEPM France/WW**,
  référence S1109398A/ S1121881B AEPM France/WW configuration », qui contient

[1] Chargement réalisé avant la phase 7 du cycle de vie de la carte. Correspond au terme *pré-issuance* en anglais.
[2] *Over-The-Air* (OTA).

l'application sécuritaire Mobile Paypass v1.0 et les applications standards PayezMobile v1.0 et PPSE v1.0 ;

- « Carte Mobile PayPass 1.0 sur plateforme UpTeq NFC2.0.4_OFM sur composant ST33F1ME - **Configuration Bridge**,
référence S1109398A/ S1121881B Bridge configuration », qui contient l'application sécuritaire Mobile Paypass v1.0 et les applications standards PaymentBridge v1.0 et PPSE v1.0.

En effet ces quatre configurations du produit ont été prises en compte par le CESTI dans le cadre de cette évaluation.
La configuration ouverte du produit a été évaluée conformément à [NOTE.10] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2, et réalisé selon les processus audités si le chargement est réalisé pré-émission, 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 [CC AP] ont été appliqués. Le niveau VAN est ainsi calculé selon l'échelle de cotation de [CC AP], qui 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 Upteq NFC 2.0.4_OFM release B sur composant ST33F1ME (S1121881, release B) » 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-2013/28].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Carte Mobile PayPass 1.0 sur Orange NFC V2 G1 release B sur composant ST33F1ME - Configuration Bridge AEPM (S1109398/S1105439 Bridge AEPM configuration, release B) » certifié le 30 juillet 2012 sous la référence [ANSSI-CC-2012/49].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 27 mai 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

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 a été étudié dans le cadre de l'évaluation de la plateforme (voir [ANSSI-CC-2013/28]).

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 PayPass 1.0 sur plateforme UpTeq NFC2.0.4_OFM sur composant ST33F1ME - Configuration Bridge AEPM (S1109398/T1020364 Bridge AEPM configuration, version B) » 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 [GUIDES] et [GUIDESptfe]. En particulier :

- les développeurs d'applications additionnelles sur la carte doivent appliquer le guide de développement d'applications basiques [AGD-Dev_Basic] ou le guide de développement d'applications sécurisées [AGD-Dev_Sec], selon la sensibilité des applications concernées ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA].

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_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 - Mobile PayPass 1.0 on UpTeq NFC2.0.4_OFM », référence D1270292, release 1.01. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Security Target - Mobile PayPass 1.0 on UpTeq NFC2.0.4_OFM », référence D1270292, release 1.01p.
[RTE]	Rapport technique d'évaluation : - "Evaluation technical report - Project: ALLEGRO-M », référence ALGM_ETR, revision 3.0.
[CONF]	- « Configuration list 1 », référence LIS_MPP1.0_all___MPP1.0-NFC2.0.4_OFM.txt, release 1.70.1.3 ; - « Configuration list 2 », référence LIS_MPP1.0_delivery___MPP1.0-FC2.0.4_OFM.txt, release 1.9 ; - « Configuration list 3 », référence DAL_MPP1.0-NFC2.0.4_OFM___30-11-2012, release A09.
[GUIDES]	Guide de préparation du produit : - « Mobile Paypass 1.0 on UpTeq NFC2.0.4_OFM - Preparation Guidance », référence D1270296, release 1.01 ; - « Mobile MasterCard Paypass – Card Applications V1.0 - Installation Guide », référence D2148603, version 1.0.0 ; Guides opérationnel du produit : - « Mobile Paypass 1.0 on UpTeq NFC2.0.4_OFM - Guidance for administration", référence D1270295, release 1.01 ; - « Mobile MasterCard Paypass – Card Applications V1.0 - Administration Guide », référence D2148601, version 1.0.0 ; - « Mobile MasterCard Paypass Card Applications V1.0, Developing Client Applications Guide », référence D2148602, version 1.0.0.
[GUIDESptfe]	Guide de préparation de la plateforme: - Guide de réception et d'installation : « UpTeq NFC2.0.4_OFM - Preparation Guidance for Personalization by Morpho », référence D1263509_V13, release 1.3 ; Guides opérationnel du produit : - Guide d'administration : « Guidance for administration of M-NFC 2.0 platform with Controlling Authority and Optional Verification Authority », référence D1224697_w_CA, release 1.3 ; - Annexe au guide d'administration : « Annex of Guidance for

	administration of UpTeq NFC2.0.4_OFM », reference D1263600, release 1.4 ; - Guidance for application development • Guide de développement d'applications basiques [AGD-Dev_Basic]: « Rules for applications on Upteq mNFC certified product », référence D1186227, release A092 ; • Guide de développement d'applications sécuritaires [AGD-Dev_Sec]: « Guidance for secure application development on Upteq mNFC platforms », référence D1188231, release A07 ; - Guide pour l'autorité de vérification [AGD-OPE_VA]: « Guidance for Verification Authority for Orange NFC V2 G1 card », référence D1226483v, release 1.5.
[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-2012/49]	Application Mobile PayPass 1.0 sur plateforme Orange NFC V2 G1 release B sur composant ST33F1ME. *Certifiée par l'ANSSI sous la référence ANSSI-CC- 2012/49.*
[ANSSI-CC-2013/28]	Plateforme Upteq NFC 2.0.4_OFM release B sur composant ST33F1ME (S1121881, release B). *Certifiée par l'ANSSI sous la référence ANSSI-CC- 2013/28.*

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 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.
[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.