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-2019/20

ST54J A01

Paris, le 18 avril 2019

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-2019/20

Nom du produit

ST54J A01

Référence/version du produit

A01

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

ALC_DVS.2, AVA_VAN.5

Développeur

STMicroelectronics

190 avenue Célestin Coq, ZI de Rousset, 13106 Rousset Cedex, France

Commanditaire

STMicroelectronics

190 avenue Célestin Coq, ZI de Rousset, 13106 Rousset Cedex, 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 EAL 2.

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 le microcontrôleur « ST54J A01 » développé par *STMICROELECTRONICS*. Ce microcontrôleur, aussi appelé « ST54J_SE », est inclus dans la plateforme ST54J composée également d'un module NFC et d'un module IORING nommés respectivement ST54J_CLF et ST54J_IOs dans la figure ci-dessous. Ces derniers sont en dehors du périmètre d'évaluation.

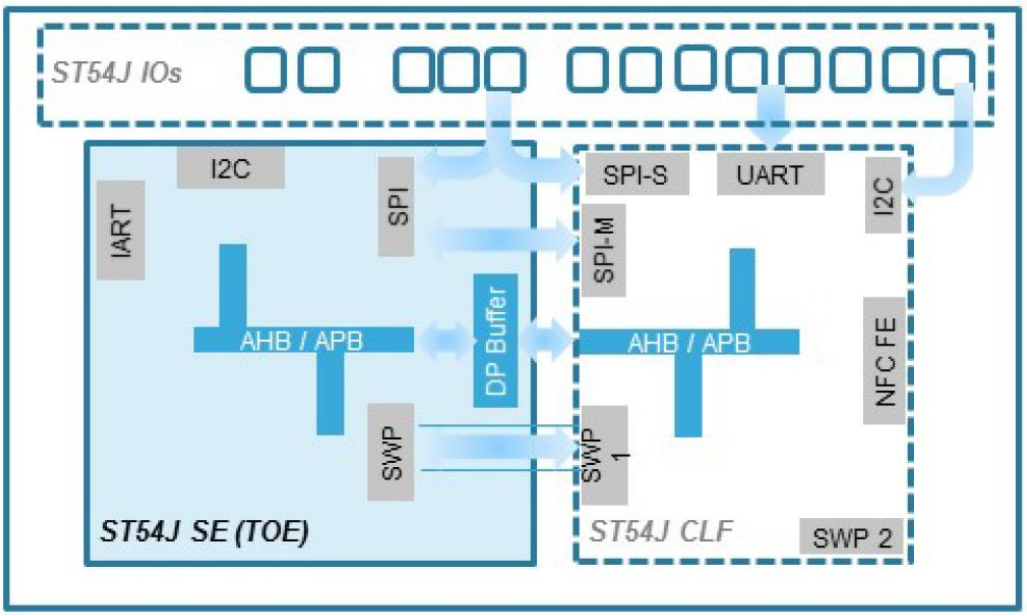

Figure 1 : Présentation de la plateforme ST54J

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 évalués 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 matériel au chiffrement cryptographique à clés symétriques ;
- le support à la génération de nombres non prédictibles.

1.2.3. Architecture

Le microcontrôleur « ST54J A01 » est constitué d'une partie matérielle et d'une partie logicielle, toutes deux décrites dans la cible de sécurité [ST] au chapitre 1.6 « *TOE description* ».

