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-2019/11

J-SAFE3 sur ST31G480
Version 1.2.5

Paris, le 27 février 2019

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

Guillaume POUPARD
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2019/11

Nom du produit

J-SAFE3 sur ST31G480

Référence/version du produit

Version 1.2.5

Conformité à un profil de protection

Java Card System – Closed Configuration Protection Profile, version 3.0, décembre 2012

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

STMicroelectronics S.r.l.
Z.I. Marcianise SUD
81025 MARCIANISE, Italy

STMicroelectronics
190 avenue Célestin Coq – ZI de Rousset
BP2 – 13106 Rousset Cedex, France

Commanditaire

STMicroelectronics S.r.l.
Z.I. Marcianise SUD, 81025 MARCIANISE, Italy

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.

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 « J-SAFE3 sur ST31G480, version 1.2.5 ». Il s'agit d'une plateforme Java Card, en configuration fermée, développée par *STMICROELECTRONICS S.R.L.* et embarquée sur le microcontrôleur « ST31G480 A04 » fabriqué par *STMICROELECTRONICS*.

La plateforme est une carte à puce offrant les modes contact et/ou sans contact. Elle est en configuration fermée, elle ne correspond donc pas à un produit utilisable en tant que tel. Elle est destinée à héberger une ou plusieurs applications (dite *applets* dans la terminologie Java Card). Ces dernières ne sont pas couvertes par la présente évaluation. Elles peuvent revêtir un caractère sécuritaire différent (selon qu'elles soient « sensibles » ou « basiques ») et doivent être chargées et instanciées avant émission du produit (*pre-issuance*).

Ce produit 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.

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection [PP JCS]. La conformité est démontrable.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont décrits au chapitre 7.7 de la cible de sécurité [ST]. Ils comprennent notamment :

- la gestion du cloisonnement entre les différents modules gérés par la plateforme Java Card ;
- la gestion sécurisée des fonctionnalités de la plateforme Java Card, de la mémoire, des opérations sur les clefs et de l'état de fonctionnement de la plateforme ;
- la gestion des clefs : génération, distribution, accès et destruction ;
- les opérations cryptographiques de chiffrement/déchiffrement et signature/vérification, et la génération de nombres aléatoires ;
- la gestion transactionnelle garantissant l'exécution complète de la transaction ;
- la gestion et les opérations sur le PIN ;
- la gestion de la libération de la mémoire ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications ;
- la gestion des fonctionnalités offertes par le microcontrôleur sous-jacent.

1.2.3. Architecture

Le produit est constitué :

- du microcontrôleur « ST31G480 A04 » et de la librairie cryptographique associée « NesLib v4.2.10 », certifiés sous la référence [CER-IC] ;
- de la plateforme « J-SAFE 3 » composée :
  - d'un système d'exploitation (*OS*) natif fournissant au système Java Card une interface aux fonctionnalités du microcontrôleur et composé :
    - d'un gestionnaire de mémoire *Memory Management* ;
    - d'un gestionnaire de communication *Communication*,
  - d'un système Java Card (*JCS*), développé selon le standard *Java Card 3.0.4* et contenant, notamment :
    - un environnement d'exécution *(Runtime Environment*) ;
    - une machine virtuelle Java Card (*Virtual Machine)* ;
    - des interfaces de programmation *Java Card*,
  - d'interfaces de programmation propriétaires (*Proprietary API*) ;
  - d'un module développé selon le standard *Global Platform 2.2.1 (GP API)* fournissant notamment les fonctionnalités Global Platform de gestion du cycle de vie, de canal sécurisé, de Global PIN et de gestion contrôlée du contenu de la carte,
- d'un gestionnaire d'applications (*Card Manager*).

La cible d'évaluation[1] est décrite au chapitre 7.1.6 de la cible de sécurité [ST]. Elle porte sur les éléments illustrés par la figure suivante. Le *Card Manager* et les *applets* pouvant être chargées en *pre-issuance* (« *unkown applications* » selon [OPEN]) n'en font pas partie.

