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-2017/51

ST33J2M0 B02 including optional cryptographic library Neslib and optional technology MIFARE4Mobile

Paris, le 5 septembre 2017

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

Guillaume POUPARD
[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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2017/51

Nom du produit

ST33J2M0 B02 including optional cryptographic library Neslib and optional technology MIFARE4Mobile

Référence/version du produit

B02

Conformité à un profil de protection

Security IC Platform Protection Profile with Augmentation Packages, version 1.0

certifié BSI-CC-PP-0084-2014 le 19 février 2014

avec conformité aux packages

“Authentication of the security IC”
“Loader dedicated for usage in Secured Environment only”
“Loader dedicated for usage by authorized users only”

Critères d’évaluation et version

Critères Communs version 3.1 révision 4

Niveau d’évaluation

EAL 5 augmenté

ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_FUN.2 et AVA_VAN.5

Développeur(s)

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France

Commanditaire

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France

Centre d’évaluation

Serma Safety & Security

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.

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. Introduction 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 7
1.2.4. Identification du produit 8
1.2.5. Cycle de vie 9
1.2.6. Configuration évaluée 10

2. L'EVALUATION 11

2.1. REFERENTIELS D'EVALUATION 11
2.2. TRAVAUX D'EVALUATION 11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 11
2.4. ANALYSE DU GENERATEUR D'ALEAS 11

3. LA CERTIFICATION 12

3.1. CONCLUSION 12
3.2. RESTRICTIONS D'USAGE 12
3.3. RECONNAISSANCE DU CERTIFICAT 13
3.3.1. Reconnaissance européenne (SOG-IS) 13
3.3.2. Reconnaissance internationale critères communs (CCRA) 13

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 14

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 15

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 17

1. Le produit

1.1. Présentation du produit

Le produit évalué est le microcontrôleur « ST33J2M0 B02 including optional cryptographic library Neslib and optional technology MIFARE4Mobile » développé par *STMICROELECTRONICS.*
Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

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 strictement conforme au profil de protection [PP0084], avec :

- le package « *authentication of the security IC* » ;
- le package « *loader dedicated for usage in secured environment only* » ;
- le package « *loader dedicated for usage by authorized users only* ».

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'initialisation de la plate-forme matérielle et des attributs ;
- la gestion sécurisée du cycle de vie ;
- l'intégrité logique du produit ;
- les tests du produit ;
- des contrôles d'accès aux mémoires dont un dédié à la bibliothèque embarquée ;
- la protection physique ;
- la gestion des violations sécuritaires ;
- la non-observabilité des informations sensibles ;
- le chargement et la gestion sécurisés de la mémoire *Flash* ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support au chiffrement cryptographique à clés asymétriques ;
- le support à la génération de nombres non prédictibles ;
- le service optionnel de bibliothèque cryptographique Neslib offrant des fonctionnalités RSA, ECC, AES, DES, DRBG, ainsi que la génération sécurisée de nombres premiers et de clés RSA ;
- la technologie (optionnelle) MIFARE4Mobile.

1.2.3. Architecture

Le produit est constitué d'une partie matérielle et d'une partie logicielle, toutes deux décrites dans la cible de sécurité au chapitre 1.6 « *TOE description* ».

La partie matérielle comporte principalement :

- un processeur, 32-bit RISC ARM, double cœur SecureCore SC300 ;
- des mémoires ROM, *Flash* (jusqu'à 2048Ko de mémoire utilisateur) et RAM (50Ko de mémoire utilisateur) ;
- des modules de sécurité : protection de la mémoire (MMU, *Memory Management Unit*), génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;
- des modules fonctionnels : gestion des entrées / sorties en mode contact (ISO7816), interface sans contact (protocole de communication SWP), interfaces I2C et SPI, générateur de nombres aléatoires (TRNG, *True Random Number Generator*) ;
- des coprocesseurs cryptographiques optionnels pour accélérer les calculs AES pour le support des algorithmes AES, EDES pour le support des algorithmes DES et de NESCRYPT (NExt Step CRYPTography) muni d'une RAM dédiée pour le support des algorithmes cryptographiques à clé publique.

La partie logicielle est composée :

- d'un logiciel dédié, nommé OST[1], participant au démarrage du composant (*boot sequence*) ;
- d'un logiciel dédié, nommé *firmware*, assurant la gestion du cycle de vie, le chargement de la mémoire *Flash* (*Secure Flash loader*), et l'interfaçage avec l'application (*drivers*) ;

De manière optionnelle, le client peut choisir d'intégrer :

- la bibliothèque cryptographique Neslib fournissant des implémentations de fonctions cryptographiques. La bibliothèque Neslib est embarquée partiellement ou en totalité selon son besoin, avec le code client, dans la mémoire *Flash* du produit ;
- la bibliothèque MIFARE4Mobile (en version 2.2.9 ou 2.2.10). Cette bibliothèque inclut les fonctionnalités MIFARE DESFire® EV1 et MIFARE® Classic. Les fonctionnalités MIFARE® Classic sont en dehors du périmètre de certification.

