



*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-2013/57**

**Application Mobile PayPass 1.0 (S1109398,  
release A) sur plateforme Orange NFC V2 G1  
release B sur composant ST33F1ME,  
configuration MIFARE activé ou configuration  
MIFARE désactivé**

*Paris, le 06 août 2013*

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

Dominique Riban  
[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 présumées 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](mailto:certification.anssi@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

**ANSSI-CC-2013/57**

Nom du produit

**Carte Mobile PayPass 1.0 sur Orange NFC V2 G1 release B sur composant ST33F1ME, configuration MIFARE activé ou configuration MIFARE désactivé - configuration Bridge AEPM version S1109398/S1105439**

Nom de la TOE

**Application Mobile PayPass 1.0 (S1109398, release A) sur plateforme Orange NFC V2 G1 release B sur composant ST33F1ME, configuration MIFARE activé ou configuration MIFARE désactivé**

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



**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](http://www.ssi.gouv.fr).

## Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
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 .....	8
1.2.4. Architecture .....	9
1.2.5. Cycle de vie .....	11
1.2.6. Configuration évaluée .....	12
<b>2. L’EVALUATION .....</b>	<b>14</b>
2.1. REFERENTIELS D’EVALUATION .....	14
2.2. TRAVAUX D’EVALUATION .....	14
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	14
2.4. ANALYSE DU GENERATEUR D’ALEAS .....	14
<b>3. LA CERTIFICATION .....</b>	<b>14</b>
3.1. CONCLUSION .....	15
3.2. RESTRICTIONS D’USAGE .....	15
3.3. RECONNAISSANCE DU CERTIFICAT .....	16
3.3.1. Reconnaissance européenne (SOG-IS) .....	16
3.3.2. Reconnaissance internationale critères communs (CCRA) .....	16
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT .....</b>	<b>17</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>18</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>20</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la « Carte Mobile PayPass 1.0 sur Orange NFC V2 G1 release B sur composant ST33F1ME, configuration MIFARE activé ou configuration MIFARE désactivé - configuration Bridge AEPM version S1109398/S1105439 » développée par Gemalto et STMicroelectronics.

Ce produit est une carte (U)SIM<sup>1</sup> destinée à être insérée dans un téléphone portable disposant de la technologie NFC<sup>2</sup>. 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.

Ce produit est spécifique à l'opérateur de téléphonie mobile Orange.

## 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].

Le tableau suivant fournit les commandes et réponses permettant d'identifier les applications considérées 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-2013/56].

---

<sup>1</sup> *Universal Subscriber Identity Module.*

<sup>2</sup> *Near Field Communication, communication en champs proche.*



Application (commande)	Réponse en ASCII	Réponse en chaîne de caractère
<b>Mobile PayPass v1.0</b> (About APDU 00 AB 00 00 40)	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_b002 6_110829_2102
<b>PaymentBridge v1.0</b> (About APDU 00 AB 00 00 40)	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_b002 6_110829_2102
<b>PayezMobile v1.0</b> (About APDU 00 AB 00 00 3C)	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_b002 6_110829_2102
<b>PPSE v1.0</b> (About APDU 00 AB 00 00 33)	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 30 30 39 5F 31 35 35 33	PPSE Application MPPv1_AEPMv3_1_0_b002 7_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<sup>1</sup>.

	SHA1	SHA2
<b>Mobile PayPass v1.0</b>	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
<b>PaymentBridge v1.0</b>	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
<b>PayezMobile v1.0:</b>	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
<b>PPSE v1.0</b>	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

Pour vérifier que l'application Mifare est activée sur le produit, la réponse à la commande *GetStatus* est la suivante : **A000000184D6966617265410301**.

### 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-2013/56] ;
- ceux de l'application Mobile PayPass v1.0 :
  - o la communication hors ligne avec le terminal de paiement (POS, *Point Of Sale*) ;
  - o l'authentification hors ligne ;
  - o l'authentification en ligne et la communication avec la banque émettrice de la carte ;
  - o la vérification et la gestion du code personnel ;
  - o l'analyse de la gestion de risque transactionnel ;
  - o la certification des transactions ;
  - o le traitement de la remise à zéro des compteurs ;
  - o le traitement de scripts reçus par OTA (*Over-The-Air*) ;
  - o l'audit ;
  - o la lecture et la mise à jour des journaux d'audit ;
  - o la gestion du cycle de vie sans contact de l'application.