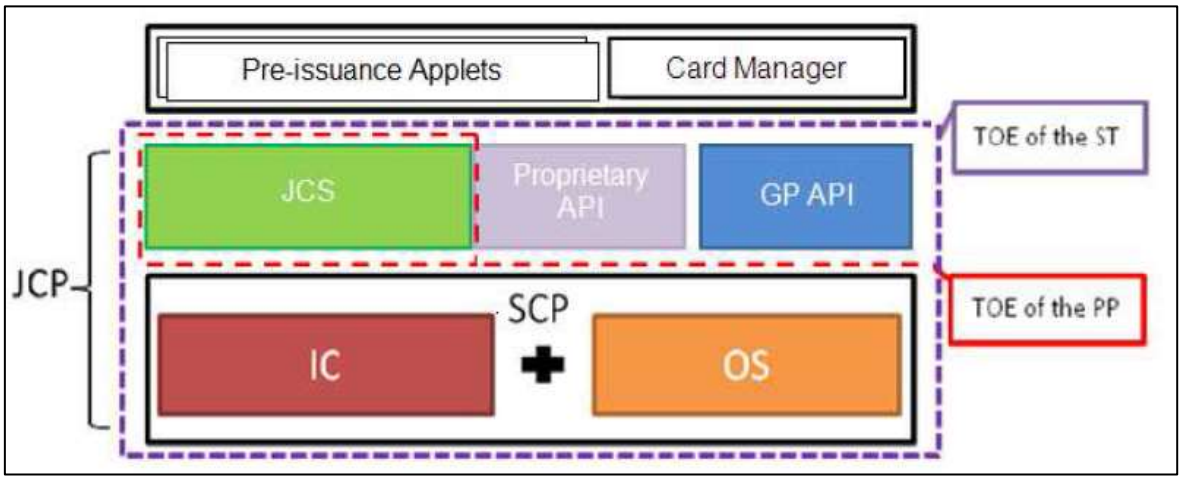

Figure 1 : Architecture de la TOE

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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 7.1 « ST Introduction » et dans le document « J-SAFE3 release manifest » (voir [GUIDES]).

[1] *Target of evaluation (TOE)*

Eléments de configuration		Origine
Nom et version du produit	J-SAFE3 v1.2.5	*STMICROLECTRONICS S.R.L*
Nom et version de la TOE	J-SAFE3 on ST31G480, v1.2.5	
Identification de la plateforme	'00 00 00 7F' (J-SAFE3 OS ID) '00 01 02 05' (pour 1.2.5)	
Identification du microcontrôleur	'00 B8' (ST31G480) '02 01 00' (version du *firmware*) '01 04 02 0A' (version de la Neslib)	*STMICROLECTRONICS*

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET DATA avec les tags :
- « FF04 » pour l'identification de la plateforme ;
- « FF06 » pour l'identification du microcontrôleur.

La procédure d'identification est décrite dans le guide « User manual, J-SAFE3 Java Card platform » (voir [GUIDES]).

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au chapitre 7.1.7 « TOE Life-Cycle » de la cible de sécurité [ST]. Il est décomposé en quatre étapes, qui reprennent les sept phases du [PP0084] :
- étape 1 : développement (phase 1) ;
- étape 2 : fabrication (phase 2 à 5) ;
- étape 3 : personnalisation (étape 6) ;
- étape 4 : utilisation (étape 7).

Le produit a été développé sur les sites suivants :

Site de développement de l'application et la plateforme	Sites de développement du microcontrôleur
STMICROELECTRONICS S.R.L. Z.I. Marcianise, 81025 Maricianise, Italie (voir [SITE])	Voir [CER_IC]

Le point de livraison de la TOE se situe :
- soit en sortie de la phase 3 (voir figure 2). Dans ce cas, des applications peuvent être chargées en phase 1 ou en phase 3, la construction du produit est effectuée par le fabriquant du microcontrôleur, sur un site audité (voir [CER-IC]) ;
- soit en sortie de la phase 5 (voir figure 3). Dans ce cas, des applications peuvent être chargées en phase 1 ou en phase 5, la construction du produit est effectuée sur le site de développement de la plateforme, voir [SITE].

De plus, le guide [AGD-App] décrit les règles de développement des applications destinées à être chargées sur cette carte ainsi que les règles de vérification qui doivent être appliquées par l'autorité de vérification.

