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-2016/22

Carte UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F

Paris, le 23 mai 2016

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

Guillaume POUPARD
[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 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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2016/22

Nom du produit

Carte UpTeq NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F

Référence/version du produit

T1032507, Release A

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 4

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

Serma Safety & Security
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL2.

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 NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F **(**T1032507, Release A) » développée par Gemalto et STMicroelectronics.

Ce produit est une plateforme (U)SIM[1] Java Card ouverte embarquée dans un micro-module destiné à être inséré 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 comme suit :
La réponse à la commande *GetData* (tag 0x00FE) correspondant aux informations CPLC[5] suivantes : 06 0a 2b 06 01 04 01 2a 02 6e 01 03 06 09 d0 02 1a 12 ab 41 56 cc 01 90 00

Version JavaCard	06 0a 2b 06 01 04 01 2a 02 6e 01 03
*Hard Mask (*ST33G1M2)	d0 02 1a
*Flash Mask (*NFC3.2.2_Generic v1.0)	12 ab
Mode (CC Card)	41 56 cc 01

[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 après la 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 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 paquetages (*packages)* inclus dans le produit, associés à leurs noms et AID[1].
La commande *GetStatus* permet à l'utilisateur du produit de vérifier quelles applications et quels *packages* sont installés dans le produit à sa disposition.

1.2.3. Services de sécurité

Les principaux services de sécurité 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 ;
- la protection du chargement d'applications *post-issuance* ;
- 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[2], en tant qu'émetteur de la carte[3], 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[4] 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[5] (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] *Application Identifier.*
[2] *Mobile Network Operator, opérateur mobile.*
[3] *Card Issuer.*
[4] *Application Provider (AP).*
[5] *Verification Authority (VA).*

1.2.4. Architecture

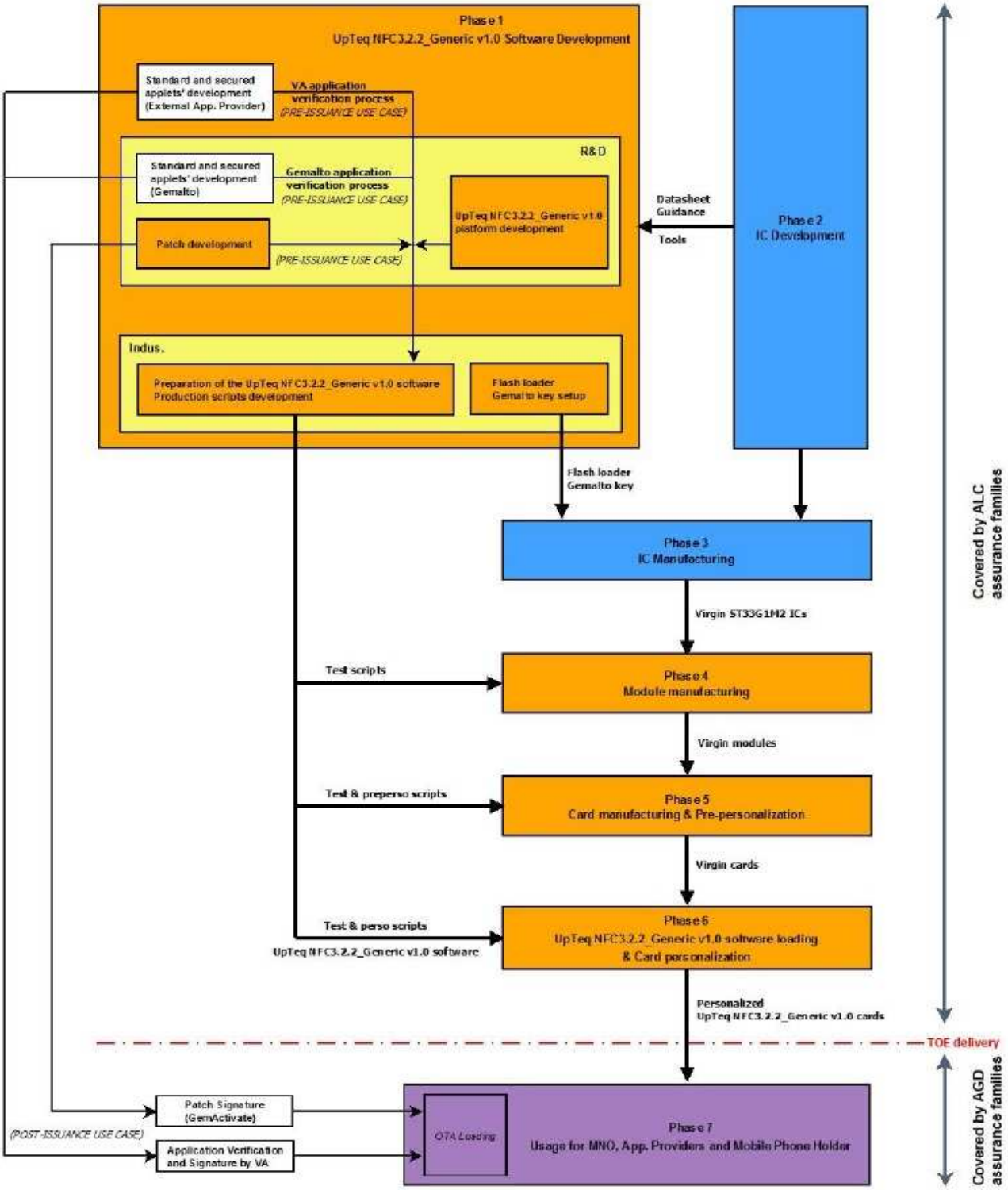
Le produit est composé des éléments suivants :

