



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-2012/75

Plateforme M-NFC2.0.3_TUR sur composant ST33F1ME

Paris, le 22 octobre 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

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

Référence du rapport de certification

ANSSI-CC-2012/75

Nom du produit (référence/version)

**Carte M-NFC2.0.3_TUR sur composant ST33F1ME
(T1019850 / Release A)**

Nom de la TOE (référence/version)

**Plateforme M-NFC2.0.3_TUR sur composant ST33F1ME
(S1112312 / Release A)**

Conformité à un profil de protection

**[PP JCS-O], version 2.6
Java Card System Protection Profile - Open 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 - 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.



Table des matières

1. LE PRODUIT	6
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>Configuration évaluée</i>	12
2. L’EVALUATION	13
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
3. LA CERTIFICATION	14
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
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	16
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	17
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	19

1. Le produit

1.1. Présentation du produit

Le produit évalué est la « Carte M-NFC2.0.3_TUR sur composant ST33F1ME, référence T1019850, Release A » développée par Gemalto et STMicroelectronics.

La cible d'évaluation correspond à la plateforme (U)SIM¹ 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 *pre-issuance*) soit à travers le réseau de l'opérateur mobile, dans un environnement connecté et sans manipulation physique du produit (chargement *post-issuance, over-the-air -OTA-*).

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 [PP JCS-O]. Cette conformité est de type démontrable. Des objectifs de sécurité ont été ajoutés à la cible de sécurité [ST] pour traiter les particularités Télécom de ce produit (communications OTA : SMS² et BIP³).

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 *Data Sheet* du produit [DS] :

- La réponse à la commande *GetData* (0x00 0xCA 0x9F 0x7F) correspond aux informations CPLC⁴ 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 0x41 (YYDD)
Version de l'OS	0x01 0x06

¹ *Universal Subscriber Identity Module.*

² *Short Message Service.*

³ *Bearer Independent Protocol.*

⁴ *Card manager Production Life Cycle.*



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

TOE: S112312/release A (Product : T1019850/ release A)	
Label complet de la TOE (incluant les outils de développement)	1.47.1.3.1.22.1.6
Card Recognition Data	<p>66 5D 73 5B 06 07 2A 86 48 86 FC 6B 01 60 0B 06 09 2A 86 48 86 FC 6B 02 02 02 63 09 06 07 2A 86 48 86 FC 6B 03 64 0B 06 09 2A 86 48 86 FC 6B 04 80 00 64 0B 06 09 2A 86 48 86 FC 6B 04 02 55 66 1E 06 0A 2B 06 01 04 01 2A 03 6E 00 01 06 10 53 54 33 33 46 31 4D 20 01 2F 01 03 01 16 01 06</p> <p>Label de la précédente version du logiciel développé par Gemalto (S1105273) : 0x01, 0x2F , 0x01, 0x03, 0x01, 0x16</p> <p>Label de la version courante du logiciel : 0x01, 0x06</p>

Le produit correspond à la TOE (la plateforme) associée aux applications chargées *pre-issuance*¹ sur cette plateforme.

Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans les documents [App_list] qui indiquent les applications et les *packages* inclus dans le produit, associés à leurs noms et AID².

La Commande *GetStatus* permet à l'utilisateur du produit de vérifier quelles applications et quels *packages* sont installés dans le produit à leur disposition. Le label complet du produit correspond à celui de la TOE associés aux AIDs obtenus suite à l'appel de cette commande.

1.2.2. Services de sécurité

Les services de sécurité évalués fournis par le produit sont :

- la confidentialité et de l'intégrité des clés cryptographiques et des données applicatives pendant l'exécution des opérations cryptographiques ;
- 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 ;
- la confidentialité et 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 MNO³, en tant qu'émetteur de la carte⁴, correspond initialement à l'unique entité autorisée à gérer les applications de la carte (chargement, instanciation, suppression) au travers d'un canal de communication sécurisé⁵, avec la

¹ Chargement réalisé avant la phase 7 du cycle de vie de la carte.

² *Application Identifier*.

³ *Mobile Network Operator*, opérateur mobile.

⁴ *Card Issuer*.

⁵ *Secure channel*.

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'applications¹ à l'aide de la fonctionnalité *Global Platform* de délégation de cette gestion d'applications : *Delegated Management*. Dans ce cas le MNO génère un *Token* cryptographique qui sera vérifié par la TOE pour autoriser le chargement de l'application considérée ;

- l'activation de services optionnels par OTA : l'activation de ces services est réalisée par les administrateurs de la fonction GemActivate et les opérations associées au *secure channel* sont réalisées sous le contrôle du MNO ;
- 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.

