Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

# Rapport de certification ANSSI-CC-2014/56

# Plateforme UpTeq NFC 2.0.4_OFM release B sur composant ST33F1ME (S1121881 / Release B), configuration MIFARE activé ou configuration MIFARE désactivé

*Paris, le 11 août 2014*

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

Contre-amiral Dominique RIBAN
[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-2014/56

*Nom du produit (référence/version)*

## Carte UpTeq NFC 2.0.4_OFM release B, configuration MIFARE activé ou MIFARE désactivé, sur composant ST33F1ME (T1020364/release B)

*Nom de la TOE (référence/version)*

## Plateforme UpTeq NFC 2.0.4_OFM release B sur composant ST33F1ME (S1121881 / Release B), configuration MIFARE activé ou configuration MIFARE désactivé

*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*

### 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 UpTeq NFC 2.0.4_OFM release B, configuration MIFARE activé ou MIFARE désactivé, sur composant ST33F1ME (T1020364/release B) » développée par Gemalto et STMicroelectronics.

La cible d'évaluation correspond à la plateforme (U)SIM[1] Java Card ouverte embarquée dans la 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[2]) soit à travers le réseau de l'opérateur mobile, dans un environnement connecté et sans manipulation physique du produit (chargement post-émission[3], via le réseau de communication[4]).

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

### *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 :

- la réponse à la commande *GetData* (0x00 0xCA 0x9F 0x7F) correspondant aux informations CPLC[5] 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 0x67(YYDD) |
| Version de l'OS | 0x01 0x19 |

[1] *Universal Subscriber Identity Module.*
[2] Chargement réalisé avant la phase 7 du cycle de vie de la carte. Correspond au terme *pre-issuance* en anglais.
[3] Chargement réalisé en phase 7 du cycle de vie de la carte. Correspond au terme *post-issuance* en anglais.
[4] *Over-The-Air* (OTA).
[5] *Card manager Production Life Cycle.*

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

| | **TOE: S1121881** (Product : T1020364, release B) |
|---|---|
| Card Recognition Data | 6661735F06072A864886FC6B01600B06092A864886FC6B02020<br>2630906072A864886FC6B03640B06092A864886FC6B04800064<br>0B06092A864886FC6B0402556622060A2B060104012A036E000<br>10614**5354333346314D20012F01020111012F01020119**[1]<br><br>Nom du composant :<br>0x53, 0x54, 0x33, 0x33, 0x46, 0x31, 0x4D, 0x20 (soit ST33F1M)<br>Release de l'OS :<br>0x01, 0x2F, 0x01, 0x02, 0x01, 0x11 (soit 1.47.1.2.1.17 en décimal)<br>Label du logiciel :<br>0x01, 0x2F, 0x01, 0x02, 0x01, 0x19 (soit 1.47.1.2.1.25 en décimal) |

La principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées en 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[2].
La Commande *GetStatus* permet à l'utilisateur du produit de vérifier quelles applications et quels paquetages (*packages)* sont installés dans le produit à sa disposition.
Pour vérifier que l'application Mifare est activée sur le produit, la réponse à la commande *GetStatus* est la suivante : **A0000000184D6966617265410301**.

### *1.2.3. Services de sécurité*

Les services de sécurité évalués fournis par le produit sont :
- la protection en confidentialité et en intégrité des clés cryptographiques et des données applicatives pendant l'exécution des opérations cryptographiques ;
- la protection en confidentialité et en 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 en confidentialité et en 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[3], en tant qu'émetteur de la carte[4], 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

[1] La signification complète est disponible dans [App_list].
[2] *Application Identifier.*
[3] *Mobile Network Operator, opérateur mobile.*
[4] *Card Issuer.*

MNO peut céder ce privilège à un fournisseur d'applications[1] à l'aide de la fonctionnalité *Global Platform* de délégation de cette gestion d'applications ;

- la vérification de la signature des applications à charger : la signature par une autorité de vérification[2] (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.