<sup>1</sup> Fichiers correspondant à des adaptations de fichiers CAP en vue de leur chargement en environnement mobile.



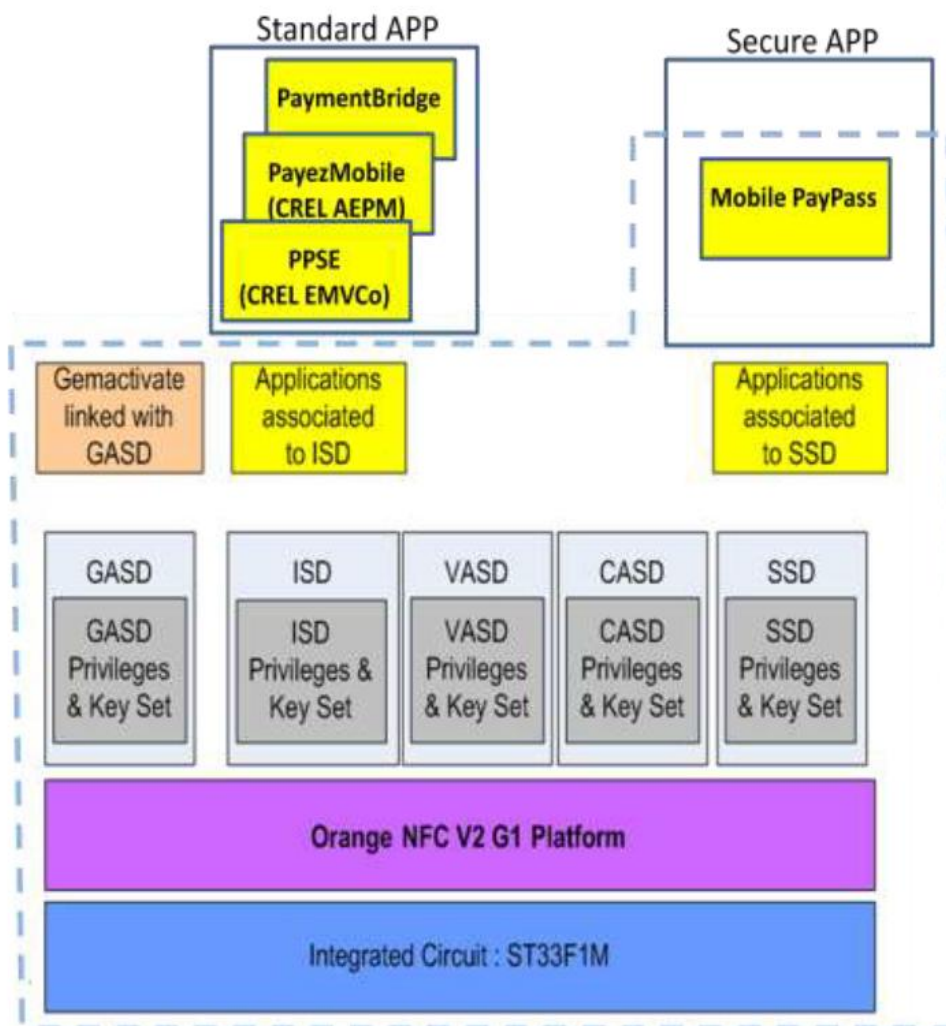
#### **1.2.4. Architecture**

Le produit est composé des éléments suivants :

- le microcontrôleur ST33F1M, revision E ;
- un système JavaCard qui gère et exécute des applications. Il fournit également des interfaces de programmation (APIs) 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 APIs 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<sup>1</sup> ;
- l'application *Mifare Classic* ;
- l'application sécuritaire Mobile PayPass v1.0 ;
- les applications standards (également dénommées applications basiques) PaymentBridge v1.0, PayezMobile v1.0 et PPSE v1.0.