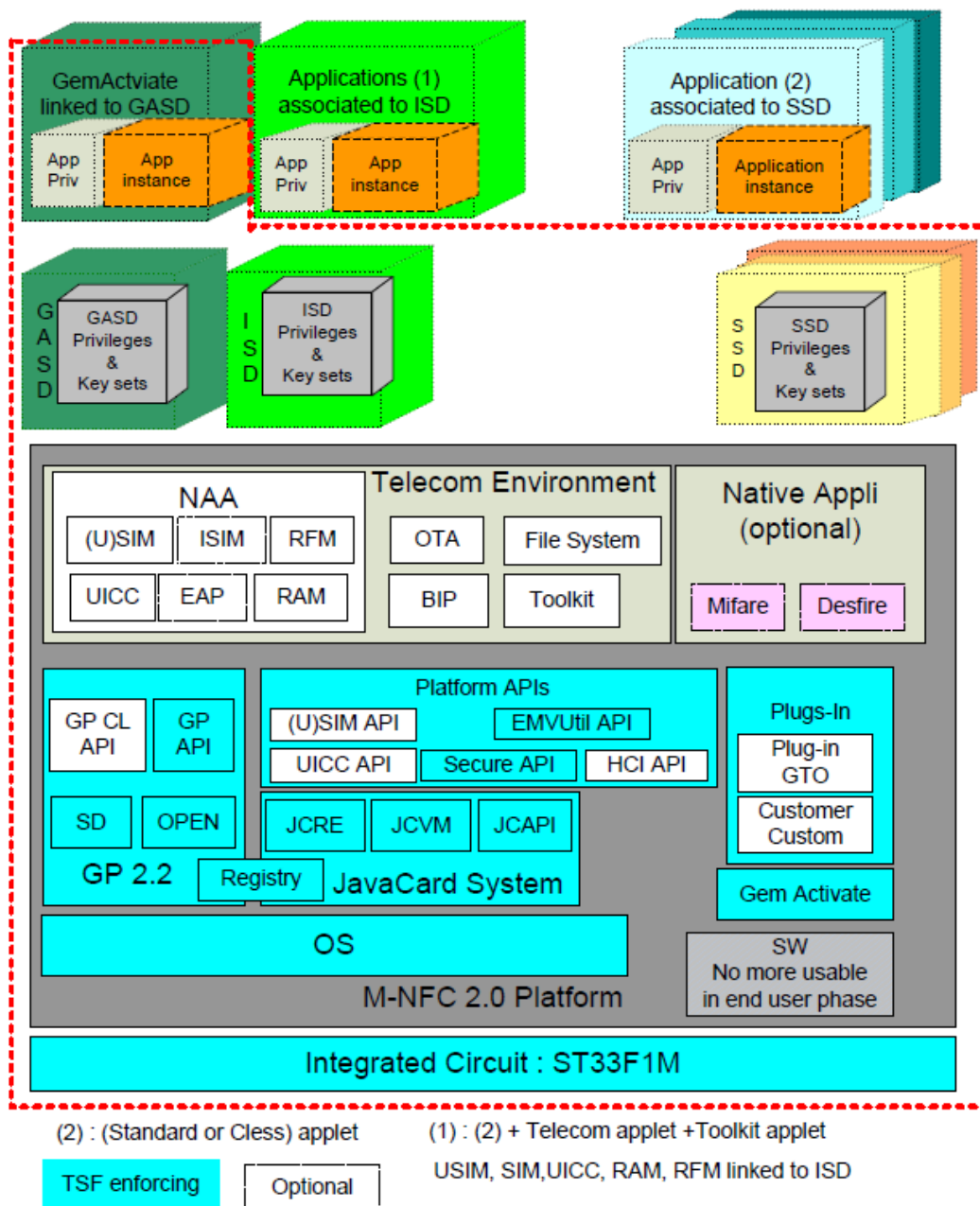
1.2.3. Architecture

La TOE 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-issuance*.

¹ *Application Provider* (AP).