- le microcontrôleur ST33G1M2, révision F ;
- 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 ;
- les applications MIFARE DESFire EV1 et MIFARE for MOBILE v2, hors de la TOE.

Les applications déjà chargées dans le produit sont toutes identifiées dans le document [App_list].
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 [OPEN]. En effet, ces applications standards ont été vérifiées conformément aux contraintes de développements d'applications décrites dans le guide [AGD-Dev_Basic].

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :



Les sites Gemalto de développement et de fabrication du produit sont les suivants :

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

12 Ayar Rajah Crescent
Singapour 139941
Singapour

525, Avenue du Pic de Bertagne
13420 Gemenos
France

Ul. Skarszewska 2
33-110 Tczew
Pologne

Rue de Saint Ulfrant
27500 Pont-Audemer
France

Rodovia Dep. Leopoldo Jacomel,
13102
83323-410 – Pinhais – PR
Brazil

Les sites de développement et de fabrication du microcontrôleur sont identifiés dans le rapport de certification [ANSSI-CC-2014/46].

Le guide [AGD-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.
Par ailleurs, les guides [AGD_APP], [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.

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 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 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.

1.2.6. Configuration évaluée

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification 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].

Quatre configurations de la plateforme ont été prises en compte dans le cadre de cette évaluation. Ces configurations correspondent aux quatre formats de signature utilisés pour le *Delegated Management*, basés sur les algorithmes RSA, AES, ECC ou DES.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour répondre aux spécificités des cartes à puce, les guides [JIWG 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 « ST33G1M2 révision F » 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 21 juillet 2014 sous la référence ANSSI-CC-2014/46 [ANSSI-CC-2014/46]. Le niveau de résistance du microcontrôleur a été confirmé le 22 octobre 2015 dans le cadre du processus de surveillance, voir [SUR-IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 13 mai 2016 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.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 les guides [AGD-Dev_Sec] et [AGD-Dev_Basic] sont appliqués.
Le générateur d'aléas utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [ANSSI-CC-2014/46]).