---

<sup>1</sup> Chargement réalisé après la phase 7 du cycle de vie de la carte. Correspond au terme *post-issuance* en anglais.



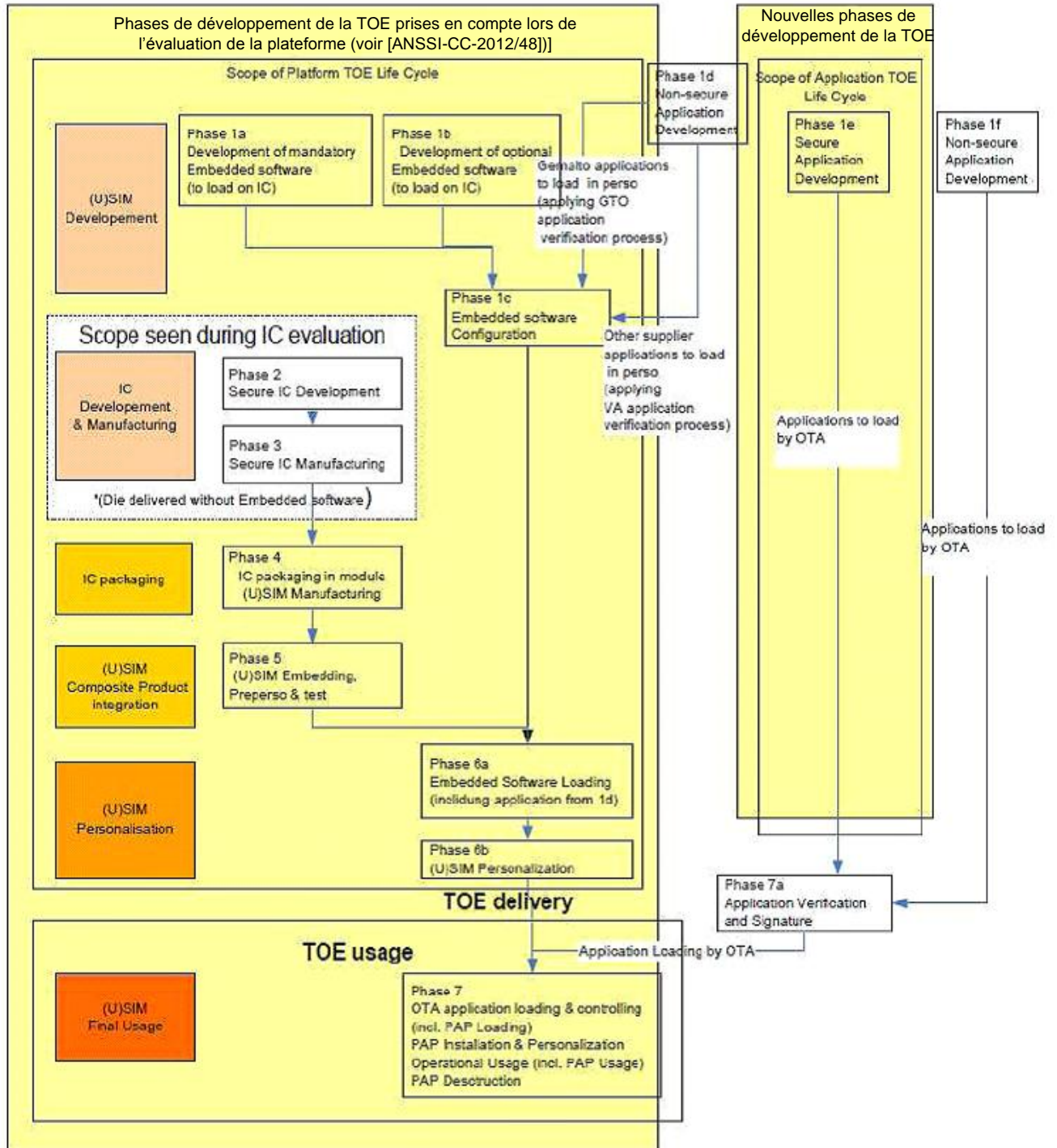
Dans la figure précédente, les pointillés détournent la cible d'évaluation (TOE, *Target Of Evaluation*). La différence entre le produit et la TOE correspond aux applications standards PaymentBridge v1.0, PayezMobile v1.0 et PPSE v1.0 chargées sur cette carte à puce.

