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-2014/88

Plateforme Upteq NFC 2.1.3_Generic sur le composant ST33F1ME avec application DESFIRE 1.1 (S1124940, release C)

Paris, le 17/12/2014

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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2014/88

Nom du produit

Plateforme Upteq NFC 2.1.3_Generic release C sur composant ST33F1ME

Référence/version du produit

T1020806, Release C

Conformité à un profil de protection

ANSSI-CC-PP-2010/03-M01 [PP JCS]

Java Card System – Open Configuration, version 3.0

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

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 « Plateforme Upteq NFC 2.1.3_Generic release C sur composant ST33F1ME (T1020806, Release C) » 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 a une conformité démontrable au profil de protection [PP JCS].

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* (80 CA 66 00) :

  73 55 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 18 06 0A 2B 06 01 04 01 2A 02 6E 01 03 06 0A 53 54 33 33 46 31 4D 20 01 14**

[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).

qui correspond aux informations suivantes :

Tag de l'identifiant du composant	66
Taille de l'identifiant du composant	18
Version JavaCard	06 0A 2B 06 01 04 01 2A 02 6E 01 03
Tag de l'identifiant de l'OS	06
Taille de l'identifiant de l'OS	0A
Nom du composant (ST33F1M) et version de l'OS (1.20)	53 54 33 33 46 31 4D 20 01 14

- la réponse à la commande *GetStatus* correspondant à l'AID de l'application DESFIRE : D2760000850100.

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]. Les applications présentes dans la configuration du produit sont dans le tableau suivant :

Application	**AID**
MPP1.0_AmendC-UICC-Interop_Release-A.2.2_121013	A0000000309000A301000010
PPSE v1.2	A0000000309006AC01000010
CRELPM	A0000000309007A300000010

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 :

- un mécanisme de contrôle d'accès aux éléments et aux propriétés de sécurité de l'application DESFIRE EV1 ;
- un mécanisme d'authentification des utilisateurs autorisés en fonction de leurs rôles respectifs ;
- l'intégrité et la confidentialité des communications lors des opérations réalisées par un mécanisme de transaction ;

[1] *Application Identifier.*

- un mécanisme de contrôle d'accès aux objets et aux attributs de sécurité de l'application DESFIRE EV1 pour l'enregistrement d'applications par une API DESFIRE spécifique ;
- 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[1], en tant qu'émetteur de la carte[2], 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[3] 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[4] (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 ;
- 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*

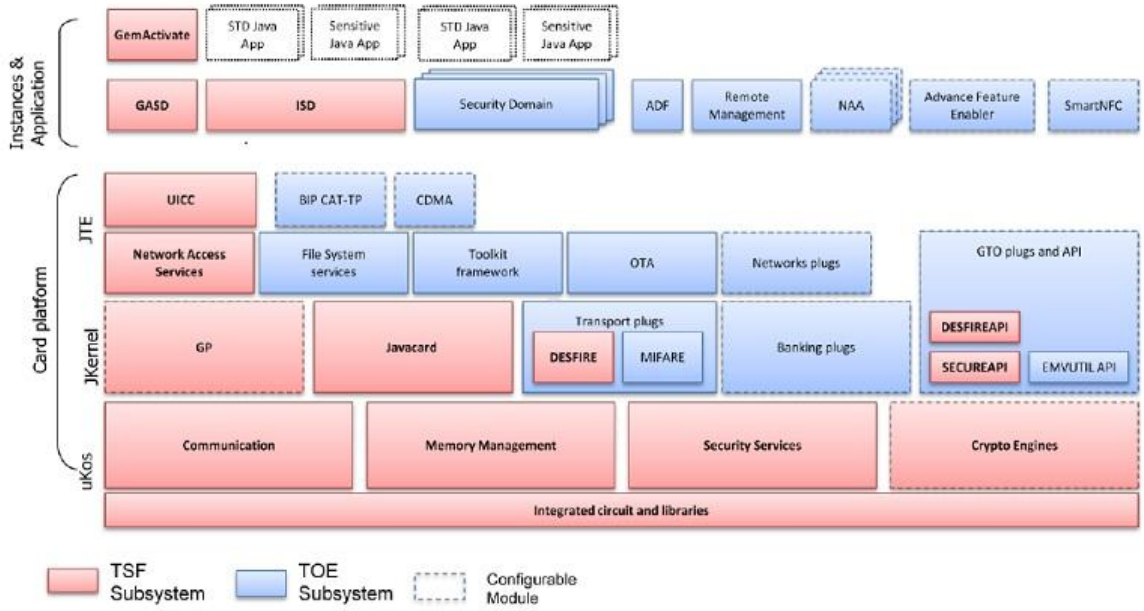
Le produit est composé des éléments suivants :

