



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-2012/48**  
**Plateforme Orange NFC V2 G1 release B sur**  
**composant ST33F1ME**

*Paris, le 30 juillet 2012*

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

Patrick Pailloux  
[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-2012/48**

Nom du produit (référence/version)

**Carte Orange NFC V2 G1 release B sur composant  
ST33F1ME (T1019210 / Release B)**

Nom de la TOE (référence/version)

**Plateforme Orange NFC V2 G1 release B sur composant  
ST33F1ME (S1105439 / Release B)**

Conformité à un profil de protection

**[PPUSIMB], version 2.0.2  
(U)SIM Java Card Platform Protection Profile - Basic  
configuration**

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

<b>Gemalto</b> La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France	<b>STMicroelectronics</b> 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 - CEACI (T3S – CNES)**  
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France  
Tél : +33 (0)5 62 88 28 01 ou 18, mél : nathalie.feyt@thalesgroup.com

Accords de reconnaissance applicables



**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. <i>Identification du produit</i> .....	6
1.2.2. <i>Services de sécurité</i> .....	7
1.2.3. <i>Architecture</i> .....	8
1.2.4. <i>Cycle de vie</i> .....	10
1.2.5. <i>Guides du produit</i> .....	12
1.2.6. <i>Configuration évaluée</i> .....	12
<b>2. L’EVALUATION .....</b>	<b>13</b>
2.1. REFERENTIELS D’EVALUATION.....	13
2.2. TRAVAUX D’EVALUATION .....	13
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	13
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	13
<b>3. LA CERTIFICATION .....</b>	<b>14</b>
3.1. CONCLUSION.....	14
3.2. RESTRICTIONS D’USAGE.....	14
3.3. RECONNAISSANCE DU CERTIFICAT .....	15
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	15
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	15
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>16</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>17</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>19</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la « Carte Orange NFC V2 G1 release B sur composant ST33F1ME, référence T1019210 » développée par Gemalto et STMicroelectronics.

La cible d'évaluation correspond à la plateforme (U)SIM<sup>1</sup> Java Card ouverte embarquée dans cette carte (U)SIM destinée à être insérée dans un téléphone portable ou tout autre équipement téléphonique.

Ce produit permet d'accueillir des applications qui peuvent être chargées et instanciées soit avant diffusion de la carte à l'utilisateur final (chargement pré-émission<sup>2</sup>) soit à travers le réseau de l'opérateur mobile, dans un environnement connecté et sans manipulation physique du produit (chargement post-émission<sup>3</sup>, via le réseau de communication<sup>4</sup>).

## 1.2. Description du produit

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

Cette cible de sécurité est conforme au profil de protection [PPUSIMB]. Cette conformité est de type démontrable.

### 1.2.1. Identification du produit

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

La version certifiée du produit est identifiable par plusieurs moyens décrits dans la documentation du produit [DS] :

- La réponse à la commande *GetData* (0x00 0xCA 0x9F 0x7F) correspond aux informations CPLC<sup>5</sup> suivantes:

Fabricant du microcontrôleur	0x47 0x50 (ST)
Type du microcontrôleur	0x00 0x1A (ST33F1M)
Identifiant de l'OS	0x00 0x08 (STM008)
Date de l'OS	0x20 0x30 (YYDD)
Version de l'OS	0x01 0x18

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

<sup>2</sup> Chargement réalisé avant la phase 7 du cycle de vie de la carte. Correspond au terme *pre-issuance* en anglais.

<sup>3</sup> Chargement réalisé après la phase 7 du cycle de vie de la carte. Correspond au terme *post-issuance* en anglais.

<sup>4</sup> *Over-The-Air* (OTA).

<sup>5</sup> *Card manager Production Life Cycle.*

- La réponse à la commande *GlobalPlatform GetData* du *Card Manager* (0x00 0xCA 0x00 0x66) fournit le Card Recognition Data :

<b>TOE: S1105273 (Product : T1019172)</b>	
Label complet du produit (incluant les outils de développement)	1.47.1.2.1.25
Label du logiciel (retourné par la carte)	<b>1.47.1.2.1.24</b>
Card Recognition Data	06 14 53 54 33 33 46 31 4D 20 <b>01 2F 01 02 01 11 01 2F 01 02 01 18</b>  Label de la précédente version du logiciel (voir [ANSSI-CC-2011/77]) : 0x01, 0x2F, 0x01, 0x02, 0x01, 0x11 Label la version courante du logiciel : 0x01, 0x2F, 0x01, 0x02, 0x01, 0x18

La principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées pré-émission sur cette carte à puce.

Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le document [App\_list] qui liste les applications et les *packages* inclus dans le produit, associés à leurs noms et AID<sup>1</sup>.

La Commande *GetStatus* permet à l'utilisateur du produit de vérifier quelles applications et quels paquetage (*packages*) sont installés dans le produit à leur disposition.

### 1.2.2. Services de sécurité

Les services de sécurité évalués fournis par le produit sont :

- la protection de la confidentialité et de l'intégrité des clés cryptographiques et des données applicatives pendant l'exécution des opérations cryptographiques ;
- la protection de la confidentialité et de l'intégrité des données d'authentification et des données applicatives pendant l'exécution des opérations d'authentification ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications ;
- l'intégrité de l'exécution du code applicatif.

De plus, des services de sécurité relatifs à la gestion des applications sont également fournis par le produit et ont été évalués :

- la délégation de privilèges : le MNO<sup>2</sup>, en tant qu'émetteur de la carte<sup>3</sup>, correspond initialement à l'unique entité autorisée à gérer les applications de la carte (chargement, instanciation, suppression) au travers d'un canal de communication sécurisé avec la carte en phase 7 (phase d'utilisation de la carte, voir chapitre 1.2.4). Cependant le MNO peut céder ce privilège à un fournisseur d'applications<sup>4</sup> à l'aide de la fonctionnalité *Global Platform* de délégation de cette gestion d'applications ;

<sup>1</sup> Application Identifier.

<sup>2</sup> Mobile Network Operator, opérateur mobile.

<sup>3</sup> Card Issuer.

<sup>4</sup> Application Provider (AP).

- la vérification de la signature des applications à charger : la signature par une autorité de vérification<sup>1</sup> (VA) de chaque application à charger est vérifiée par la carte (par le représentant du VA sur la carte) avant la finalisation du processus de chargement de l'application considérée et de son instanciation (*Mandated DAP*) ;
- l'activation de services optionnels : l'activation de ces services est réalisée par OTA sous le contrôle des administrateurs de la fonction GemActivate et du MNO pour les opérations associées au *secure channel* ;
- la gestion de *Security Domain* (SD) : les fournisseurs d'applications disposent de jeux de clés spécifiques et connus d'eux seuls associés à leurs SD. Ces clés leur permettent de s'authentifier auprès de ces SD et d'établir un canal de confiance entre la TOE et un équipement externe.

### 1.2.3. Architecture

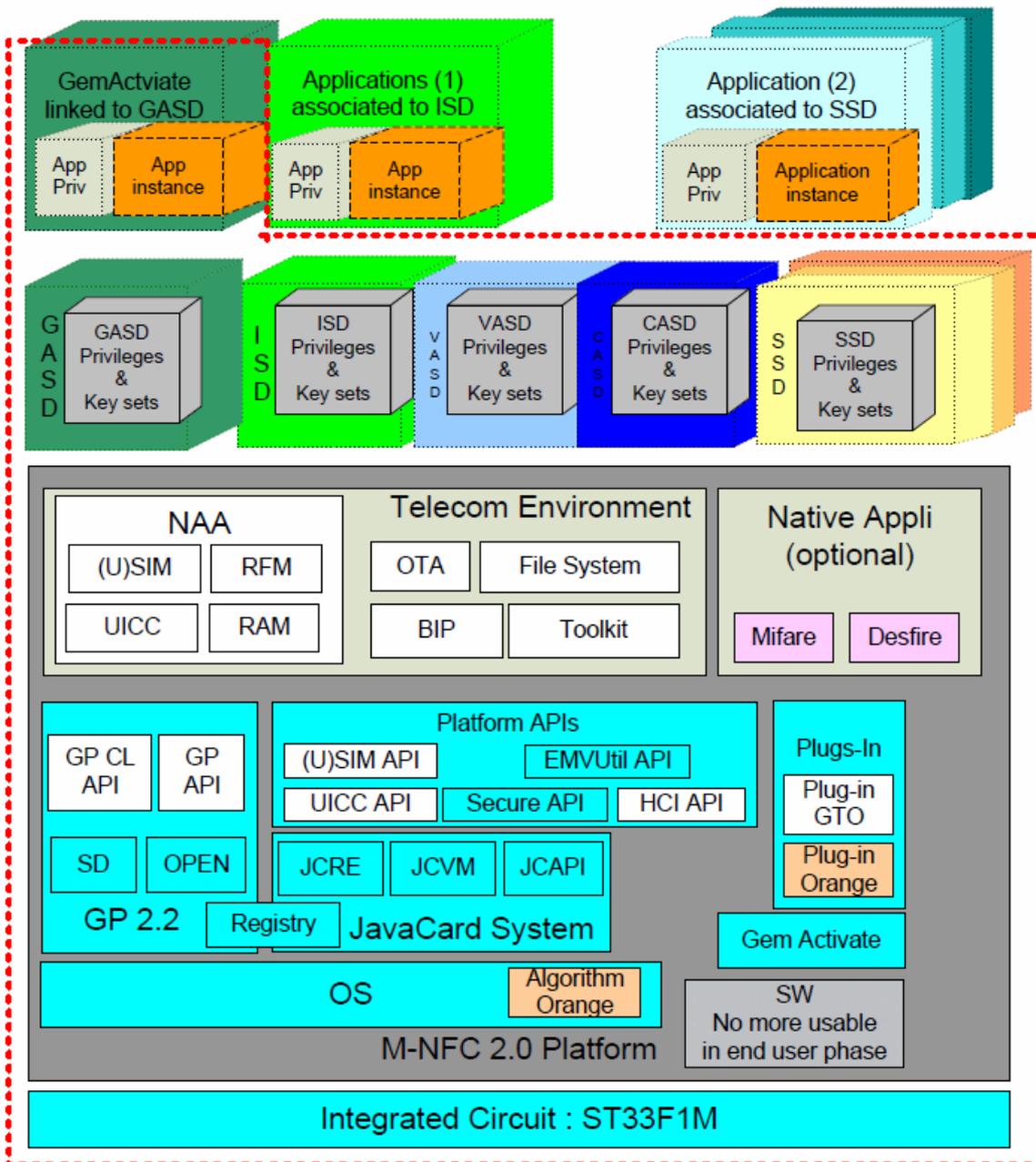
Le produit est composé des éléments suivants :