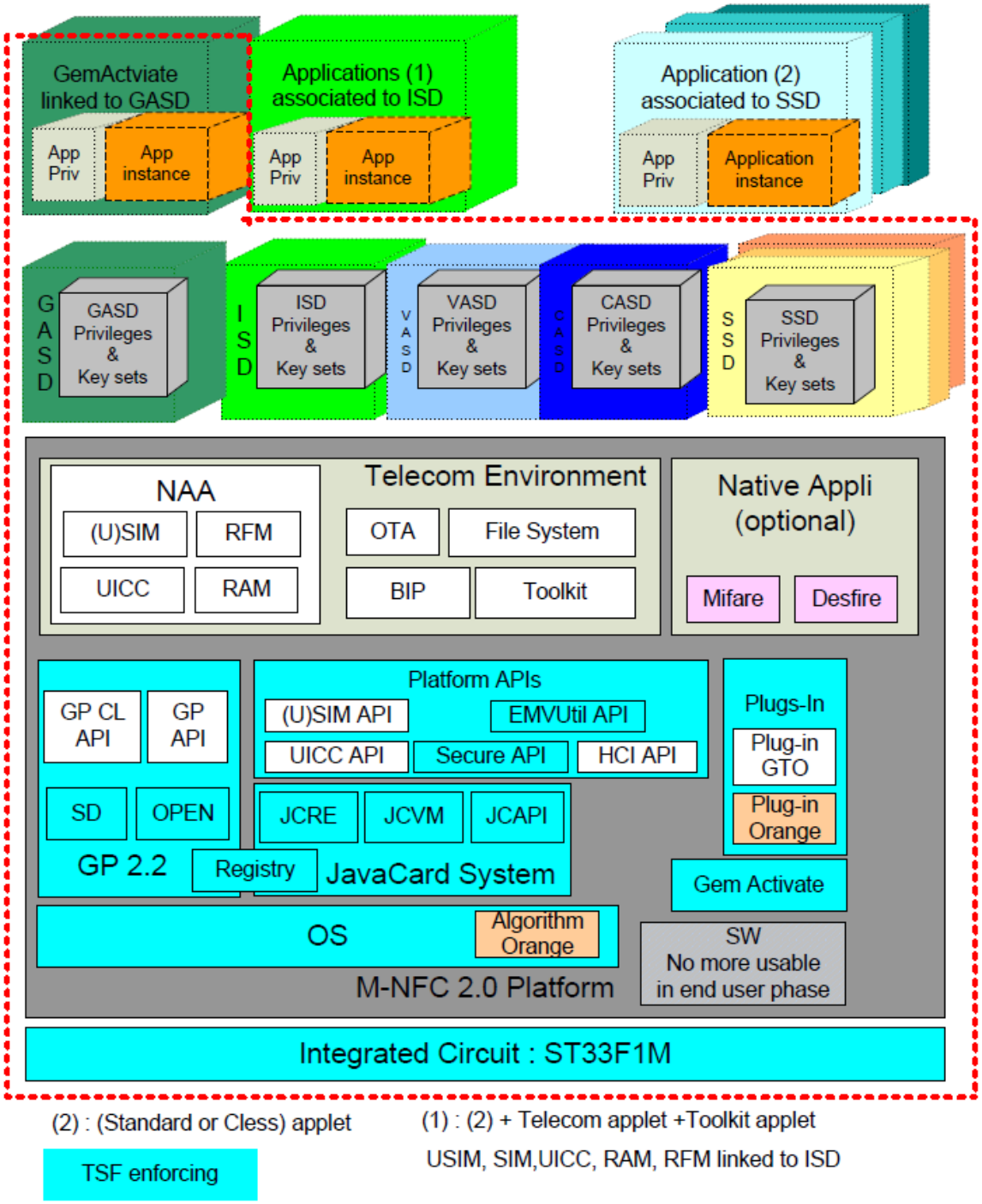
### *1.2.4. Architecture*

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 (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 ;
- l'application *Mifare Classic*.

[1] *Application Provider (AP).*
[2] *Verification Authority (VA).*

La figure suivante décrit les principaux éléments de la TOE :

