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-2020/30

ST33J2M0 D01 including optional cryptographic library NESLIB, and optional technology MIFARE4Mobile

Paris, le 9 juillet 2020

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-2020/30

Nom du produit

ST33J2M0 D01 including optional cryptographic library NESLIB, and optional technology MIFARE4Mobile

Référence/version du produit

D01

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 5

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

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 10071, 33608 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 directeur général de l'Agence national de la sécurité des systèmes d'information 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 « ST33J2M0 D01 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 plateforme 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 ;
- 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 se décline en deux versions (révision H et révision I) et comporte principalement :

- un processeur Secure SC300 dual core 32-bit ARM ;
- des mémoires ROM, *Flash* (jusqu'à 2048Ko de mémoire utilisateur) et RAM (dont 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 et des 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 se décline également en deux versions (3.2.5 et 3.3.0) et est composée de :

- un logiciel dédié, nommé OST[1], participant au démarrage du composant (*boot sequence*) ;
- 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 (en version 6.3.4) 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.

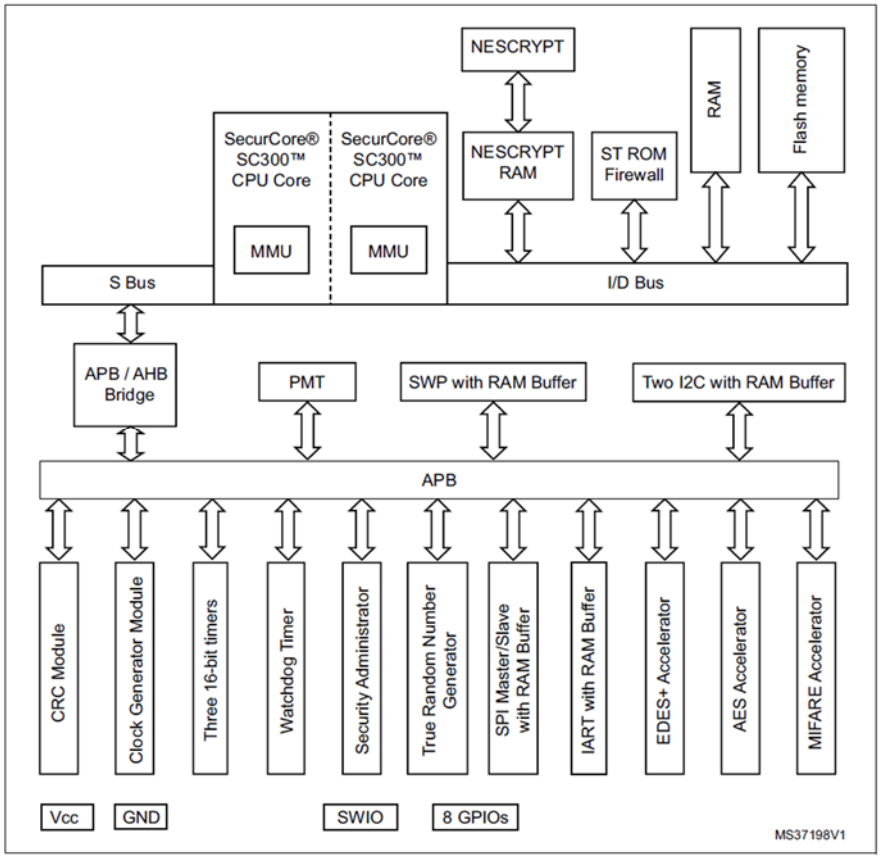

Figure 1 : Architecture du produit

La version logicielle 3.2.5 n'est embarquée que sur la révision matérielle H alors que la version logicielle 3.3.0 est embarquée sur les révisions matérielles H et I.

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 D01	*IC maskset name*		K500A
	IC versions	H	48
		I	49
	Master identification number		01 37
Identification des logiciels embarqués	*Firmware versions*	3.2.5	03 02 04 04
			10 03 02 05 *(firmware extension)*
		3.3.0	03 03 00 03
			01 03 03 00 *(firmware extension)*
	OST version 05.04		05 04
Identification des bibliothèques	*NESLIB version 6.3.4*		06 03 04
	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] :

