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-2015/17

Application J-Sign version 1.8.4 sur la plateforme J-Safe version 2.11.0

Paris, le 21 mai 2015

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

[Original signé]
Guillaume POUPARD

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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2015/17

Nom du produit

Application J-Sign version 1.8.4 sur la plateforme J-Safe version 2.11.0

Référence/version du produit

Version 1.8.4

Conformité à un profil de protection

[PP-0006] Protection Profile - Secure Signature Creation Device Type 3, version 1.05.

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

AVA_VAN.5

Développeurs

STMicroelectronics S.r.l. - Incard Division

Z.I Marcianise Sud,
81025 Marcianise,
Italie

STMicroelectronics

29 Boulevard Romain Rolland,
75669 Paris Cedex 14,
France

Commanditaire

STMicroelectronics S.r.l. – Incard Division

Z.I Marcianise Sud, 81025 Marcianise, Italie

Centre d'évaluation

Serma Technologies

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

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

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 « Application J-Sign version 1.8.4 sur la plateforme J-Safe version 2.11.0 » développée par STMicroelectronics S.r.l. – Incard Division et STMicroelectronics.

Cette carte fournit une application de création de signature électronique utilisée dans le cadre du déploiement de la CIE/CNS (carte d'identité et de services au citoyen) italienne.
Cette application est une applet *Java Card 3.0.4* embarquée sur la plateforme J-Safe en configuration fermée.

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-0006], adapté dans la cible à la version 3.1 des [CC] (ce PP ayant été rédigé selon la version 2.1 des CC).

1.2.2. 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 :

Configuration Items		Origin
Commercial name	J-SIGN V1.8.4	STMicroelectronics S.r.l. - Incard Division
TOE reference (CM label)	J-Sign (EEPROM patch version 1.8.4 / ROM version 1.6.0)	
TOE version	v1.8.4	
TOE patch reference	N/A	
OS ROM reference (J-Safe CM label)	J-Safe on SB23YR80B v.2.11.0 / 0x66 (Mask ID)	
OS version	v2.11.0	
OS patch reference	0x00021100 (Platform Patch Code ID)	
IC identifier	SB23YR80B	STMicroelectronics
IC identifier with TOE (J-Safe Maskset)	SB23YR80B (Maskset K2M0A, external Rev. B, internal Rev. H or I)	STMicroelectronics

Les éléments d'identification de la TOE peuvent être obtenus par les commandes GET CARD et GET TRACEABILITY (voir [GUIDES]) :

Application Name	0x4A 0x2D 0x53 0x69 0x67 0x6E // ASCII code of the string J-Sign
ROM Version	0x01 0x60 // Ver 1.6.0
EEPROM patch Version	0x01 0x84 // Ver 1.8.4

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la génération et la gestion de paires de clefs de signature (SCD/SVD[1]) ;
- l'export de clefs de vérification de signature vers une Application de Création de Certificats (CGA – *Certificate Generation Application*), l'import et le stockage de certificats ;
- l'initialisation du code d'authentification de l'utilisateur (PIN – *Personal Identification Number*) ;
- l'identification et l'authentification des utilisateurs et des applications autorisées par l'intermédiaire d'un PIN ;
- la création de signature électronique.

Ils sont détaillés au chapitre 10 de [ST].

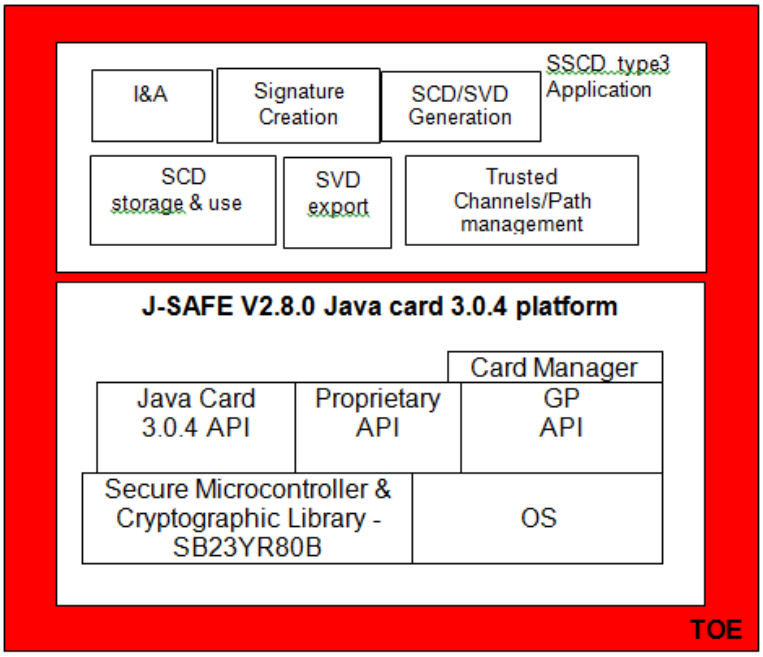
[1] Signature Creation Data / Signature Validation Data

1.2.4. Architecture

La TOE est constitué des éléments suivants:

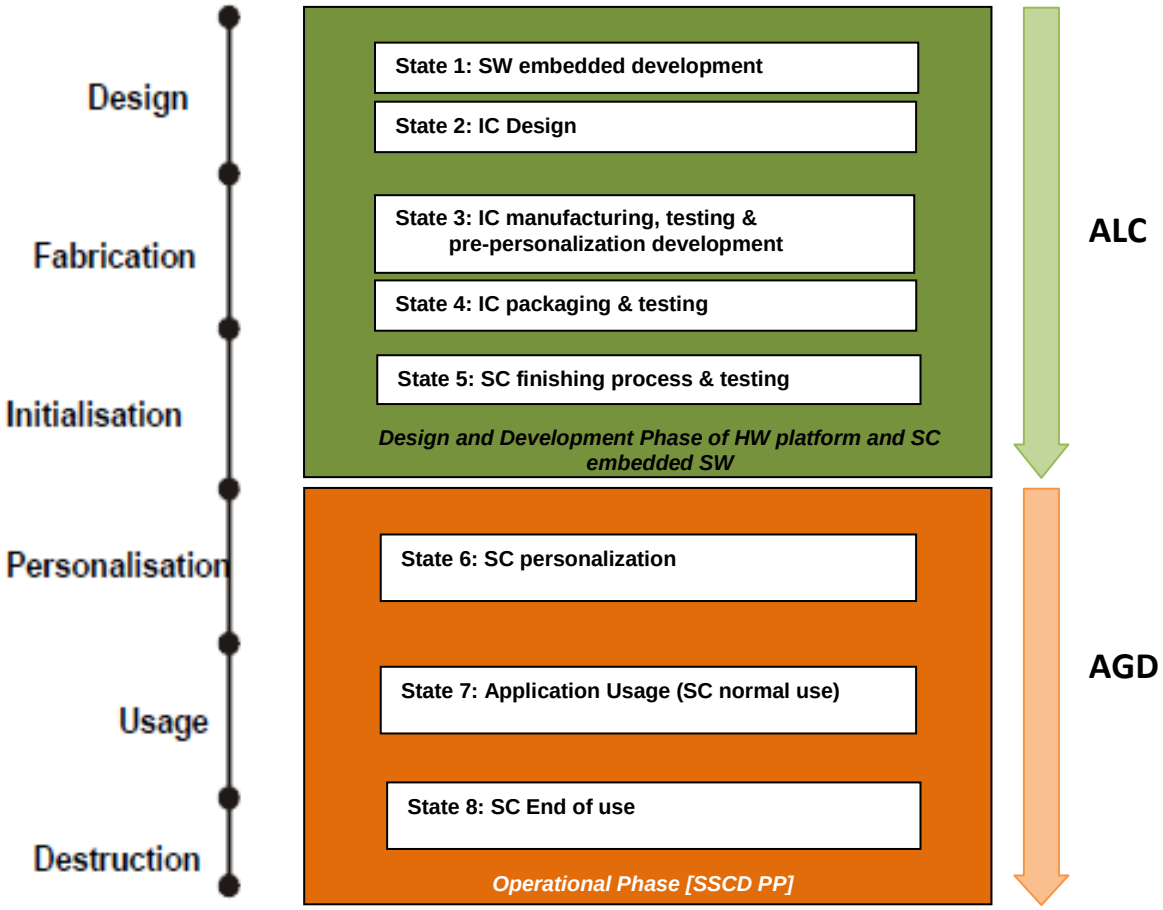
- l'application J-Sign ;
- la plateforme Java Card J-Safe ;
- le microcontrôleur SB23YR80, révision B.

Cette architecture est illustrée par le schéma suivant :



1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :



Le produit a été développé sur les sites suivant :

Site de développement de l'application

STMicroelectronics S.r.l. – Incard Division
Z.I. Marcianise,
81025 Maricianise,
Italie

Sites de développement de la plateforme

Voir [CER_PTF].

Le cycle de vie évalué au titre de la tâche ALC correspond aux phases de :

- conception (design) ;
- fabrication ;
- initialisation.

1.2.6. Configuration évaluée

Le certificat porte sur l'application J-Sign, embarquée en ROM sur la plateforme Java Card J-Safe en configuration fermée.
Aucune autre application n'est embarquée sur la carte.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [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 de l'application sur la plateforme déjà évaluée par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la « Plateforme J-Safe, en configuration fermée, version 2.11.0, sur le composant SB23YR80B » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP JCS] (voir [CER PTF]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 15 avril 2015, 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 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, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur sous-jacent à la plateforme J-Safe (voir [CER IC]).
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 « Application J-Sign version 1.8.4 sur la plateforme J-Safe version 2.11.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté du composant 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 puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. 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] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs.
Pour les évaluations enregistrées avant septembre 2014, la reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR.

[1] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

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	**1**	Identification 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 SECURITY TARGET, Référence 8434034 Version G
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report J-Sign Project, JSIGN_ETR_v1.1, Version 1.1.
[CONF]	Liste de configuration du produit : - Configuration List, Référence J-Sign_ConfigList 04/11/2014
[GUIDES]	Guide de préaparation du produit : - J-SIGN PREPARATIVE PROCEDURE, Référence 8539678, Version B. Guide d'utilisation du produit : - J-SIGN OPERATIONAL USER GUIDANCE, Référence 8539617, Version D.
[PP-0006]	Protection Profile — Secure Signature-Creation Device Type 3, version 1.05, 25 juillet 2001. *Certifié par le BSI sous la référence BSI-PP-0006-2002.*
[PP JCS]	Java Card protection profile – Closed configuration, Version 3.0, décembre 2012. *Certifié sous la reference ANSSI-CC-PP-2010/07 et maintenu sous la reference ANSSI-CC-PP-2010/07-M01.*
[CER IC]	Microcontrôleurs SA23YR48B/SB23YR48B/SA23YR80B/SB23YR80B. *Certifiés le 4 janvier 2013, sous la référence ANSSI-CC-2012/68.*
[CER PTF]	Plateforme J-Safe, en configuration fermée, version 2.11.0, sur le composant SB23YR80B, certifiée sous la référence ANSSI-CC-2015/16 le 15 mai 2015.

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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-001; Part 2: Security functional components, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-002; Part 3: Security assurance components, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-004.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[JIWG IC] *	Mandatory Technical Document – The Application of CC to Integrated Circuits, version 3.0, février 2009.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, janvier 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.

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