La figure suivante décrit les principaux éléments de la TOE :

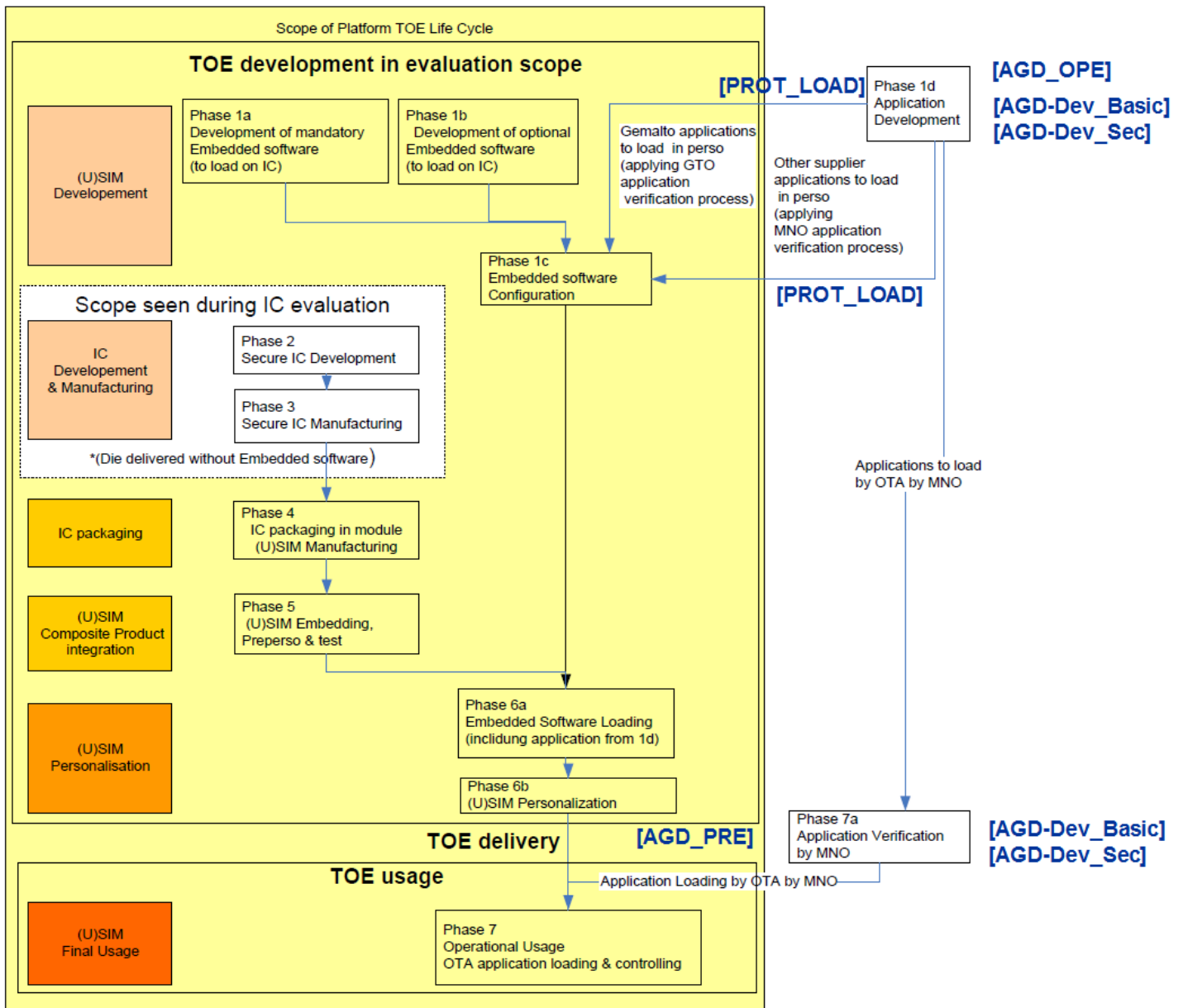


Note: le GASP correspond au *GemActivate Security Domain*, l'ISD à l'*Issuer Security Domain*, et le SSD au *Supplementary Security Domain*.

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 les documents [App_list].

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



La vérification de la conformité au guide de développement [AGD-Dev_Basic] des applications chargées *pre-issuance* développées par Gemalto (identifiées dans [App_list]) est réalisée sur le site de Singapour par des équipes distinctes de celles les ayant développées. Conformément à [NOTE.10], cette vérification a été réalisée pour toutes les applications de [App_list].

La vérification de la conformité aux guides de développement des applications développées par d'autres développeurs que Gemalto est de la responsabilité du MNO.

La protection du chargement *pre-issuance* d'applications, réalisée sur le site de Singapour pour les applications développées par Gemalto et sur le site de La Ciotat pour les autres applications, est décrite dans [PROT_LOAD]. Conformément à [NOTE.10], ce guide a été analysé et sa mise en œuvre a été audité sur les deux sites.



