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-2019/05

J-SIGN version 1.8.9

Paris, le 11 janvier 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-2019/05

Nom du produit

J-SIGN version 1.8.9

Référence/version du produit

Version EEPROM : 1.8.9

Version ROM : 1.6.0

Conformité à un profil de protection

Protection profiles for secure signature creation device:

Part 2: Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-01 ;
Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012 ;
Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012.

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

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

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

Commanditaire

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

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.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « J-SIGN version 1.8.9 » développée par *STMICROELECTRONICS S.R.L* et embarquée sur le microcontrôleur SB23YR80 fabriqué par *STMICROELECTRONICS*.

Ce produit est destiné à être utilisé comme dispositif de création de signature électronique (SSCD[1]) dans le cadre du déploiement de la CIE/CNS (carte italienne d'identité et de services au citoyen italienne telle que spécifiée dans le document [CNS]).

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 aux profils de protection *Protection profiles for Secure Signature Creation Device* [PP-SSCD-Part2], [PP-SSCD-Part4] et [PP-SSCD-Part5].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la génération et la gestion de paires de clés de signature (SCD[2]/SVD[3]) ;
- la protection de la clé privée SCD ;
- l'export sécurisé de clé publique SVD vers une application de création de certificat (CGA[4]) ;
- l'export sécurité des données à signer (DTBS[5]) et des données de vérification d'authentification (VAD[6]) à partir d'une application de création de signature (SCA[7]) ;
- l'authentification du signataire par un code PIN[8] et administration du code PIN ;
- la création de signature électronique.

1.2.3. Architecture

Le produit est constitué :

- l'application « J-Sign » en version 1.8.9 ;
- la plateforme « J-Safe » en configuration fermée et développée selon les standards *Java Card 3.0.4* et *Global Platform 2.1.1* ;

[1] *Secure Signature Creation Device.*
[2] *Signature Creation Data.*
[3] *Signature Verification Data.*
[4] *Certifiation Generation Application.*
[5] *Data To Be Signed.*
[6] *Verification Authentification Data.*
[7] *Signature Creation Application.*
[8] *Personal Identification Number.*

- le microcontrôleur « SB23YR80 » et la librairie cryptographique associée « Neslib v3.1 », certifié sous la référence [CER-IC].

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 le guide [AGD_PRE] :

Eléments de configuration		Origine
Référence de la TOE	J-SIGN V1.8.9	*STMICROELECTRONICS S.R.L.*
Identification du produit	“4A 2D 53 69 67 6E” (J-Sign) “01 89” (version EERPOM 1.8.9) “01 60” (version ROM 1.6.0)	
Référence du circuit intégré	SB23YR80	*STMICROELECTRONICS*

Ces éléments peuvent être vérifiés par l’utilisation de la commande GET DATA ou de la commande GET TRACEABILITY. La procédure d’identification est décrite dans le guide [AGD_OPE].

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au chapitre 6.4 « TOE life cycle » de la cible de sécurité [ST] et illustré par la figure suivante :

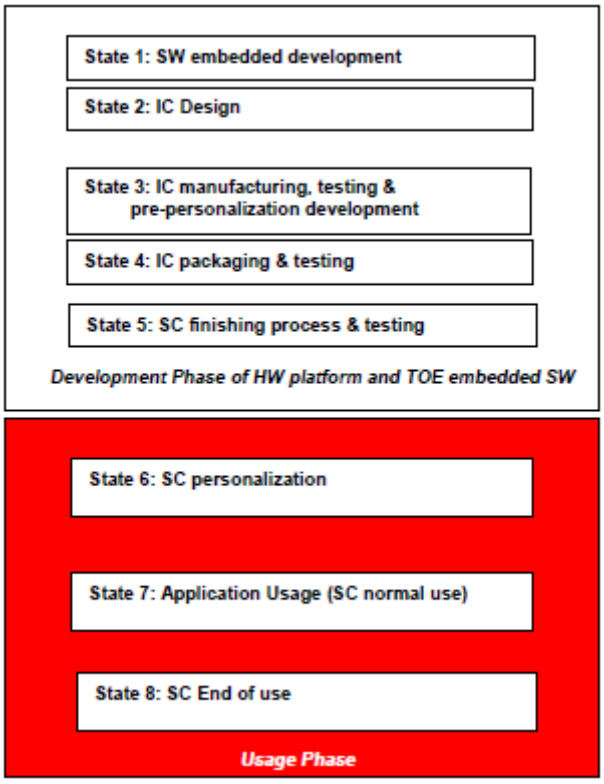


Figure 1 : Cycle de vie

Le périmètre de l'évaluation se limite aux phases 1 à 5 :

- les phases 1 « *SW embedded development* » et 2 « *IC Design* » correspondent au développement du produit (« *SSCD development* » dans le profil de protection [PP-SSCD-Part2]) ;
- les phases 3 « *IC manufacturing, testing & pre-personalization development* », 4 « *IC packaging & testing* » et 5 « *SC finishing process & testing* » correspondent à la phase de production du produit telle que décrite dans [PP-SSCD-Part2]. Il est à noter que le point de livraison du produit est en sortie de phase 5.