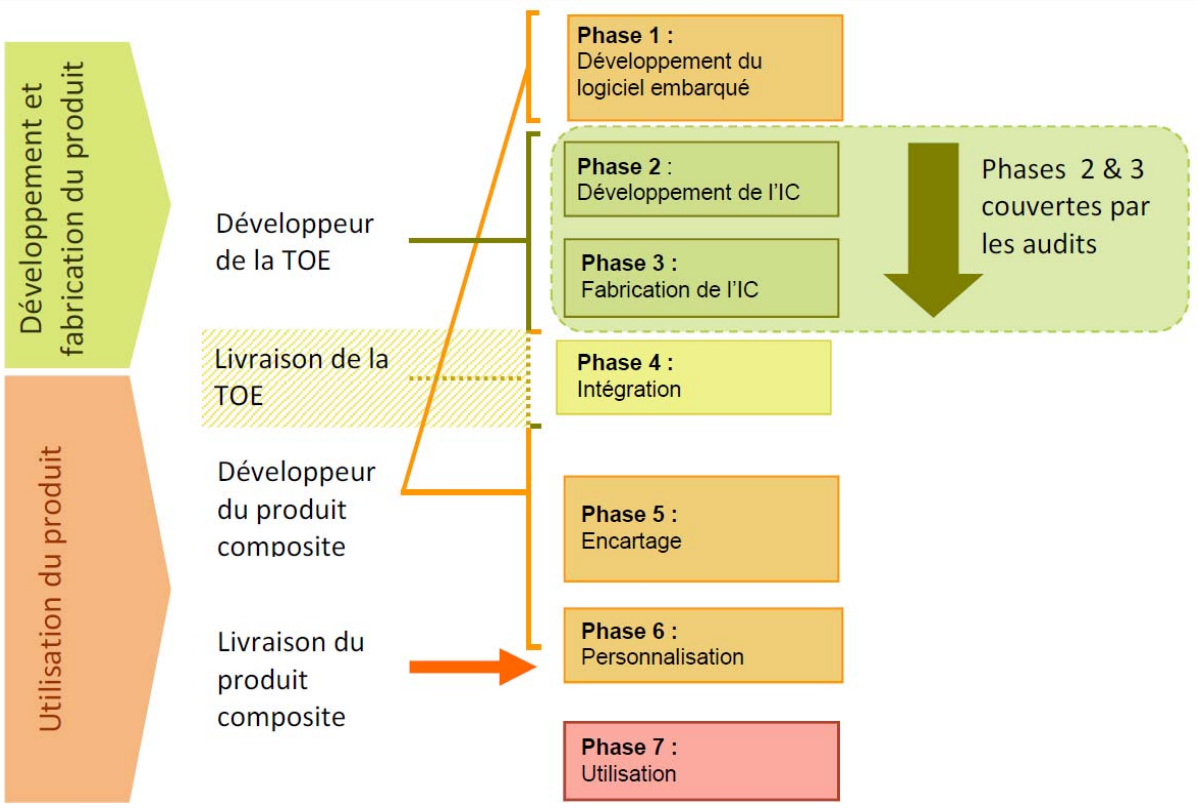

Figure 2 : Cycle de vie du produit

Le produit a été développé sur les sites suivants (voir [SITES]) :

ST Rousset 190 avenue Célestin Coq 13106 Rousset Cedex France	**ST Tunis** Elgazala Technopark, Raoued Gouvernorat de l'Ariana, PB21 2088 cedex, Ariana Tunisia
ST Crolles 850 rue Jean Monet 38926 Crolles France	**ST Ang Mo Kio 1** 5A Serangoon North avenue 5, Singapore 554574

ST Zaventem Green Square, Lambroekstraat 5 Building B, 3d floor 1831 Diegem/Machelen Belgium	**ST Grenoble** 12 rue Jules Horowitz BP 217, 38019 Grenoble Cedex France
ST Rennes 10 rue de Jouanet, ePark 35700 Rennes France	**ST Sophia** 635 route des Lucioles 06560 Valbonne France
ST Ljubljana Tehnološki park 21 1000, Ljubljana Slovenia	**ST Toa Payoh** 629 Lorong 4/6 Toa Payoh Singapore 319521
ST Ang Mo Kio 6 18 Ang Mo Kio Industrial park 2 Singapour 569505	**DNP** DNP (Dai Nippon printing Co ltd.) 2-2-1 kami Fukuoka Fujimino-shi Saitama 356-8507 Japan
DPE Via C. Olivetti, 2/A, 20041 Agrate Brianza Italy	**AMTC Dresden** Rahnitzer Allee 9, 01109 Dresden Japan
CMP Goerges Charpak 880 Avenue de Mimet 13541 Gardanne France	**ST Shenzhen** 16 Tao hua Rd., Futian free trade zone, Shenzhen, Popular Republic of China 518038
ST Bouskoura 101 Boulevard des Muriers – BP97, Bouskoura 20180 Maroc	**ST Calamba** 9 Mountain drive Light Industry & Science Park II Brgy La Mesa, 4027 Calamba Philippines
ST Loyang 7 Loyang drive Singapore 508938	**WINSTEK** No 176-5, 6 Ling, Hualung Chun, Chiung Lin, 307 Hsinchu, Taiwan