La protection du chargement *post-issuance* d'applications est de la responsabilité du MNO. Les mesures à appliquer pour assurer la protection de ce chargement sont décrites au chapitre 3.2.

Le produit a été développé sur les sites de Gemalto 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

Gemalto s.r.o. BBC Villas,
Zeletavska 1448/7 Praha 4
République Tchèque 140 00

Site de configuration du logiciel embarqué

525, Avenue du Pic de Bretagne
13420 Gemenos
France

Ul. Skarszewska 2
33-110 Tczew
Pologne

Site de *packaging*, 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].

1.2.5. Configuration évaluée

L'évaluateur a disposé des configurations suivantes du produit, qui se distinguent par les applications chargées *pré-issuance* sur la plateforme :

- profil TURKCELL ;
- profil AVEA ;
- profil MAX.

Par ailleurs, deux configurations de la plateforme ont été prises en compte dans le cadre de cette évaluation. Ces configurations correspondent aux deux modes de *Delegated Management* basés sur RSA ou 3DES.

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 question 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 [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].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 16 octobre 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 et 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 « Plateforme M-NFC2.0.3_TUR sur composant ST33F1ME, référence T1019210, release A » 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 ; la conformité à ces guides de développement doit être garantie avant toute activation d'application ;
- pour les applications chargées *pré-issuance*, les mesures organisationnelles décrites dans [PROT_LOAD] doivent être appliquées ;
- pour les applications chargées *post-issuance*, les recommandations de [AGD_OPE] relatives à la protection des mécanismes de *Delegated Management* et *Secure Channel* doivent être mises en œuvre.

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'accord¹, 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 signataires², 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	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 the 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"> - « Security Target - UpTeq NFC 2.0.3_TUR », référence D 1245410, release 1.2. <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"> - « Security Target - UpTeq NFC 2.0.3_TUR », référence D 1245410, release 1.2p.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - « Evaluation technical report - Project: LIOUQUET_T », référence LIOT_ETR, révision 3.0.
[CONF]	<p>Liste de configuration logicielle :</p> <ul style="list-style-type: none"> - « TOE file configuration list », référence DList_Of_File_NFC203_TUR_CM16 ; <p>Liste de configuration documentaire :</p> <ul style="list-style-type: none"> - « MNFC20 Document Delivery Status 2012-06-25_V2 », référence MNFC20 Document Delivery Status 2012-06-25_V2 ; <p>Liste des applications et <i>packages</i> vérifiées [App_list] :</p> <ul style="list-style-type: none"> - pour le profil TURKCELL « Evaluated Electrical Profile - Identification description - mNFC2.0 MPPv1.0 VMPA1.4.1 Mifare Mobile Signature DSTK », référence D1257129, release 2.2 ; - pour le profil AVEA « Evaluated Electrical Profile - Identification description- mNFC2.0 MPPv1.0 Mifare for Mobile, VMPA1.4.1 Wallet DSTK », référence D1257132, release 2.2 ; - pour le profil MAX « Evaluated Electrical Profile Identification-description - Max Profile », référence D1257135, release 2.2.

[GUIDES]	<p>Guide de préparation :</p> <ul style="list-style-type: none"> - Guide de réception et d'installation [AGD-PRE] : « Preparative Guidance for M-NFC 2.0 Platform and Associated Customizations », référence D1247207, release 1.2 ; - Guides de protection du chargement d'application pre-issuance [PROT_LOAD] : « Applet verification process for product profile generation », référence EWB309_001_AVP, release A0. <p>Guides opérationnel du produit :</p> <ul style="list-style-type: none"> - Guide d'administration [AGD-OPE] : <ul style="list-style-type: none"> • « Guidance for administration of M-NFC 2.0 platform without Controlling Authority and optional Verification Authority », référence D1224697 woCA, release 1.2 ; • « Annex of Guidance for administration of UpTeq NFC2.0.3_TUR » référence D1247209, release 1.2 ; - Guides de développement d'applications : <ul style="list-style-type: none"> • 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.
[PP JCS-O]	<p>Java Card System Protection Profile - Open Configuration, version 2.6, 19 avril 2010. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03.</i></p>
[PP0035]	<p>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></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>

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, cf. www.ssi.gouv.fr
[NOTE.10]	« Note d'application - Certification d'applications sur "plateformes ouvertes cloisonnantes" », référence ANSSI-CC-NOTE/10.0, voir ssi.gouv.fr
[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.