- le microcontrôleur ST33F1M, revision E ;
- un système JavaCard qui gère et exécute des applications. Il fournit également des interfaces de programmation (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 Télécom ;
- l'application GemActivate qui permet l'activation de services post-émission.

---

<sup>1</sup> *Verification Authority* (VA).

La figure suivante décrit les principaux éléments de la TOE :



(2) : (Standard or Cless) applet

(1) : (2) + Telecom applet +Toolkit applet

**TSF enforcing**

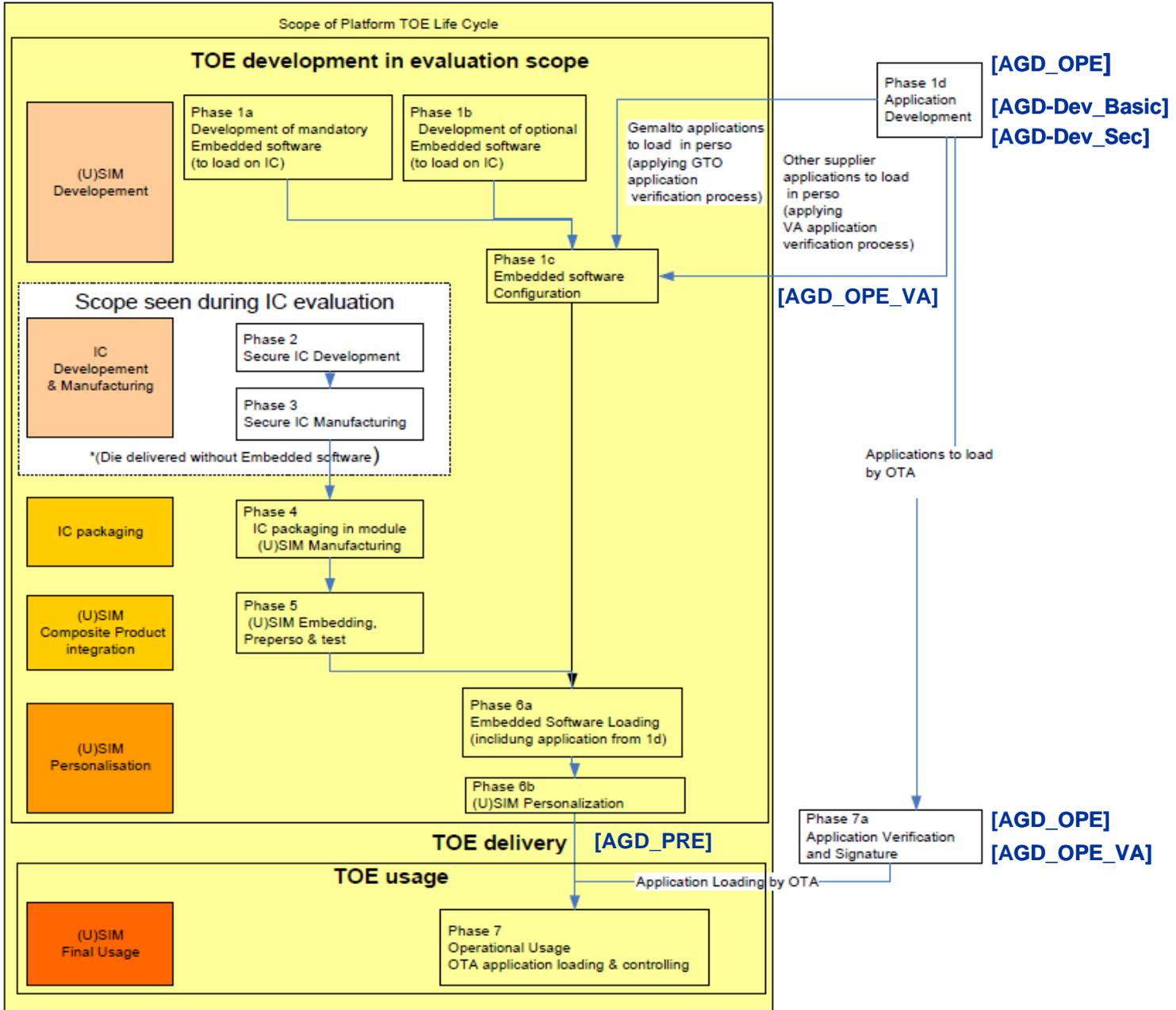
USIM, SIM,UICC, RAM, RFM linked to ISD

Note: l'ISD correspond à l'Issuer Security Domain, le VASD au Verification Authority Security Domain, le CASD au Controlling Authority Security Domain, et le SSD au Supplementary Security Domain.

Comme identifié au chapitre 1.2.4, le produit évalué est personnalisé. La création des Security Domain identifiés dans la figure précédente a été étudiée pendant cette évaluation. Les applications, déjà chargées dans le SSD, sont toutes identifiées dans le document [App\_list].

### 1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :





Le produit a été développé sur les sites suivants :

**Sites de développement du logiciel embarqué**

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

8, rue de la Verrerie  
92197 Meudon Cedex  
France

12 Ayar Rajah Crescent  
Singapour 139941  
Singapour

**Site de configuration du logiciel embarqué**

525, Avenue du Pic de Bretagne  
13420 Gemenos  
France

12 Ayar Rajah Crescent  
Singapour 139941  
Singapour

**Site d'assemblage**

Rue de Saint Ulfrant  
27500 Pont-Audemer  
France

**Site d'encartage, de pré-personnalisation et de personnalisation**

Rue de Saint Ulfrant  
27500 Pont-Audemer  
France

Ul. Skarszewska 2  
33-110 Tczew  
Pologne