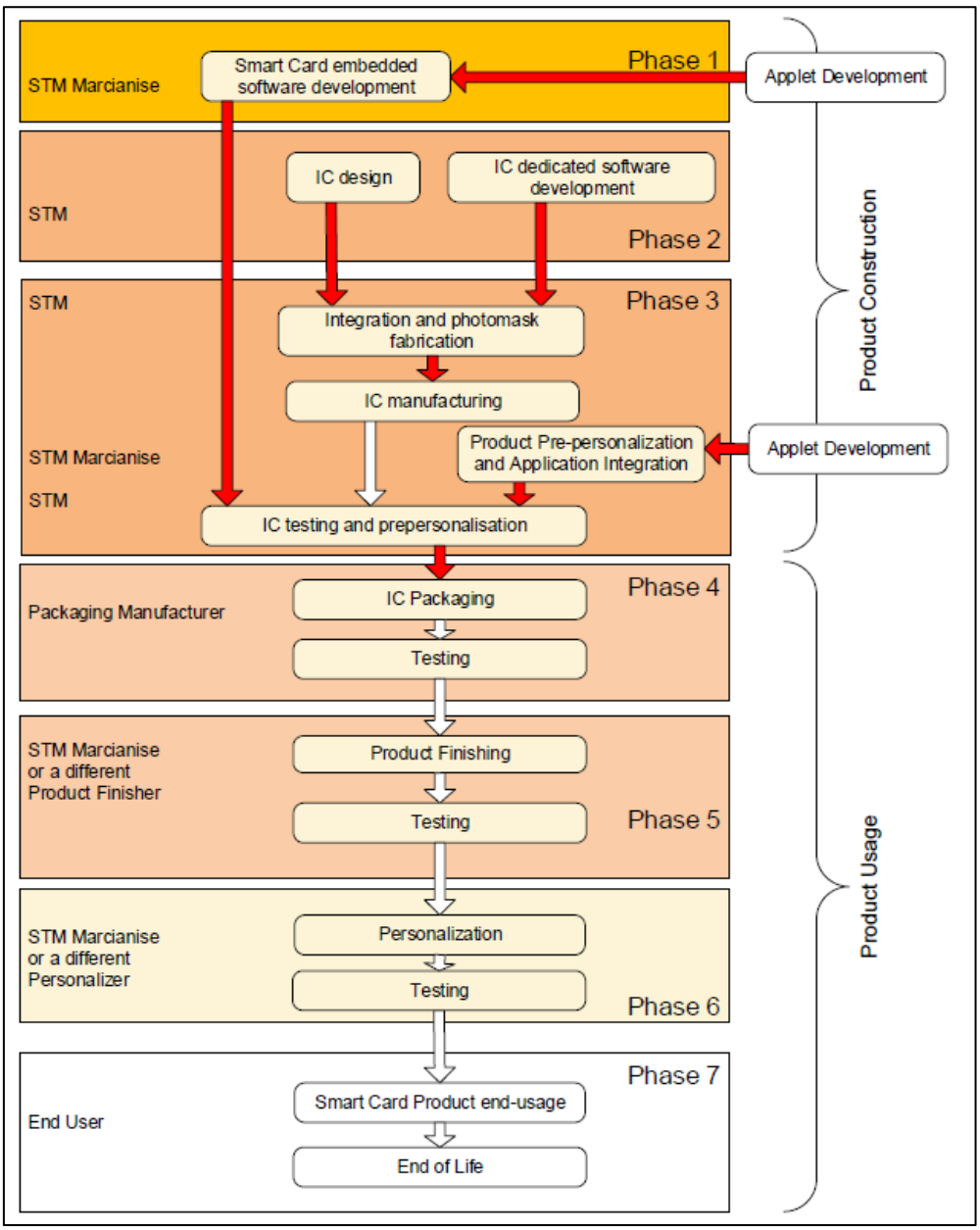

Figure 2 : Cycle de vie, point de livraison en phase 3

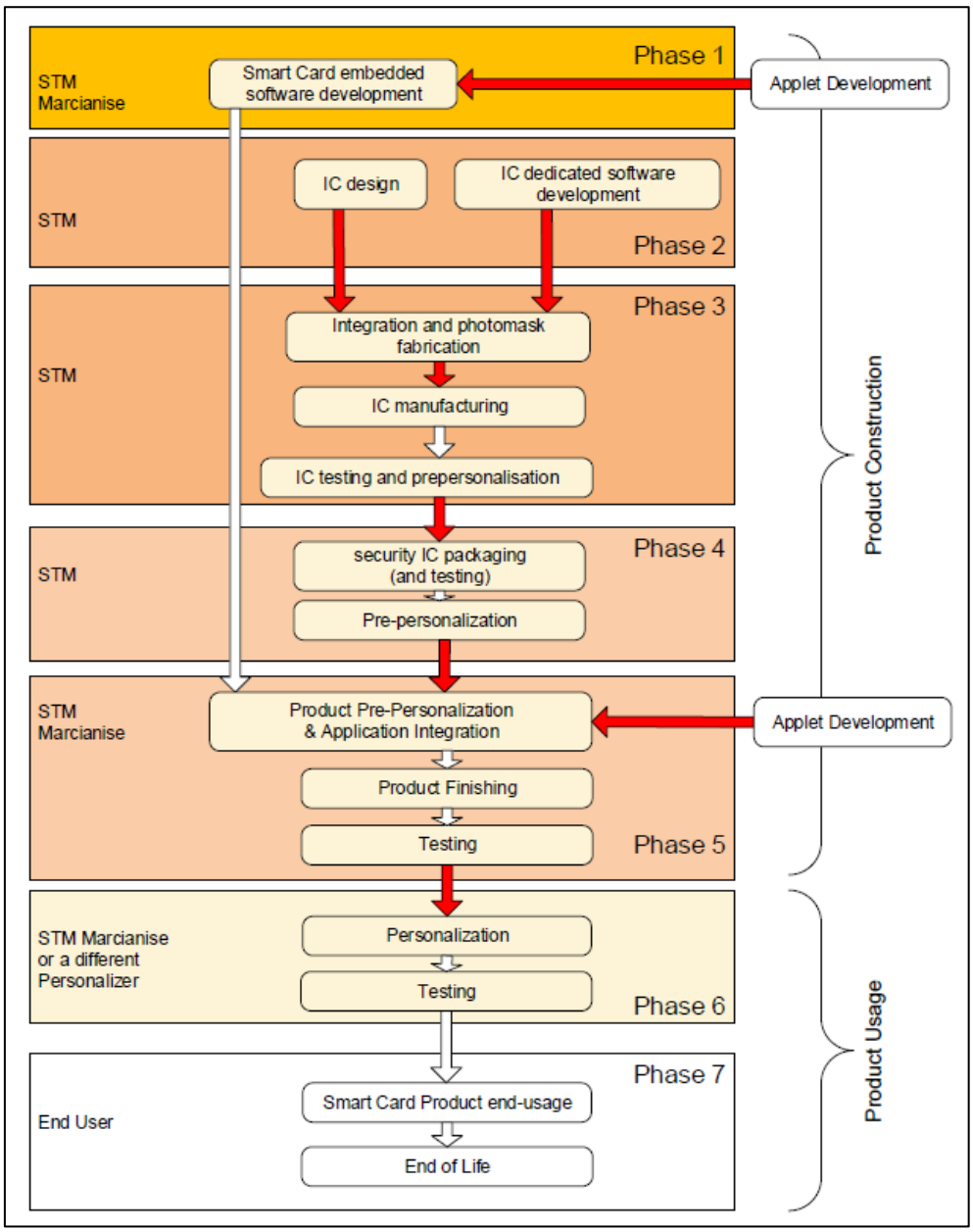

Figure 3 : Cycle de vie, point de livraison en phase 5

1.2.6. Configuration évaluée

Le certificat porte sur la plateforme Java Card fermée « J-SAFE3 », masquée sur le microcontrôleur « ST31G480 », telle qu'elle est présentée au chapitre 1.2.3 « Architecture » et identifiée au chapitre 1.2.4 « Identification du produit ».

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

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 « ST31G480 A04 including optional cryptographic livrairy NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X » au niveau EAL5 augmenté des composants ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, ASE_TSS.2 et AVA_VAN.5, conforme au profil de protection [PP0084].