- 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 des applications d'authentification réseau (non évaluées) et un protocole de communication Télécom ;

[1] *Mobile Network Operator, opérateur mobile.*
[2] *Card Issuer.*
[3] *Application Provider (AP).*
[4] *Verification Authority (VA).*

- l'application GemActivate qui permet l'activation de services post-émission ;
- l'application DESFIRE EV1 version 1.1 qui permet d'interagir avec des terminaux sans contact compatible DESFIRE.

La figure suivante décrit les principaux éléments de la cible d'évaluation :

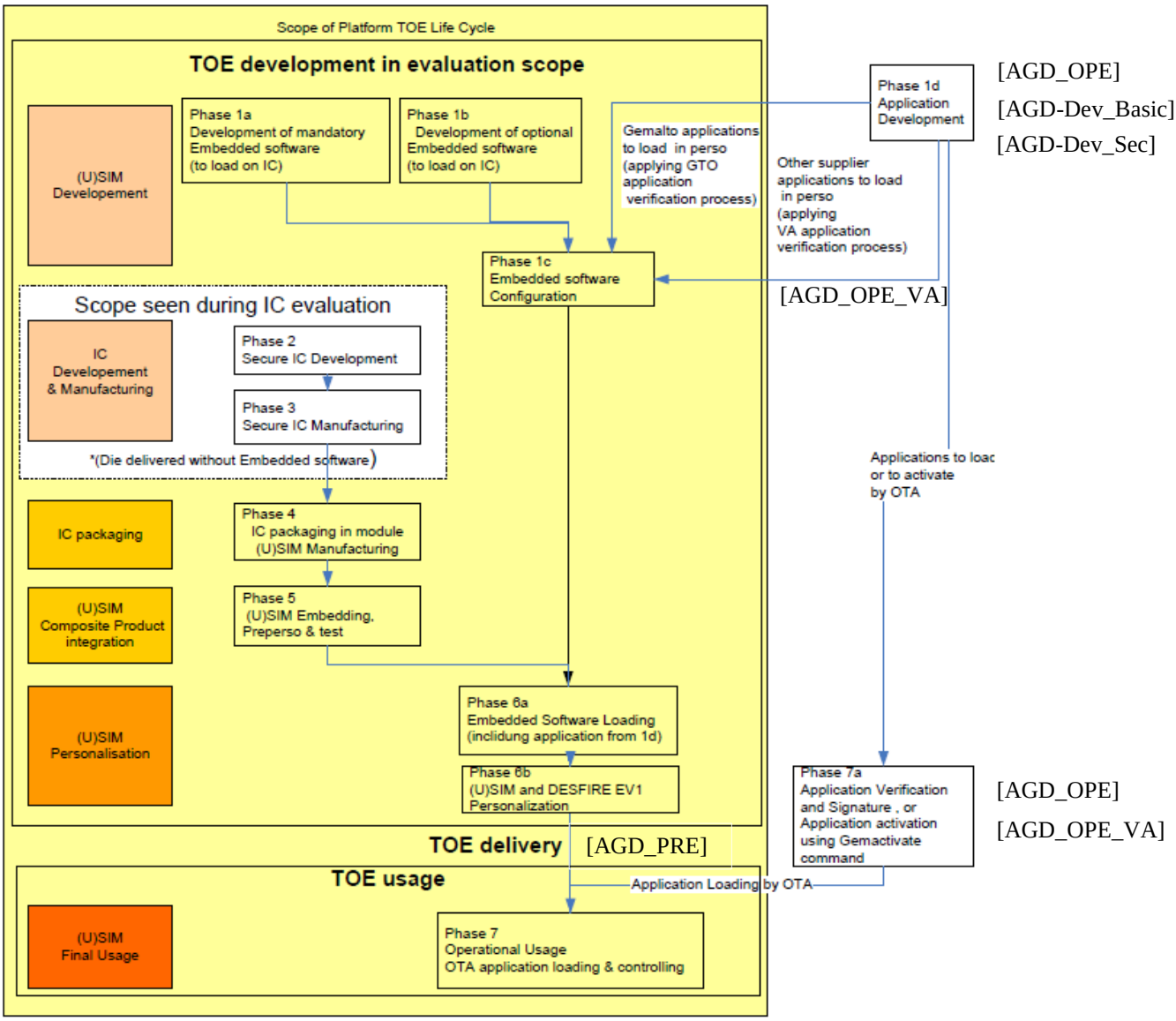


Note: le GASD correspond à *GemActivate Application Security Domain*, l'ISD à l'*Issuer Security Domain*, l'UICC à *Universal Integreted Circuit Card* (c'est une configuration GlobalPlatform).

Les applications déjà chargées dans le produit sont toutes identifiées dans le document [App_list] (voir paragraphe 1.2.2.).

1.2.5. *Cycle de vie*

Le cycle de vie du produit est le suivant :



Le produit a été développé sur les sites de Gemalto suivants :

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

Configuration du logiciel embarqué

525, Avenue du Pic de Bretagne
13420 Gemenos
France

12 Ayar Rajah Crescent
Singapour 139941
Singapour

Ul. Skarszewska 2
33-110 Tczew
Pologne

Assemblage

Rue de Saint Ulfrant
27500 Pont-Audemer
France

12 Ayar Rajah Crescent
Singapour 139941
Singapour

Encartage, pré-personnalisation et 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] ainsi que dans les maintenances successives [ANSSI-CC-2011/07-M01], [ANSSI-CC-2011/07-M02] et [ANSSI-CC-2011/07-M03].

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 [NOTE10], 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 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 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 ;
- le fournisseur de service de l'application DESFIRE EV1 qui est responsable de l'administration de l'application DESFIRE EV1 et de ses domaines de sécurité associés ;
- l'utilisateur final de l'application DESFIRE EV1 fonctionnant dans sa carte insérée dans son téléphone ;