AMKOR Taïwan ATT1 : N°1, Kao-Ping Sec, Chung-Feng road, Longtan District, Taoyuan city 325, Taiwan, R.O.C ATT3 : N°11, Guangfu road, Hsinchu industrial park, Hukou Township, Hsinchu County 303, Taiwan, R.O.C ATT6 : N° 333, Longyuan 1st Road, Hsinchu Science Park, Longtan Dist., Taoyuan City, Taïwan, R.O.C.	**AMKOR Philippines** ATP1 : Km 22 East Service Rd. South superhighway, Muntinlupa City 1771 Philippines ATP3/4 : 119 N. Science Avenue, Laguna Technopark, Binan, Laguna, 4024 Philippines
STATS ChipPAC JSCC 78 Changshan road, Jiangyin, Jangsu, 214437 China	**Feiliks** Feiliks Logistics, Zhongbao Logistics Building, No. 28 Taohua Road, FFTZ, Shenzhen, Guangdong 518038, China

1.2.6. Configuration évaluée

Le certificat porte sur le produit « ST33J2M0 D01 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.

2. L’évaluation

2.1. Référentiels d’évaluation

L’évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [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 20 janvier 2020, 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. Ceci ne permet pas d'affirmer que les données générées soient 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 produit « ST33J2M0 D01 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 produit « ST33J2M0 D01 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 micro-circuit 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 :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

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[1], 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 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 D01 Security Target, référence SMD_ST33J2M0_ST_19_003, version D01.3, 17 décembre 2019, *STMICROELECTRONICS.* Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST33J2M0 C01 Security Target for composition, référence SMD_ST33J2M0_ST_19_004, version D01.3, 17 décembre 2019, *STMICROELECTRONICS.*
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – PERCEVAL D01 Project, référence PERCEVAL_D01_ETR_v1.1, version 1.1, 20 janvier 2020, *SERMA SAFETY & SECURITY*. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation Technical Report Lite for Composition – PERCEVAL D01 Project, référence PERCEVAL_D01_ETR-Lite_v1.1, version 1.1, 20 janvier 2020, *SERMA SAFETY & SECURITY*.
[CONF]	Liste de configuration du produit : - ST33J2M0 D01 – HW Rev H Configuration List, référence SMD_ST33J2M0_D01_CFGL_19_001, version 1.2, 20 décembre 2019, *STMICROELECTRONICS* ; - ST33J2M0 D01 – HW Rev I Configuration List, référence SMD_ST33J2M0_D01_CFGL_19_002, version 1.2, 20 décembre 2019, *STMICROELECTRONICS.*

[GUIDES]	- ST33J platform AIS31 – Application note, reference implementation: Start-up, on-line and total failure tests, référence AN_ST33J_AIS1, version 1, mai 2016, *STMICROELECTRONICS* ; - Application note ST33J Secure MCU platform Security guidance, reference AN_SECU_ST33J, version 10, 11 décembre 2019, *STMICROELECTRONICS* ; - ST33J2M0 Datasheet : Secure MCU with 32-bit SecurCore SC300 CPU with SWP, ISO SPI, I2C & Flash, référence DS_ST33J2M0, version 8, 20 juin 2019, *STMICROELECTRONICS* ; - ARM® SC300 r0p1 Technical reference Manual, référence ARM_DDI_0447, version A, 24 juin 2009, *ARM* ; - ARM® Cortex-M3 r2p0 Technical Reference Manual, référence ARM_DDI_0337F3c, version F3c, 31 janvier 2008, *ARM* ; - ARM® SecurCore SC300 (AT500) Product Errata Notice, référence PR326-PRDC-009983, version 11, 24 février 2015, *ARM* ; - User manual, ST33J platform - AIS 31, compliant random number, référence UM_ST33J_AIS31, version 1, mai 2016, *STMICROELECTRONICS* ; - User manual ST33J2M0 firmware V3, référence UM_ST33J2M0_FWv3, version 19, 19 juillet 2019, *STMICROELECTRONICS* ; - MIFARE4Mobile library 2.2 for the ST33J platform - User manual, référence UM_33J_MIFARE4MOBILE-2.2, version 4, octobre 2016, *STMICROELECTRONICS* ; - MIFARE4Mobile library 2.2.9 for the ST33J platform - Application note, référence AN_ST33J_M4M_Lib, version 1, octobre 2016, *STMICROELECTRONICS* ; - MIFARE4Mobile library 2.2.10 for the ST33J platform - Application note, référence AN_ST33J_M4M_Lib, version 2, juillet 2017, *STMICROELECTRONICS* ; - User manual – NesLib cryptographic library NesLib 6.3, version 4, 18 juillet 2019, *STMICROELECTRONICS* ; - Application Note – ST33J secure MCU platforms – NesLib 6.3 security recommendations, référence AN_SECU_ST33J_NESLIB_6.3, version 4, 9 septembre 2019, *STMICROELECTRONICS* ; - Neslib 6.3.4 for ST33 Lockstep platform - Release note, référence RN_ST33J_NESLIB_6.3.4, version 3, 9 septembre 2019, *STMICROELECTRONICS.*