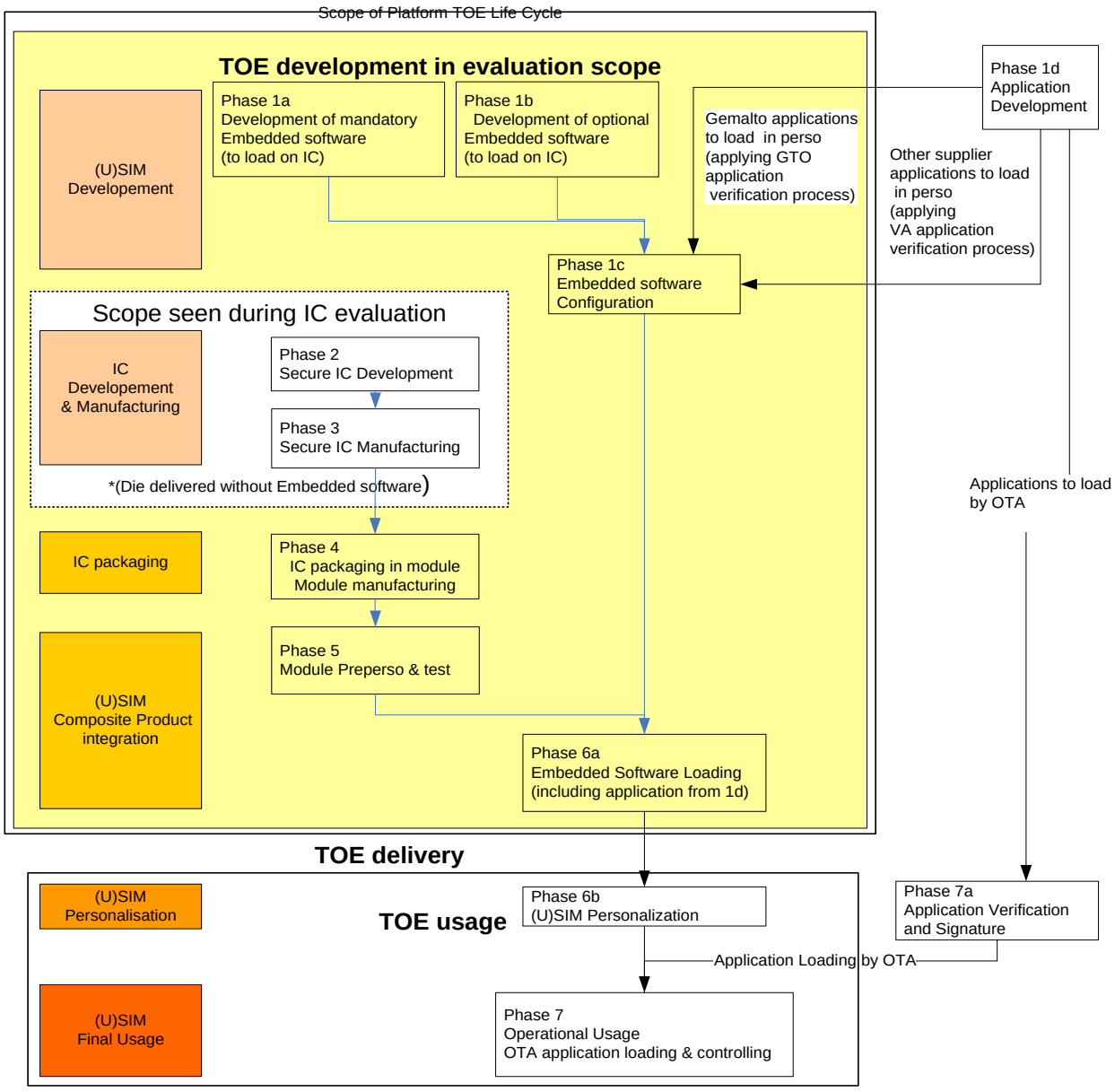



Note : l'ISD correspond à l'*Issuer Security Domain*, le VASD au *Verification Authority Security Domain*, le CASD au *Controlling Authority Security Domain*, et le SSD au *Supplementary Security Domain*.

Comme identifié au chapitre 1.2.5, 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].

### *1.2.5. Cycle de vie*

Le cycle de vie du produit est le suivant :




Le produit a été développé sur les sites Gemalto suivants :

**Sites de développement du logiciel embarqué**

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

**Sites de configuration du logiciel embarqué, d'assemblage et de pré-personnalisation**

525, Avenue du Pic de Bertagne
13420 Gemenos
France

12 Ayar Rajah Crescent
Singapour 139941
Singapour

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.

### *1.2.6. Guides du produit*

Le cycle de vie du produit évalué correspondant aux phases 1 à 6a, 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 Domains* 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'applications (*Application Provider*, AP), entité ou institution responsable des applications et de leurs services associés ;
- l'autorité de contrôle (*Controlling Authorit*y, 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 Authorit*y, VA), tierce partie agissant pour le compte du MNO et responsable de la vérification de la signature des applications à charger ;
- les administrateurs GemActivate, responsables 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.