Les sites de développement et de fabrication du microcontrôleur sont identifiés dans le rapport de certification [ANSSI-CC-2011/07].

Le développement des applications chargées pré-émission (identifiées dans [App\_list]) a été réalisé sur le site de La Ciotat. Leur livraison et leur vérification ont également été réalisées sur le site de La Ciotat mais par des équipes distinctes de celles les ayant développées. Conformément à [NOTE.10], ces procédures ont été analysées et auditées pendant cette évaluation.

### 1.2.5. Guides du produit

Le cycle de vie du produit évalué correspondant aux phases 1 à 6, le guide de préparation du produit personnalisé [AGD-PRE] est essentiellement dédié à la description des recommandations relatives à la gestion de clés associée aux *Security Domain* VASD, CASD, ISD et APSD.

Le guide opérationnel [AGD-OPE] fournit des recommandations pour chacun des utilisateurs suivants du produit :

- le MNO (opérateur télécom) en sa qualité d'émetteur de la carte ;
- les fournisseurs d'application (*Application Provider*, AP), entité ou institution responsable des applications et de leurs services associés ;
- l'autorité de contrôle (*Controlling Authority*, CA), entité indépendante du MNO représentée sur la carte, responsable de la protection, de la gestion des clés de la carte ainsi que de la personnalisation des *Security Domain* des fournisseurs d'applications (*Application Provider Security Domain*, APSD) ;
- l'autorité de vérification (*Verification Authority*, VA), tierce partie représentée sur la carte, agissant pour le compte du MNO et responsable de la vérification de la signature des applications à chargées ;
- les administrateurs GemActivate, responsable de l'activation post-émission, par le canal de communication OTA, des services optionnels de la plateforme.