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 [STAR])	Voir [CER_IC]

1.2.6. Configuration évaluée

Le certificat porte sur le logiciel composé de l'application « J-Sign » en version 1.8.9 et de la plateforme Java Card « J-Safe » en configuration fermée, masqué sur le microcontrôleur SB23YR80, tel qu'il est présenté au chapitre « 1.2.3 Architecture » et identifié dans le 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 « SB23YR80 » au niveau EAL6 augmenté du composant ALC_FLR.1 et conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 4 janvier 2013 sous la référence ANSSI-CC-2012/68, voir [CER_IC]. Le niveau de résistance du microcontrôleur a été confirmé le 30 avril 2018 dans le cadre du processus de surveillance, voir [SUR_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 3 janvier 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 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, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).
Par ailleurs, 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-SIGN version 1.8.9 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

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

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].

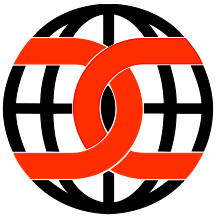
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 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].

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

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 4+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	**4**	Complete functional specification
	ADV_IMP				1	1	2	2	**1**	Implementation representation of TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**3**	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	**4**	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			1	1	1	2	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	**1**	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	**1**	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	**2**	Analysis of coverage
	ATE_DPT			1	1	3	3	4	**1**	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	**1**	Functional testing
	ATE_IND	1	2	2	2	2	2	3	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - J-Sign EIDAS, Security Target, révision H, 18 juillet 2018, référence J-SIGN_EIDAS_SecurityTarge, *STMICROELECTRONICS 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-Sign EIDAS Security Target – Public Version, révision A, 26 juillet 2018, référence J-SIGN_EIDAS_Security_Target_Lite, *STMICROELECTRONICS S.R.L.*
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – JSIGN2 project, version 1.1, 3 janvier 2019, référence JSIGN2_ETR_v1.1, *SERMA SAFETY & SECURITY.*
[STAR]	Site Technical Audit Report Marcianise, version 1.0, 7 janvier 2019, référence ALC_GEN_STMAR_STAR_v1.0, *SERMA SAFETY & SECURITY.*
[CONF]	Liste de configuration du produit : - J-SIGN Configuration List, 19 juillet 2018, référence J-SIGN_ConfigList, *STMICROELECTRONICS S.R.L.*
[GUIDES]	Guide de préparation du produit [AGD_PRE] : - J-SIGn - Preparative Procedures, révision E, 12 juillet 2018, référence AGD_PRE, *STMICROELECTRONICS S.R.L.* Guide d'utilisation du produit [AGD_OPE] : - J-SIGn-eIDAS - Operational User Guidance, révision F, 29 juin 2018, référence AGD_OPE, *STMICROELECTRONICS S.R.L.*
[PP-SSCD-Part2]	Protection profiles for secure signature creation device – Part 2: Device with key generation, référence : prEN 14169-2:2012, version 2.0.1 datée du 23 janvier 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.*
[PP-SSCD-Part4]	Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, référence : prEN 14169-4:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.*
[PP-SSCD-Part5]	Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, référence : prEN 14169-5:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.*

[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]	Microcontrôleurs SA23YR48B/SB23YR48B/SA23YR80B/SB23YR80B. *Certifiés par l'ANSSI le 4 janvier 2013, sous la référence ANSSI-CC-2012/68 et maintenus le 13 décembre 2016 sous la référence ANSSI-CC-2012/68-M01.*
[SUR-IC]	Microcontrôleurs SA23YR48B/SB23YR48B/SA23YR80B/SB23YR80B. *Surveillés par l'ANSSI le 30 avril 2018, sous la référence ANSSI-CC-2012/68-S05.*
[CNS]	CNS – Carta Nazionale dei Servizi Functional Specification, version 1.1.6, 2 Avril 2011.

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 1.5.1, mai 2018.
[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.

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