- le développeur d'application pour le terminal qui est responsable du développement des applications du terminal communicant avec l'application DESFIRE ;
- le développeur d'application pour le téléphone qui est responsable du développement des applications du téléphone communicant ou non avec l'application DESFIRE ;
- le développeur d'application pour la carte ;
- les autres fournisseurs de service qui sont responsables de l'administration des autres applications existantes ainsi que des autres *security domains.*

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 (voir [CONF]).

1.2.7. *Configuration évaluée*

Le certificat porte sur la configuration du produit telle qu'elle est décrite au paragraphe 1.2.2.

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 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].
Deux configurations de la plateforme ont été prises en compte dans le cadre de cette évaluation : la configuration maximale [App_max] et la configuration minimale [App_min]. Les tests ont été effectués sur la configuration maximale [App_max] et couvrent donc les deux configurations possibles.

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 les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

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 « 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] puis maintenu sous les références [ANSSI-CC-2011/07-M01], [ANSSI-CC-2011/07-M02] et [ANSSI-CC-2011/07-M03].
Le niveau de résistance du microcontrôleur a été confirmé le 11 août 2014 dans le cadre du processus de surveillance sous la référence [SUR_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 2 octobre 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 les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF], 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.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 « Plateforme Upteq NFC 2.1.3_Generic release C sur composant ST33F1M, T1020806, release C » 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 :

- toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doivent respecter les contraintes de développement de la plateforme (guides [AGD-Dev_Basic] et [AGD-Dev_Sec]) selon la sensibilité de l'application considérée ;
- 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 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 : - « Security Target : DESFIRE 1.1 on Upteq NFC 2.1.3_Generic », référence D1314435, version 1.2. Pour les besoin de la publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Security Target : DESFIRE 1.1 on Upteq NFC 2.1.3_Generic », référence D1314435, version 1.0p.
[RTE]	Rapport technique d'évaluation : - « Evaluation technical report – Project : SUGITON_T », référence : SUG_T_ETR, version 2, 2 octobre 2014.
[CONF]	Liste de configuration du produit : - Platform identification and configurability Upteq NFC2.1.3_Generic v1.1, version 1.0 ; Liste des applications et *packages* vérifiées [App_list] : - pour la configuration maximale [App_max] « Sample Profile Description Max RSA with MPP », référence : D1306899_GEM01.00_ProfileDescription, version 1.3, 20 janvier 2014 ; - pour la configuration minimale [App_min] « Sample Profile Description Min », référence : D1306899_GEM03.00_ProfileDescription, version 1.1, 18 octobre 2013.
[GUIDES]	Guide d'installation du produit : - Guide de réception et d'installation [AGD-PRE] : « Uteq NFC 2.Y_Generic Preparation Guidance », référence : D1310908, version 1.0 ; Guides d'administration du produit : - Guide de l'application DESFIRE [AGD_OPE] : « DESFIRE EV1 on Uteq NFC 2.Y_Generic Guidance Administration », référence : D1310909, version : 1.0e ; - Guide de la plateforme avec *Controlling Authority :* « Guidance for administration of Upteq NFC 2.Y platform », référence : D1310910_VA, version 1.0 ; - Guide de la plateforme sans *Controlling Authority :* « Guidance for administration of Upteq NFC 2.Y platform without Controlling Authority and Optional Verification Authority », référence : D1310912_wo_CA, version 1.0 ;

	Guides d'utilisation du produit : - Guide de développement d'applications basiques [AGD-Dev_Basic]: « Rules for basic application development on Upteq certified product », référence D1186227 (A12b) ; - Guide de développement d'applications sécuritaires [AGD-Dev_Sec]: « Guidance for secure application development on Uteq mNFC platforms », référence D1188231 (A11) ; - Guide pour l'autorité de vérification [AGD-OPE_VA] : « Guidance for Verification Authority for Upteq NFC 2.Y platform », référence : D1310910_VA, version 1.0.
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[PP JCS]	"Java Card Protection Profile – Open Configuration", version 3.0, 18 mai 2012. *Maintenu par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01.*
[ANSSI-CC-2011/07]	Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E avec la bibliothèque cryptographique optionnelle NesLib v3.0. *Certifié par l'ANSSI sous la référence ANSSI-CC- 2011/07.*
[ANSSI-CC-2011/07-M01]	Rapport de maintenance émis par l'ANSSI le 15 mai 2012 sous la référence ANSSI-CC-2011/07-M01, pour le produit « Microcontrôleurs sécurisés ST33F1ME, ST33F1M0E, SC33F1M0E, ST33F896E, SC33F896E, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E and SC33F384E avec la version logicielle B ou C, incluant optionnellement la bibliothèque cryptographique Neslib v3.0 », initialement certifiée par l'ANSSI (voir [ANSSI-CC-2011/07]).
[ANSSI-CC-2011/07-M02]	Rapport de maintenance émis par l'ANSSI le 16 avril 2013 sous la référence ANSSI-CC-2011/07-M02, pour le produit « Microcontrôleurs sécurisés ST33F1ME, ST33F1M0E, SC33F1M0E, ST33F896E, SC33F896E, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E and SC33F384E avec la version logicielle B ou C, incluant optionnellement la bibliothèque cryptographique Neslib v3.0 », initialement certifiée par l'ANSSI (voir [ANSSI-CC-2011/07]).
[ANSSI-CC-2011/07-M03]	Rapport de maintenance émis par l'ANSSI le 19 août 2014 sous la référence ANSSI-CC-2011/07-M03, pour le produit «Microcontrôleurs sécurisés ST33F1ME, SC33F1ME, ST33F1M0E, SC33F1M0E, ST33F896E, SC33F896E, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E avec la version logicielle B ou C, incluant optionnellement la bibliothèque cryptographique Neslib v3.0 », initialement certifiée par l'ANSSI (voir [ANSSI-CC-2011/07]).

[SUR_IC]	Rapport de surveillance émis par l'ANSSI le 11 août 2014, sous la référence ANSSI-CC-2011/07-S02, pour le produit « Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E incluant optionnellement la bibliothèque cryptographique NesLib v3.0 », initialement certifié par l'ANSSI (voir [ANSSI-CC-2011/07]).

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, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref 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, January 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[NOTE.10]	« Note d'application - Certification d'applications sur "plateformes ouvertes cloisonnantes" », référence ANSSI-CC-NOTE-10/1.0, voir www.ssi.gouv.fr.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.

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