[1] *Operating System for Test* – sytème d'exploitation pour test.

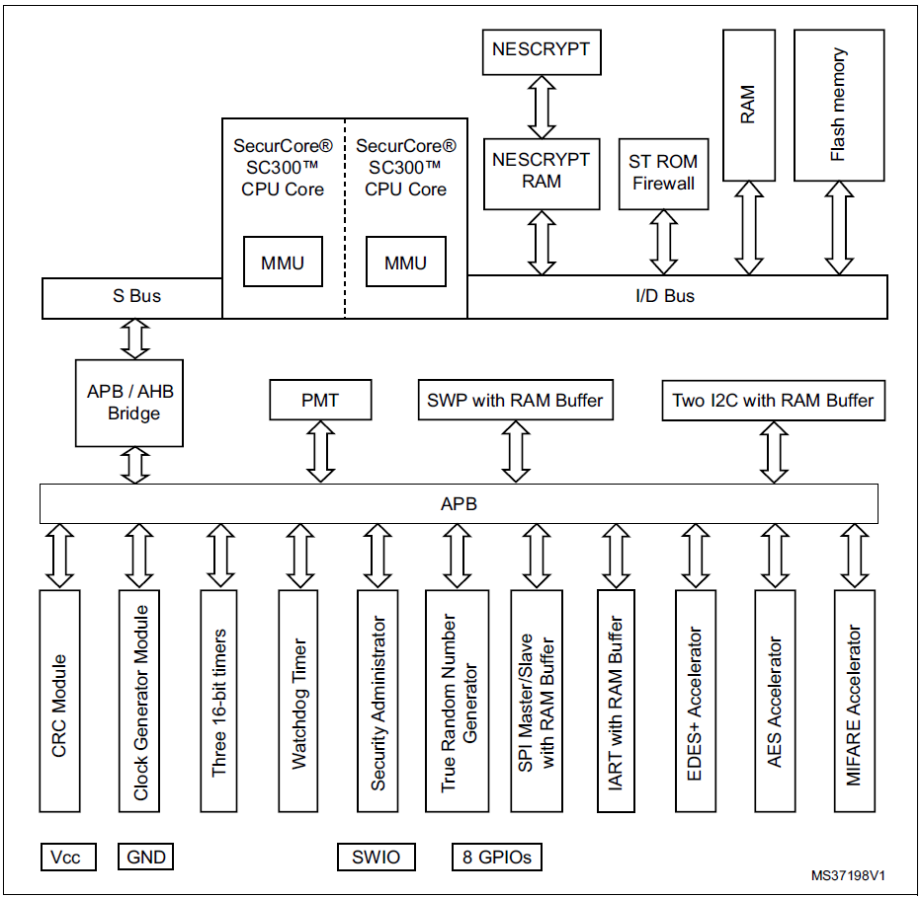


Figure 1 : Architecture du produit

1.2.4. Identification du produit

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

La version certifiée du microcontrôleur est identifiable par les éléments donnés dans la table ci-après.

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur ST33J2M0 B02	*IC maskset name*	K500A
	IC version H	48
	Master identification number	0137
Identification des logiciels embarqués	*Firmware version 3.2.5*	03020404 (*initial kernel*) 10030205 (*firmware extension*)
	OST version 05.04	0504
Identification des bibliothèques	*Neslib version 5.2.2*	01 05 02 02
	MIFARE4Mobile version 2.2.9	02 02 09 00
	MIFARE4Mobile version 2.2.10	02 02 0A 00

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans le guide « *User manual ST33J2M0 firmware V3* », voir [GUIDES]. De plus, la valeur de l'élément *IC maskset name*, « K500A », est gravée sur la surface du composant.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité [ST] ; il est conforme au cycle de vie de 7 phases décrit dans [PP0084] :