[AGD-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs, les guides [AGD-Dev\_Basic] et [AGD-Dev\_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD-OPE-VA] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

### 1.2.6. Configuration évaluée

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 ne remet pas en cause le présent rapport de certification.

Toutes les applications identifiées dans [App\_list] ont été vérifiées conformément aux contraintes décrites dans [AGD-OPE\_VA].

Deux configurations de la plateforme ont été prises en compte dans le cadre de cette évaluation. Ces configurations correspondent aux deux formats de signature utilisés pour le *Delegated Management*, basés sur RSA ou 3DES.

## 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 [JIL AP] ont été appliqués. 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 du microcontrôleur « ST33F1ME » au niveau EAL5 augmenté des composants ALC\_DVS.2, et AVA\_VAN.5, conforme au profil de protection [PP0035]. Ce microcontrôleur a été certifié le 5 avril 2011 sous la référence ANSSI-CC-2011/07 [ANSSI-CC-2011/07].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Plateforme Orange NFC V2 G1 sur composant ST33F1ME » certifié le 23 décembre 2011 sous la référence ANSSI-CC-2011/77 [ANSSI-CC-2011/77].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 4 juin 2012, 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 ni de construction pour le niveau AVA\_VAN visé.

### 2.4. Analyse du générateur d'aléas

Le retraitement de la sortie du générateur matériel du microcontrôleur sous-jacent a été étudié dans le cadre de cette évaluation.

L'évaluation n'a pas mis en évidence de vulnérabilités exploitables pour le niveau AVA\_VAN visé si le guide [AGD-Dev\_Sec] est appliqué.

## 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 Orange NFC V2 G1 release B sur composant ST33F1ME, référence T1019210 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 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 :

- 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
<b>ADV</b> Développement	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	3	Basic modular design
<b>AGD</b> 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
<b>ALC</b> 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
<b>ASE</b> 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
<b>ATE</b> 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
<b>AVA</b> 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]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- « Security Target - Orange NFC V2 G1 card », référence D1226479, release 1.4.</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>- « Security Target - Orange NFC V2 G1 card », référence D1226479, release 1.4p.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- « Evaluation technical report - Project: LIOUQUET OR2 », référence LIOOR2_ETR, révision 3.0.</li> </ul>
[CONF]	<p>Liste de configuration logicielle :</p> <ul style="list-style-type: none"> <li>- « TOE file configuration list », référence ListeFichiersPhenix_1_47_1_3_25 ;</li> </ul> <p>Liste de configuration documentaire :</p> <ul style="list-style-type: none"> <li>- « MNFC20 Document Delivery Status 2012-06-01_V1 », référence MNFC20 Document Delivery Status 2012-06-01_V1 ;</li> </ul> <p>Liste des applications et <i>packages</i> vérifiées [App_list] :</p> <ul style="list-style-type: none"> <li>- pour la configuration avec <i>Delegated Management</i> RSA « Evaluated Electrical Profile Identification description DM RSA2 », référence FTM_N5.CC_v8 - Identification Document v1.1 ;</li> <li>- pour la configuration avec <i>Delegated Management</i> 3DES « Orange NFC v2.0 G1 Certified - DM DES », référence FTM_N5.CC_v7 - Identification Document v1.1.</li> </ul>
[GUIDES]	<p>Guide de préparation :</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 1.2 ;</li> </ul> <p>Guides opérationnel du produit :</p> <ul style="list-style-type: none"> <li>- Guide d'administration [AGD-OPE] : « Orange NFC V2 G1 card - Guidance for Administration », référence D1226483, release 1.5 ;</li> <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]	(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>
[PP0035]	Security IC Platform Protection Profile, version 1.0, 15 juin 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI_PP_0035.</i>
[ANSSI-CC-2011/07]	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>
[ANSSI-CC-2011/77]	Plateforme Orange NFC V2 G1 sur composant ST33F1ME <i>Certifié par l'ANSSI sous la référence ANSSI-CC- 2011/77.</i>

### Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, référence CCDB-2009-03-002 version 3.0, revision 1, mars 2009.
[JIL AP]	Joint Interpretation Library - Application of attack potential to smart-cards, version 2.8, janvier 2012.
[COMP]	Joint Interpretation Library - Composite product evaluation for smart cards and similar devices, version 1.2, janvier 2012.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 dated 26 January 2010 attached to the Référentiel général de sécurité, voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
[NOTE.10]	« 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> .
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, mai 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.