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 ces trois applications standards ont été vérifiées conformément aux contraintes de développements d'applications décrites dans le rapport de certification [ANSSI-CC-2013/56].

Les applications embarquées sur ce produit correspondent exactement à celles certifiées dans la précédente version du produit (voir [ANSSI-CC-2012/49]). Seules des modifications de la plateforme précédemment certifiée [ANSSI-CC-2013/56], sans impact sur les applications, ont été réalisées entre les deux versions de la carte à puce.

### 1.2.5. 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-2013/56].

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

#### **Site de développement des applications**

8, 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<sup>1</sup> (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-2013/56] ;
- ou post-émission à travers le réseau de l'opérateur mobile (chargement via le réseau de communication<sup>2</sup>). 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.

#### **1.2.6. Configuration évaluée**

Le certificat porte sur les configurations suivantes du produit :

- « Carte Mobile PayPass 1.0 sur Orange NFC V2 G1 release B sur composant ST33F1ME - Configuration Bridge AEPM, ref. S1109398/S1105439 Bridge AEPM configuration, release B », contenant :
  - o l'application sécuritaire Mobile Paypass v1.0 ;
  - o les applications standards PaymentBridge v1.0, PayezMobile v1.0 et PPSE v1.0.
- « Carte Mobile PayPass 1.0 sur Orange NFC V2 G1 release B sur composant ST33F1ME - Configuration Mastercard EMVCo, ref. S1109398/S1105439 Mastercard EMVCo configuration, release B », contenant :
  - o l'application sécuritaire Mobile Paypass v1.0 ;
  - o l'application standard PPSE v1.0.
- « Carte Mobile PayPass 1.0 sur Orange NFC V2 G1 release B sur composant ST33F1ME - Configuration AEPM France/WW, ref. S1109398/S1105439 AEPM France/WW configuration, release B », contenant :
  - o l'application sécuritaire Mobile Paypass v1.0 ;
  - o les applications standards PayezMobile v1.0 et PPSE v1.0.

<sup>1</sup> Chargement réalisé avant la phase 7 du cycle de vie de la carte. Correspond au terme *pré-issuance* en anglais.

<sup>2</sup> *Over-The-Air* (OTA).



- « Carte Mobile PayPass 1.0 sur Orange NFC V2 G1 release B sur composant ST33F1ME - Configuration Bridge, ref. S1109398/S1105439 Bridge configuration, release B », contenant :
  - l'application sécuritaire Mobile Paypass v1.0 ;
  - 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]. 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 [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 Orange NFC V2 G1 release B-MIFARE activé sur composant ST33F1ME (S1105439 / 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-2013/56].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Carte Mobile PayPass 1.0 sur Orange NFC V2 G1 release B sur composante 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 19 juillet 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 PayPass 1.0 sur Orange NFC V2 G1 release B sur composant ST33F1ME, configuration MIFARE activé ou configuration MIFARE désactivé - configuration Bridge AEPM version S1109398/S1105439 » 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 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<sup>1</sup>, 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<sup>2</sup>, 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 :



<sup>1</sup> 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.

<sup>2</sup> 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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

## Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- « Mobile PayPass 1.0 on Orange NFC V2 G1 with or without MIFARE ACTIVATED - Security Target », référence R0 R21486_001_CCD_ASE, release 2.04.</li> </ul> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> <li>- « Mobile PayPass 1.0 on Orange NFC V2 G1 with or without MIFARE ACTIVATED - Security Target », référence R0 R21486_001_CCD_ASE, release 2.04p.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- "Evaluation technical report - Project: ALLEGRO-OR2 », référence ALL_OR2_RE_ETR, revision 2.0, 30 juillet 2013.</li> </ul>
[CONF]	<ul style="list-style-type: none"> <li>- « Configuration list 1 », référence LIS_MPP1.0_MPPv1_AEPMv3_Orange2__MPPv1_AEPMv3_1_0_CAR, release 1.70 ;</li> <li>- « Configuration list 2 », référence LIS_MPP1.0_MPPv1_AEPMv3_Orange2__MPPv1_AEPMv3_1_0_CAR, release 1.9 ;</li> <li>- « Configuration list 3 », référence R0R21486_001_DAL__25-07-2013.xls, release A08.3.</li> </ul>
[GUIDES]	<p>Guide de préparation du produit :</p> <ul style="list-style-type: none"> <li>- « Mobile Paypass 1.0 Preparation Guidance », référence R0R21486_009_CCD_AGD-PRE, version 2.04 ;</li> <li>- « Mobile MasterCard Paypass – Card Applications V1.0 - Installation Guide », référence D2148603, version 1.0.0 ;</li> </ul> <p>Guides opérationnel du produit :</p> <ul style="list-style-type: none"> <li>- « Mobile Paypass 1.0 Guidance for administration », référence R0R21486_008_CCD_AGD-OPE, version 2.04 ;</li> <li>- « Mobile MasterCard Paypass – Card Applications V1.0 - Administration Guide », référence D2148601, version 1.0.0 ;</li> <li>- « Mobile MasterCard Paypass Card Applications V1.0, Developing Client Applications Guide », référence D2148602, version 1.0.0.</li> </ul>
[GUIDESptfe]	<p>Guide de préparation de la plateforme :</p> <ul style="list-style-type: none"> <li>- Guide de réception et d'installation [AGD-PRE] : « Orange NFC V2 G1 card - Preparation Guidance », référence D1226480, release 1.3 ;</li> </ul> <p>Guides opérationnel du produit de la plateforme :</p> <ul style="list-style-type: none"> <li>- Guide d'administration [AGD-OPE] : « Orange NFC V2 G1 card - Guidance for Administration », référence D1226483, release 1.6.1b ;</li> </ul>



	<ul style="list-style-type: none"> <li>- Guidance for application development                             <ul style="list-style-type: none"> <li>• Guide de développement d'applications basiques [AGD-Dev_Basic]: « Rules for applications on Upteq mNFC certified product », référence D1186227, release A092 ;</li> <li>• Guide de développement d'applications sécuritaires [AGD-Dev_Sec]: « Guidance for secure application development on Upteq mNFC platforms », référence D1188231, release A07 ;</li> </ul> </li> <li>- Guide pour l'autorité de vérification [AGD-OPE_VA]: « Guidance for Verification Authority of Orange NFC V2 G1 card », référence D1226483v, release 1.5.</li> </ul>
[PPUSIMB]	<p>(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.  <i>Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/04.</i></p>
[ANSSI-CC-2011/07]	<p>Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E avec la bibliothèque cryptographique optionnelle NesLib v3.0.  <i>Certifié par l'ANSSI sous la référence ANSSI-CC- 2011/07.</i></p>
[ANSSI-CC-2012/49].	<p>Application Mobile PayPass 1.0 sur plateforme Orange NFC V2 G1 release B sur composant ST33F1ME  <i>Certifiée par l'ANSSI sous la référence ANSSI-CC- 2012/49.</i></p>
[ANSSI-CC-2013/56]	<p>Plateforme Orange NFC V2 G1 release B sur composant ST33F1ME (S1105439 / Release B), configuration MIFARE activé ou configuration MIFARE désactivé  <i>Certifiée par l'ANSSI sous la référence ANSSI-CC- 2013/56.</i></p>

### Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.</p>
[CC]	<p>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.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation :          Evaluation Methodology,          July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.</p>
[JIWG AP]	<p>Joint Interpretation Library - Application of attack potential to smart-cards, version 2.9, janvier 2013.</p>
[COMP]	<p>Joint Interpretation Library - Composite product evaluation for smart cards and similar devices, version 1.2, janvier 2012.</p>
[NOTE.10]	<p>« Note d'application - Certification d'applications sur "plateformes ouvertes cloisonnantes" », référence ANSSI-CC-NOTE/10.0, voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</p>
[SOG-IS]	<p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</p>
[REF-CRY]	<p>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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p>
[CC IC]	<p>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.</p>