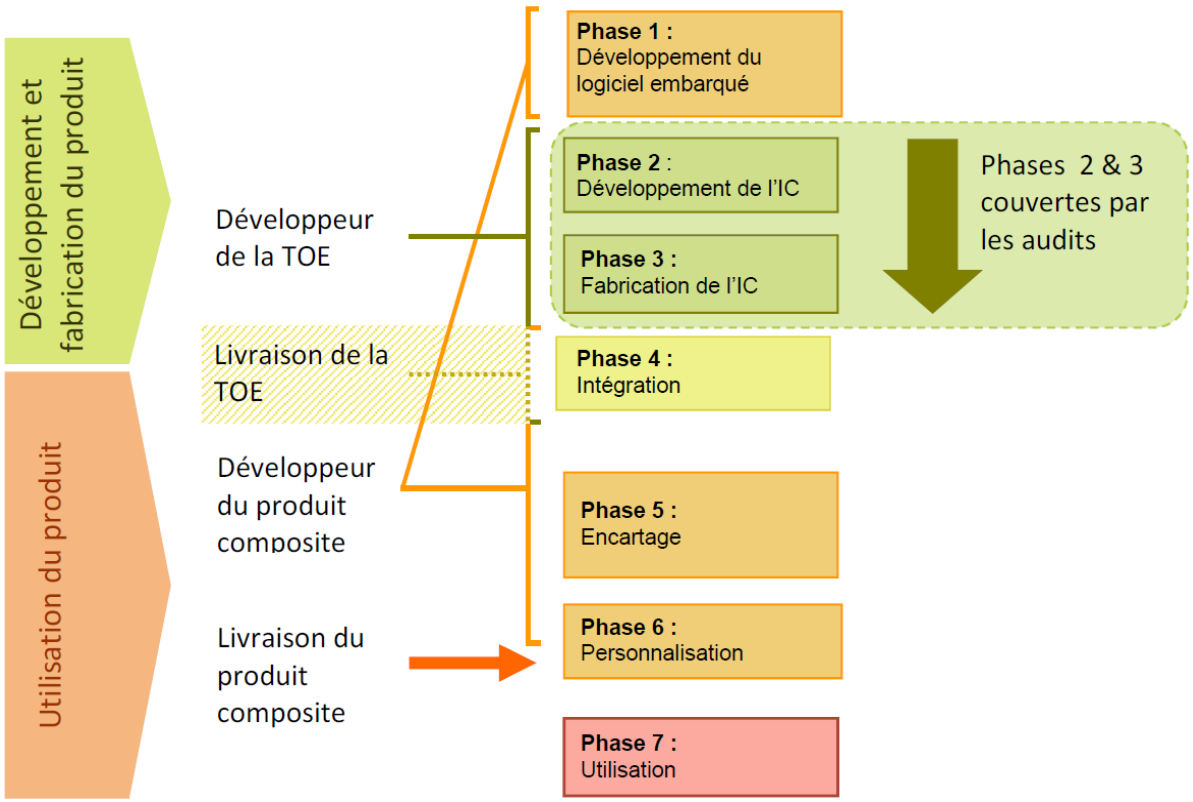


Figure 2 : Cycle de vie du produit

Les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous forme de *wafers* ou de *wafers* sciés (*dices)*. En option, la TOE peut également être livrée après la phase 4, dans sa forme finale, par exemple en format carte.

La phase 2 correspond à la phase de développement du microcontrôleur et comprend notamment les étapes suivantes :

- la conception du circuit ;
- le développement du logiciel dédié.

La phase 3, qui couvre la fabrication du microcontrôleur, comprend les étapes suivantes :

- l'intégration et la fabrication du masque ;
- la fabrication du circuit ;
- le test du circuit ;
- la préparation ;
- la pré-personnalisation du microcontrôleur.

La phase 4, pouvant être gérée optionnellement par *STMICROELECTRONICS*, comprend les étapes suivantes :

- le conditionnement ;
- le test ;
- la pré-personnalisation si nécessaire.

Les sites impliqués dans le cycle de vie pour les phases 2, 3 et 4 sont indiqués dans la table 16 de la cible de sécurité [ST].

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit le développeur de l'application à embarquer dans le microcontrôleur.

Le produit gère son cycle de vie sous la forme de cinq configurations :

- le mode « *test* » qui permet aux sites d'assemblages d'effectuer des tests restreints, sous le contrôle de l'OST, pour vérifier la qualité de l'assemblage. Ce mode est réservé à *STMICROELECTRONICS ;*
- le mode « *admin* » qui est utilisé sous le contrôle du *Flash loader*. Il peut être utilisé dans des environnements non audités. Ce mode permet notamment le chargement de la mémoire *Flash* en environnement non audité, incluant le chargement du *firmware*, le logiciel utilisateur et les données associées. Le microcontrôleur peut être livré dans ce mode ;
- le mode « *user* » qui est le mode final d'utilisation. Dans ce mode, le produit peut exécuter le logiciel applicatif chargé en mémoire *Flash.* Le microcontrôleur peut être livré dans ce mode ;
- le mode « *diagnostic* » qui est un mode réservé à *STMICROELECTRONICS* permettant l'analyse de la qualité du microcontrôleur sur le terrain. Par défaut, ce mode est désactivé dans un état réversible à la fin de la phase 3. Il est ensuite possible de l'activer ou de le désactiver de manière irréversible ;
- le mode « *genuine* » qui vérifie l'authenticité du produit. Ce mode reste actif durant toute la vie du produit.