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 NFC3.2.2_Generic v1.0 sur composant ST33G1M2-F, T1032507, 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 [AGD_APP] ainsi que 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 EAL2 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, 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 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 : - « UpTeq NFC3.2.2_Generic v1.0 USIM Platform – Security Target », référence D1350235, release 1.0. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « UpTeq NFC3.2.2_Generic v1.0 USIM Platform – Security Target Public version », référence D1350235p, release 1.0.
[RTE]	Rapport technique d'évaluation : - « Evaluation technical report – RIGEL Project », référence RIGEL_ETR_PTF_v1.3, version 1.3, 13 mai 2016.
[CONF]	Liste de configuration - « LIS_NFC322-Generic__1-21-1-25 », 12 novembre 2015. Liste des applications et *packages* vérifiées [App_list] : - Profile name: Max AES, reference : « D1349732_ProfileDescription_MaxAES v1.1 for UpTeq NFC 3.2.2_Generic v1.0 » - Profile name: Max DES, reference : « D1349732_ProfileDescription_MaxDES v1.1 for UpTeq NFC 3.2.2_Generic v1.0 » - Profile name: Max DES with POR Custom, reference : « D1349732_ProfileDescription_MaxDESPorCustom v1.1 for UpTeq NFC 3.2.2_Generic v1.0 » - Profile name: Max ECC, reference : « D1349732_ProfileDescription_MaxECC v1.1 for UpTeq NFC 3.2.2_Generic v1.0 »; - Profile name: Max RSA, reference : « D1349732_ProfileDescription_MaxRSA v1.1 for UpTeq NFC 3.2.2_Generic v1.0 »; - Profile name: Min CC, reference : « D1349732_ProfileDescription_MinCC v1.1 for UpTeq NFC 3.2.2_Generic v1.0 »
[GUIDES]	Guide de préparation : - Guide de réception et d'installation [AGD-PRE] : « UpTeq NFC3.X platform – Preparation Guidance », référence D1351549, release 1.1 ; Guides opérationnels du produit : - Guides d'administration [AGD-OPE] : • « Guidance for administration of Upteq NFC 3.X platform with Controlling Authority and Optional Verification Authority », référence D1341170_w_CA, release 1.1 ; • « Guidance for administration of Upteq NFC 3.X platform without Controlling Authority and Optional Verification Authority », référence D1341170_wo_CA, release 1.1 ;

	- Guide pour l'autorité de vérification [AGD-OPE_VA] : • « Guidance for Verification Authority for Upteq NFC 3.X platform », référence D1341169_VA, release 1.0 ; - Guidance de développement d'applications • Guide [AGD_APP]: « Applications management for certified Secure Elements », référence D1258682, release C01 ; • Guide de développement d'applications basiques [AGD-Dev_Basic]: « GlobalPlatform Card – Composition Model Security Guidelines for Basic Applications », référence GPC_GUI_050, version 2.0 ; • Guide de développement d'applications sécuritaires [AGD-Dev_Sec] : « Guidance for secure application development on Upteq NFC platforms », référence D1188231, release A13.1 ; - Patch loading Management for certified Secure Element, référence D1344508, release A00.
[PPUSIMB]	(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations (Basic configuration), référence PU-2009-RT-79, version 2.0.2, 17 juin 2010. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/04.*
[PP0035]	Security IC Platform Protection Profile, version 1.0, 15 juin 2007. *Certifié par le* BSI *(Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI_PP_0035.*
[ANSSI-CC-2014/46]	Microcontrôleurs sécurisés ST33G1M2 Secure microcontroller revision F, Firmware revision 9, with optional NesLib 4.1 cryptographic library and MIFARE® DESFire® EV1 library revision 3.7 or 3.8. *Certifié par l'ANSSI sous la référence ANSSI-CC- 2014/46.*
[SUR-IC]	Rapport de surveillance ANSSI-CC-2014/46-S01, Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révision 9, incluant optionnellement la bibliothèque cryptographique Neslib 4.1 et la bibliothèque MIFARE® DESFire® EV1 révision 3.7 ou 3.8, délivré le 22 octobre 2015.

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, janvier 2012.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
[OPEN]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[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.