[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - ALC Class Evaluation Report - C15P0036 Project, référence C15P0036_ALC_GEN_V2.0, version 2.0, 11 juillet 2018, *SERMA SAFETY & SECURITY* ; - ALC Class Evaluation Report - STM Project, référence STM_GEN_v2.0, version 2.0, 21 décembre 2018, *SERMA SAFETY & SECURITY* ; - ALC Class Evaluation Report – STM 2020 Project, référence STM-2020_GEN_v1.1, version 1.1, 20 novembre 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - Ang Mo Kio 1 Site Audit, référence STM2020_AMK1_STAR_V1.0, version 1.0, 26 novembre 2019 ; - Site Technical Audit Report - ATP1 & ATP3/4, référence STM_ATP1-3-4_STAR_v1.1, version 1.1, 13 mai 2019, *SERMA SAFETY & SECURITY* ; - STMicroelectronics Development Environment Amkor Technology Taiwan 1 & 3 Site Technical Audit Report, référence STM2020_ATT1-3_STAR_v1.0, version 1.0, 6 janvier 2020, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - STMicroelectronics Bouskoura Site Technical Audit Report, référence STM2020_BSK_STAR_v1.0, version 1.0, 27 décembre 2019, *SERMA SAFETY & SECURITY* - Site Technical Audit Report STM Calamba, référence STM2020_CAL_STAR_v1.1, version 1.1, 10 janvier 2020, *SERMA SAFETY & SECURITY* ; - Site Visit Lite Report – STM CROLLES site audit, référence STM_Crolles_SVR-M_v1.0, version 1.0, 18 juillet 2018, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - STM Grenoble, référence 18-0337_STM Grenoble_STAR_v1.0, version 1.0, 9 mai 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - STM Ljubljana, référence STM_LJU_STAR_v1.0, version 1.0 du 7 mars 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - STMicroelectronics Loyang (LYG) Site Audit, référence STM2020_Loyang_STAR_v1.0, version 1.0, 21 novembre 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - STM Rennes, référence STM_RNS_STAR_v1.0, version 1.0, 22 mai 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report – STM Rousset, référence STM2020_RST_STAR_v1.0, version 1.0, 5 février 2020, *SERMA SAFETY & SECURITY* ; - Site Visit Lite Report – STS Shenzhen site audit, référence 17-0317_STS Shenzhen_SVR-M_v1.1, version 1.1, 14 décembre 2018, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report TPY and AMK 6, référence STM2020_TPY-AMK6_STAR_v1.0, version 1.0, 24 février 2020, *SERMA SAFETY & SECURITY* ;

	- Site Technical Audit Report - STM Tunis Site Audit, référence STM_TNS_STAR_v1.0, version 1.0, 5 septembre 2019, *SERMA SAFETY & SECURITY* ; - Site Audit Technical Report - STM Zaventem site audit, référence STM_Zaventem_STAR_v1.0, version 1.0, 8 mars 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - Winstek, référence STM-WIN_STAR_v1.1, version 1,1, 19 décembre 2018, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - DNP, référence STM-DNP_STAR_v1.2, version 1.2, 27 mai 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - DPE Agrate site audit, référence STM-DPE_STAR_v1.0, version 1.0 du 5 juillet 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - FEILIKS, référence STM_FEILIKS_STAR_v1.0, version 1.0, 24 avril 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - JSCC, référence STM_JSCC_STAR_v1.0, version 1.0, 27 juin 2019, *SERMA SAFETY & SECURITY* ; - Site Technical Audit Report - STM Sophia, référence STM_Sophia_STAR_v1.0, version 1.0, 28 décembre 2018, *SERMA SAFETY & SECURITY*.
[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, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[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 3.0, avril 2019.
[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.
[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.
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 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.