1.2.6. Configuration évaluée

Le certificat porte sur le produit « ST33J2M0 B02 including optional cryptographic library Neslib, and optional technology MIFARE4Mobile » tel que décrit au paragraphe 1.2.4. Toute autre application, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre de l'évaluation.
Au regard du cycle de vie détaillé au chapitre 1.2.5, le produit évalué est celui obtenu à l'issue de la phase 3 lorsque le produit est livré sous forme de *wafer* ou de *dice*, en mode « *user* » ou « *admin* » avec le mode « *diagnostic* » désactivé.

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].
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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 25 août 2017, 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 vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS31] et il répond aux exigences de la classe PTG.2.

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées sont réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [REF], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

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 microcontrôleur « ST33J2M0 B02 including optional cryptographic library Neslib, and optional technology MIFARE4Mobile » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_FUN.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.

Ce certificat donne une appréciation de la résistance du microcontrôleur « ST33J2M0 B02 including optional cryptographic library Neslib, and optional technology MIFARE4Mobile » à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le microcontrôleur ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

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].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

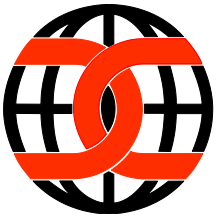
Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

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 puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. 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] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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 5+	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**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**2**	Complete mapping of the implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**3**	Minimally complex internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**5**	Complete semiformal 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	**5**	Advanced support
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools 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								**1**	Basic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**3**	Compliance with implementation standards - all parts
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	**2**	TOE summary specification with architectural design summary
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**3**	Rigorous analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**3**	Testing: modular design
	ATE_FUN		**1**	1	1	1	**2**	2	**2**	Ordered 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 : - ST33J2M0 B02 including optional cryptographic library NESLIB, and optional technology MIFARE4Mobile Security Target, référence SMD_ST33J2M0_ST_16_003, version B02.4, août 2017. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST33J2M0 B02 including optional cryptographic library NESLIB, and optional technology MIFARE4Mobile Security Target for composition, référence SMD_ST33J2M0_ST_17_002, version B02.4, août 2017.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – PERCEVAL4 project, référence Perceval4_ETR_v1.1, version 1.1, 24 août 2017. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ETR Lite for Composition – PERCEVAL4 project, référence Perceval4_ETR_lite_v1.1, version 1.1, 24 août 2017.
[CONF]	Liste de configuration du produit : - ST33-K500 configuration list, référence SMD_ST33J2M0_CFGL_17_002, version 4.0, 18 août 2017 ; - Neslib 5.2.2 for ST33 lockstep configuration list, référence SSS_NesLib522ST33LS_CFGL_16_001, version 1-02, 31 janvier 2017.

[GUIDES]	- ST33J2M0 Datasheet, référence DS_ST33J2M0, version 3, janvier 2017 ; - ST33J2M0 firmware V3 - User manual, référence UM_ST33J2M0_FWv3, version 10, mars 2017 ; - ST33J Secure MCU platform, security guidance - Application note, référence AN_SECU_ST33J, version 5.0, novembre 2016 ; - ARM® SC300 r0p1 Technical reference Manual, référence ARM_DDI_0447, version A, 24 juin 2009 ; - ARM® Cortex-M3 r2p0 Technical Reference Manual, référence ARM_DDI_0037F3c, version F3c, 31 janvier 2008 ; - ARM® SecurCore SC300 (AT500) Product Errata Notice, référence PR326-PRDC-009983, version 11, 24 février 2015 ; - ST33J platform - AIS 31, compliant random number - User manual, référence UM_ST33J_AIS31, version 1, mai 2016 ; - ST33J platform AIS31 – Application note, reference implementation: Start-up, on-line and total failure tests, référence AN_ST33J_AIS1, version 1, mai 2016 ; - NesLib cryptographic library Neslib 5.2 - User manual, référence UM_NesLib_5.2, version 2, juillet 2016 ; - ST33J Secure MCU platform NesLib 5.2 security recommendations, référence AN_SECU_ST33J_NESLIB_5.2, version 3, décembre 2016 ; - Neslib 5.2.2 for ST33 Lockstep platform - Release note, référence RN_ST33J_NESLIB_5.2.2, version 2, janvier 2017 ; - MIFARE4Mobile® library 2.2 for the ST33J platform - User manual, référence UM_33J_MIFARE4MOBILE-2.2, version 4, octobre 2016 ; - MIFARE4Mobile® library 2.2.9 for the ST33J platform - Application note, référence AN_ST33J_M4M_Lib, version 1, octobre 2016 ; - MIFARE4Mobile® library 2.2.10 for the ST33J platform - Application note, référence AN_ST33J_M4M_Lib, version 2, juillet 2017.
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, 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, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 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.
[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.
[AIS31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 September 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

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