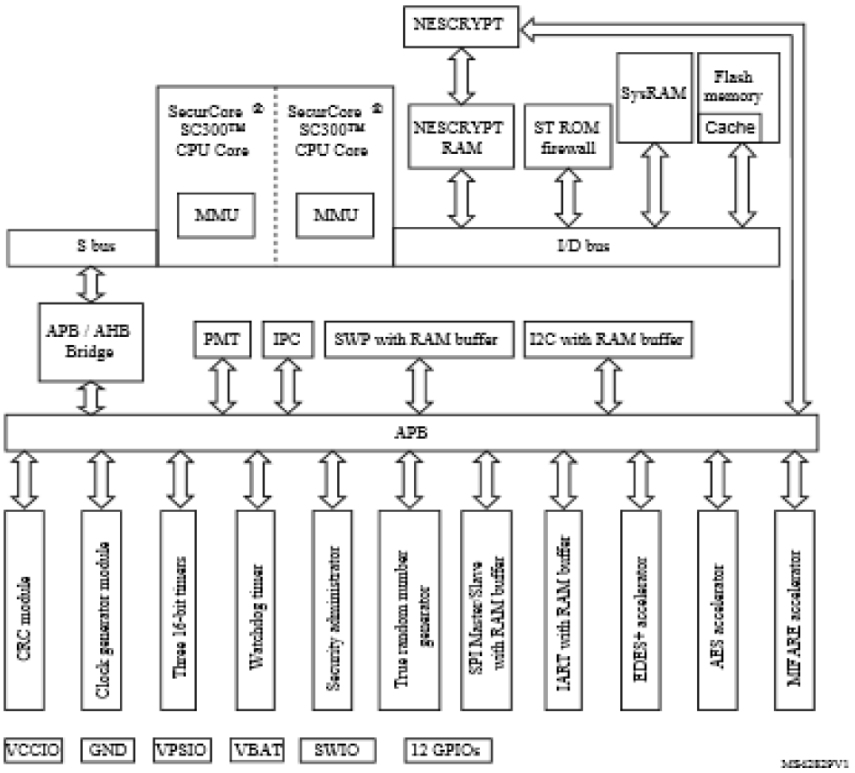

Figure 2 : Architecture du microcontrôleur ST54J A01

L'architecture matérielle du microcontrôleur « ST54J A01 » est illustrée par la figure 2. Elle comporte principalement :

- un processeur Secure SC300 ™ core 32-bit ARM ;
- des mémoires ROM, *Flash* (jusqu'à 2048Ko de mémoire utilisateur) et RAM (dont 64Ko 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[1] muni d'une RAM dédiée pour le support des algorithmes cryptographiques asymétriques.

La partie logicielle est composée de :

- un logiciel dédié, nommé OST[2], 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*).

1.2.4. 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 :

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur ST54J A01	*IC masket name*	K520B
	IC version C	43
	Master identification number	01 CA
Identification des logiciels embarqués	*Firmware version 3.1.2*	03 01 02
	OST version 09.01	09 01
Identification des bibliothèques	*N/A*	N/A

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 « ST54J_SE firmware V3 - User manual », voir [GUIDES].

[1] Bien que dans le périmètre de l'évaluation, le crypto-processeur NESCRYPT (NExt Step CRYPTography) n'adresse pas de SFR spécifique dans la cible de sécurité [ST].
[2] *Operating System for Test* – sytème d'exploitation pour test.

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] :