Ce microcontrôleur a été certifié le 25 août 2016 sous la référence ANSSI-CC-2016/58 (voir [CER-IC]) et maintenu le 16 juin 2017 sous la référence ANSSI-CC-2016/58-M02 (voir [MAI-IC]). Le niveau de résistance du microcontrôleur a été confirmé le 18 juillet 2018 dans le cadre du processus de surveillance, voir [SUR-IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 21 novembre 2018, 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 produit comporte un générateur de nombres aléatoires qui a fait l'objet d'une évaluation selon la méthodologie [AIS31], il répond aux exigences des classes DRG.3, comme revendiqué dans la cible de sécurité [ST]. Ainsi, comme requis dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

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 « J-SAFE3 sur ST31G480, version 1.2.5 » 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.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- les autorités de vérification doivent appliquer le guide [AGD-App] ;
- la protection du chargement de toutes les applications chargées *pre-issuance* doit être activée conformément aux indications de [AGD-App].

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)

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

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	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 : - JSAFE3 on ST31G480 Security Target, référence DM00517937, version 4.0, 15 octobre 2018, *STMICROLECTRONICS S.R.L.*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - J-SAFE3 on ST31G480 Security Target – Public Version, référence J-SAFE3_ST_Lite_C, version C, février 2019, *STMICROELECTRONICS S.R.L.*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report JSAFE-3 Project, référence JSAFE_3_ETR_v1.1, version 1.1, 21 novembre 2018, *SERMA SAFETY & SECURITY*. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ETR Lite for Composition JSAFE-3 Project, référence JSAFE_3_ETR_v1.1_lite, version 1.1, 21 novembre 2018, *SERMA SAFETY & SECURITY*.
[CONF]	Liste de configuration du produit : - JSAFE3 Configuration List, référence jsafe3_ConfigList, 16 novembre 2018, *STMICROELECTRONICS S.R.L.*.
[GUIDES]	Guide d'installation, d'administration et d'utilisation du produit : - JSAFE3 on ST31G480 – Guidance Document (AGD), référence DM00517960, version 4, 15 octobre 2018, *STMICROELECTRONICS S.R.L.* ; - User manual J-SAFE3 Java Card platform, référence UM_J-SAFE3, version 3, 6 juin 2018, *STMICROELECTRONICS S.R.L.* ; - J-SAFE3 release manifest, référence RN_J-Safe3_RM, version 3, 11 septembre 2018 *STMICROELECTRONICS S.R.L.* ; - User Manual – Proprietary API Documentation, référence J-SAFE3_UserManual_Annex_Rev_B, version B, 28 mai 2018, *STMICROELECTRONICS S.R.L.*. Guide de développement d'applications [AGD-App] : - Security Guidelines of application development on the JSAFE3 secure solution, référence AN_SECU_J-SAFE3, version 5, octobre 2018, *STMICROELECTRONICS S.R.L.*.

[SITE]	Rapports d'analyse documentaire et d'audit de site pour la reutilisation : - STMicrolectronics S.r.l. Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence 17_v1.0, version 1.0, 7 mai 2018, *SERMA SAFETY & SECURITY*. - Site Technical Audit Report Marcianise, référence ALC_GEN_STMAR_STAR_v1.0, version 1.0, 7 janvier 2019, *SERMA SAFETY &SECURITY*.
[PP JCS]	Java Card System – Closed Configuration Protection Profile, version 3.0, décembre 2012. *Certifié par l'ANSSI sous la reference ANSSI-CC-PP-2010/07 et maintenu sous le reference ANSSI-CC-2010/07-M01*.
[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.*
[CER-IC]	ST31G480 A02 including optional cryptographic livrairy NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X. *Certifié par l'ANSSI le 25 août 2016 sous la reference ANSSI-CC-2016/58.*
[MAI-IC]	ST31G480 A04 including optional cryptographic livrairy NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X. *Maintenu par l'ANSSI le 16 juin 2017 sous la reference ANSSI-CC-2016/58-M02.*
[SUR-IC]	ST31G480 A02 including optional cryptographic livrairy NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X. *Surveillés par l'ANSSI le 18 juillet 2018 sous la reference ANSSI-CC-2016/58-S02.*

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.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5, octobre 2017.
[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]	Functionnality classes and evaluation methodology for physical random number generator, AIS31, version 1, 25 septembre 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).
[OPEN]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013.

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