### *1.2.7. 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, 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 [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

## 2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation 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]. Le niveau de résistance du microcontrôleur a été confirmé le 22 juillet 2014 dans le cadre du processus de surveillance, voir [SUR-IC].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Plateforme UpTeq NFC 2.0.4_OFM release B sur composant ST33F1ME (S1121881, release B) » certifié le 29 mai 2013 sous la référence ANSSI-CC-2013/28 [ANSSI-CC-2013/28].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 août 2014, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

## 2.3. Cotation des mécanismes cryptographiques selon le référentiel technique 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.5 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.5 visé si le guide [AGD-Dev_Sec] est appliqué.

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 UpTeq NFC 2.0.4_OFM release B, configuration MIFARE activé ou MIFARE désactivé, sur composant ST33F1ME (T1020364/release B) » 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[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_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 :<br>- « Security Target: UpTeq NFC 2.0.4_OFM (with or without MIFARE activated) », référence D1255596, release 1.3.<br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>- « Security Target - UpTeq NFC 2.0.4_OFM (with or without MIFARE activated) », référence D1255596, release 1.3p. |
| [RTE] | Rapport technique d'évaluation :<br>- « Evaluation technical report - Project: LIOUQUET_M_RE », référence LIOM_RE_ETR_v2.0, révision 2.0, 6 août 2014. |
| [CONF] | Liste de configuration logicielle :<br>- « NFC_2.0.4_OFM configuration list – projet LIOUQUET & LIOUQUET2 », référence D1273931, release A.2 ;<br>Liste de configuration documentaire :<br>- « MNFC20 Document Delivery Status 2013-07-01_V1 », référence MNFC20 Document Delivery Status 2013-07-01_V1 ;<br>- « Liouquet-M-RE_Deliverables_251113», addendum au document précédent ;<br>Liste des applications et *packages* vérifiées [App_list] :<br>- « Evaluated Electrical Profile Identification description », référence FTM_N8.MO_v8 - Identification Document_GTO v1.4, version 1.4. |
| [GUIDES] | Guide de préparation :<br>- Guide de réception et d'installation [AGD-PRE] : « UpTeq NFC2.0.4_OFM - Preparation Guidance for personalization by Morpho », référence D1263509, release 1.4 ;<br>Guides opérationnels du produit :<br>- Guide d'administration [AGD-OPE] : « Guidance for administration of M-NFC 2.0 platform with Controlling Authority and Optional Verification Authority », référence D1224697_w_CA, release 1.3.2 ;<br>- Annexe au guide d'administration [AGD_OPE-Annex] : « Annex of Guidance for administration of UpTeq NFC2.0.4_OFM », référence D1263600, release 1.4 ;<br>- Guidance for application development<br>• Guide de développement d'applications basiques [AGD-Dev_Basic] : « Rules for applications on Upteq mNFC certified product », référence D1186227, release A092 ;<br>• Guide de développement d'applications sécuritaires [AGD-Dev_Sec] : « Guidance for secure application development on Upteq mNFC platforms », référence D1188231, release A07 ;<br>- Guide pour l'autorité de vérification [AGD-OPE_VA] : |

| | |
|---|---|
| | « Guidance for Verification Authority for Orange NFC V2 G1 card », référence D1226483v, release 1.5 ;<br>- Guide pour la personnalisation : « Personalization User Guide for UpTeq NFC2.0.4_OFM », référence D1262845, release A1.3. |
| [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.<br>*Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/04.* |
| [PP0035] | Security IC Platform Protection Profile, version 1.0, 15 juin 2007.<br>*Certifié par le* BSI *(Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI_PP_0035.* |
| [ANSSI-CC-2011/07] | Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E avec la bibliothèque cryptographique optionnelle NesLib v3.0.<br>*Certifié par l'ANSSI sous la référence ANSSI-CC- 2011/07.* |
| [SUR-IC] | Rapport de surveillance partielle ANSSI-CC-2011/07-S02-P1, Microcontrôleurs sécurisés ST33F1M (sans la libraire Neslib), délivré le 22 juillet 2014. |
| [ANSSI-CC-2013/28] | Plateforme UpTeq NFC 2.0.4_OFM release B sur composant ST33F1ME (S1121881, release B).<br>*Certifié 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 :<br>Part 1: Introduction and general model,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001;<br>Part 2: Security functional components,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002;<br>Part 3: Security assurance components,<br>July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology,<br>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. |
| [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. |
| [REF-CRY] | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20, 26 Janvier 2010, Référentiel général de sécurité, voir www.ssi.gouv.fr. |
| [NOTE.10] | « Note d'application – Certification of open smart card products », référence ANSSI-CC-NOTE/10EN.01deW10. |
| [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. |

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