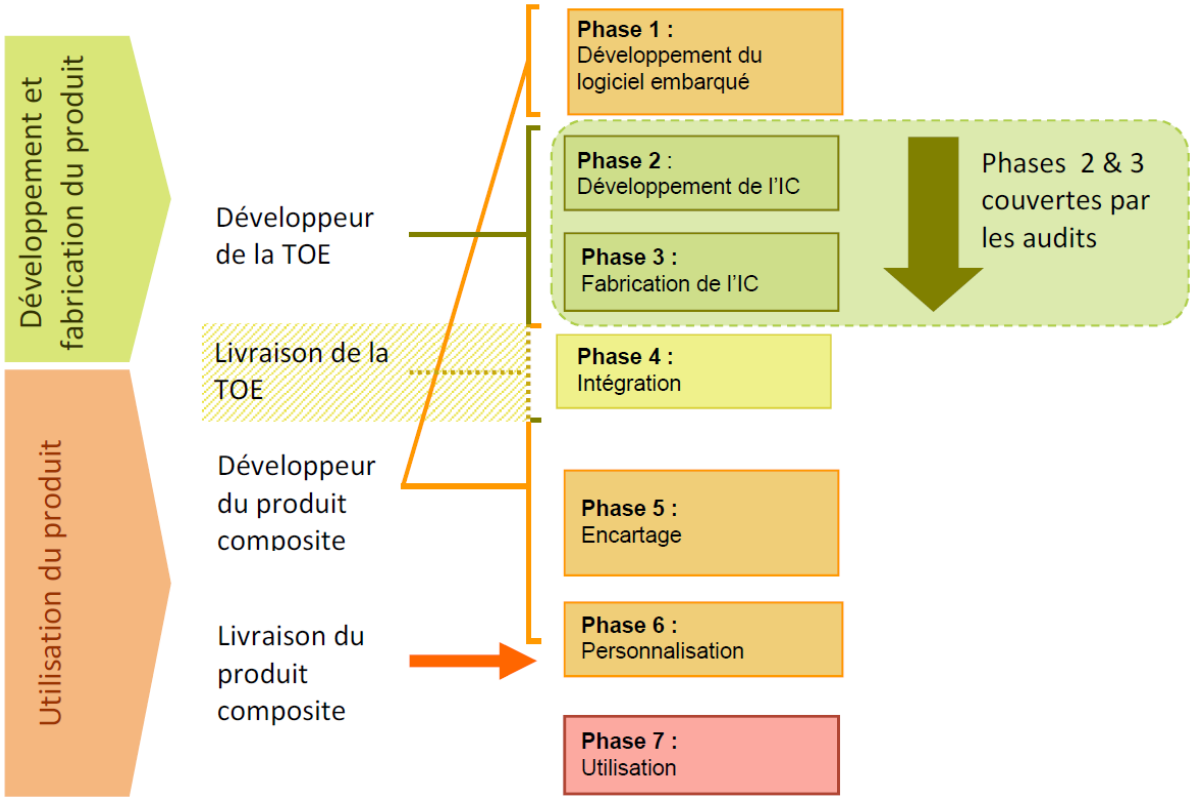

Figure 3 : Cycle de vie du produit

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 :

- conception du circuit ;
- développement du logiciel dédié.

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

- intégration et fabrication du masque ;
- fabrication du circuit ;
- test du circuit ;
- préparation ;
- pré-personnalisation du microcontrôleur.

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

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

Les sites impliqués dans le cycle de vie pour les phases 2, 3 et 4 sont indiqués dans la table 15 de la cible de sécurité [ST], (voir [SITES] pour les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés).

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

1.2.6. Configuration évaluée

Le certificat porte sur le microcontrôleur tel que définis au chapitre 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 à l'issue de la phase 4 lorsque le produit est livré en boîtiers (micro-modules, etc.).

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 5 avril 2019, 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 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 produit « ST54J A01» 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 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.

Ce certificat donne une appréciation de la résistance du produit « ST54J A01 » 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 composant 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 EAL 7 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 EAL 2 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	**1**	Implementation representation of the TSF
	ADV_INT					2	3	3	**2**	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**4**	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	**4**	Production support, acceptance procedures and automation
	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									
	ALC_LCD			1	1	1	1	2	**1**	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	**2**	Compliance with implementation standards
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	**3**	Testing: modular 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 : - ST54J A01 Security Target, référence SMD_ST54J_ST_17_001, version A01.3, mars 2019. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST54J A01 Security Target for composition, référence SMD_ST54J_ST_17_002, version A01.3, mars 2019.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - Peacock 1 project, référence PEACOCK1_ETR_v1.1, version 1.1, 05/04/2019. 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 - Peacock 1 project, référence PEACOCK1_ETR_Lite_v1.1, version 1.1, 05/04/2019.
[CONF]	Liste de configuration du produit : ST33-K520 configuration list, référence ST54_CFGl_18_001, version 1.0, 18/12/2018.
[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.*
[GUIDES]	- NFC controller and secure element system in package - ST54J datasheet, référence DS_ST54J, version 0.5, novembre 2018 ; - ST54J platform SE subsystem OS developer's guide - Preliminary user manual, référence UM_ST54J_SE, version 6, novembre 2018 ; - ST54J platform SE subsystem Security guidance, référence AN_SECU_ST54J_SE, version 2, octobre 2018 ; - ST54J_SE firmware V3 - User manual, référence UM_ST54J_SE_FWv3, version 5, octobre 2018 ; - 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_0037, version F3c, 31 janvier 2008 ; - ARM® Core SC300 Product Errata, référence ARM-EPM-041935 (précédemment PR326-PRDC-009983), version 11, 24/02/2015 ; - ST54J_SE platform - AIS31 compliant random number - User manual, référence UM_ST54J_SE_AIS31, version 1, mars 2018 ; - ST54J_SE platform - AIS Reference implementation: Startup, on-line and total failure tests – AN, référence AN_ST54J_SE_AIS1, version 1, avril 2017.

[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - ALC Class Evaluation Report – STM Project, référence STM_GEN_v1.0, version 1.0, 18 octobre 2018 ; - ALC Class Evaluation Report – STM Project, référence STM_GEN_v2.0, version 2.0, 21 décembre 2018 ; - ALC Class Evaluation Lite Report – C15P0036 Project, référence C15P0036_GEN_Lite_V1.0, version 1.0, 2 juin 2016 ; - ALC Class Evaluation Report – C15P0036 Project, référence C15P0036_ALC_GEN_V2.0, version 2.0, 11 juillet 2018 ; - Site Technical Audit Report – STM Sophia, référence STM_Sophia_STAR_v1.0, version 1.0, 28 décembre 2018 ; - Site Visit Lite Report – STM ROUSSET site audit, référence 17-0317_STM-ROUSSET_SVR-M_v1.1, version 1.1, 20 juillet 2018 ; - Site Visit Lite Report – STM CROLLES site audit, référence STM_Crolles_SVR-M_v1.0, version 1.0, 18 juillet 2018 ; - Site Visit Lite Report – STM Zaventem site audit, référence 16-0227-STM-ZAV_SVR-M_v1.0, version 1.0, 14 juin 2017 ; - Site Visit Lite Report – STM Rennes site audit, 16-0227-STM-RNS_SVR-M_v1.0, version 1.0, 20 juillet 2017 ; - Site Visit Lite Report – STM Grenoble, 16-0227_STGrenoble_SVR-M_v1.0, version 1.0, 13 septembre 2017 ; - Sites Visit Report Lite – STM AMK1, Loyang & Calamba site audits, référence 17-0317-STM_SVR-M_v1.0, version 1.0, 20 décembre 2017 ; - Site Visit Lite Report – DPE site audit, référence 17_0317_SVR-DPE-M_v1.0, version 1.0, 21 décembre 2017 ; - Site Visit Lite Report – Toa Payoh site audit, référence 17-0317_TPY_SVR-M_v1.0, version 1.0, 12 mars 2018 ; - Site Visit Lite Report – STM Tunis site audit, référence 16-0227-STM-TNS_SVR-M_v1.0, version 1.0, 20 octobre 2017 ; - Site Visit Lite Report - ATT1 & ATT3 site audit, référence 17-0317_AMKOR-Taiwan_SVR-M_v1.1, version 1.1, 25 janvier 2019 ; - Site Technical Audit Report – Winstek, référence STM-WIN_STAR_v1.1, version 1.1, 19 décembre 2018 ; - Site Technical Audit Report – DNP, référence STM-DNP_STAR_v1.1, version 1.1, 19 décembre 2018.

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 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 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.