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-2019/16

JSAFE3_EPASS BAC
(Rev. M)

Paris, le 9 avril 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-2019/16

Nom du produit

JSAFE3_EPASS BAC

Référence/version du produit

Rev. M

Conformité à un profil de protection

Machine Readable Travel Document with "ICAO Application", Basic Access Control

version 1.10, 25 mars 2009, BSI-CC-PP-0055-2009

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2

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

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 « JSAFE3_EPASS BAC, Rev. M » développé par *STMICROELECTRONICS S.R.L.*, en configuration fermée. Il s'agit d'une application en composition sur la plateforme Java Card « J-SAFE3 » embarquée sur le microcontrôleur « ST31G480 A04 » fabriqué par *STMICROELECTRONICS*.

Le produit certifié est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit est destiné à permettre la vérification de l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels, dans une *eCover* ou dans une *eDatapage*. Le produit final peut prendre différentes formes, de carte ou de module, avec et/ou sans contact.

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 [PP BAC].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont décrits au chapitre 5.3.3 de la cible de sécurité [ST]. Ils comprennent notamment :

- la protection en intégrité des données du porteur stockées dans la carte : nations ou organisations émettrices, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- l'authentification du microcontrôleur par le mécanisme optionnel « *Active Authentication* » ou « *Chip Authentication* » ;
- l'authentification entre le microcontrôleur et le système d'inspection lors du contrôle aux frontières par le mécanisme BAC (« *Basic Access Control* ») ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de « *Secure Messaging* », des données lues.

1.2.3. Architecture

L'architecture du produit est décrite au chapitre 5.3.2 de la cible de sécurité [ST], elle est constituée :

- d'un microcontrôleur ST31G480 A04 développé par *STMICROELECTRONICS* ;
- de la plateforme JSAFE-3 développée par *STMICROELECTRONICS S.R.L.* ;
- de l'application JSAFE3_EPASS BAC développée par *STMICROELECTRONICS S.R.L.*.

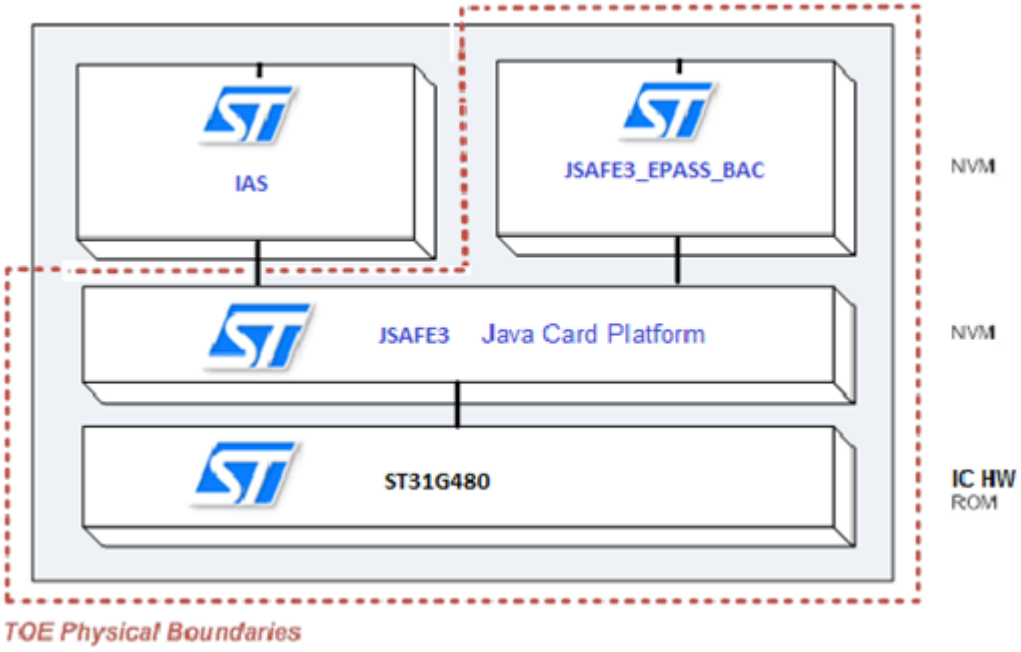


Figure 1

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 [GUIDES].

Eléments de configuration		Origine
Nom et version du produit	JSAFE3_EPASS BAC Rev. M	*STMICROELECTRONICS S.R.L.*
Nom et version de la TOE	JSAFE3_EPASS_BAC V1.0.0	
Identification de l'application	0x'030004' (pour JSAFE3_EPASS V.3.0.4)	
Identification de la TOE	0x'475000B8007F81450005'	

Ces éléments peuvent être vérifiés en utilisant la commande GET DATA, décrites dans [GUIDES] :

- en utilisant le tag « *CPLC data* » (0x9F7F) pour les données de l'application MRTD ;
- en utilisant le tag « *proprietary applet data* » (0x9F7D) pour la version de l'application.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au chapitre 5.3.4 « *TOE Life-Cycle* » de la cible de sécurité [ST]. Il est décomposé en quatre étapes, qui reprennent les sept phases du [PP0084] :

- phase 1 : développement (étape 1 à 2) ;
- phase 2 : fabrication (étape 3 à 5) ;
- phase 3 : personnalisation (étape 6) ;
- phase 4 : utilisation (étape 7).

Le point de livraison de la TOE se situe en sortie de la phase de fabrication (phase 2, étape 3).

Le produit a été développé sur le site suivant :

STMICROELECTRONICS S.R.L.
Z.I. Marcianise, 81025 Maricianise, Italie
(voir [SITE])

Les sites intervenant dans le cycle de vie de la plateforme et du microcontrôleur sont listés respectivement dans [CER-PTF] et [CER-IC].

1.2.6. Configuration évaluée

Le certificat porte sur l'application « JSAFE3_EPASS BAC (rev. M) », en configuration fermée et 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 de la plateforme Java Card « J-SAFE3 » certifiée au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5. Cette plateforme a été certifiée le 27 février 2019 sous la référence ANSSI-CC-2019/11 (voir [CER-PTF]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 19 mars 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.3 visé.

2.4. Analyse du générateur d'aléas

Ce générateur a fait l'objet d'une analyse dans le cadre de l'évaluation de plateforme (voir [CER-PTF]).
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.3 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 « JSAFE3_EPASS BAC, Rev. M » 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 ALC_DVS.2.

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].

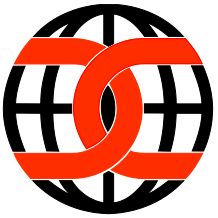
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 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	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - JSAFE3_EPASS BAC Security Target, référence JSAFE3_EPASS_BAC_SecurtyTarget_M, version Rev.M, 23 janvier 2019. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - JSAFE3_EPASS BAC Security Target Public Version, référence JSAFE3_EPASS_BAC_SecurtyTarget_Lite, version Rev.A, 13 mars 2019.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report J-SAFE3 ePass Project, référence J-SAFE3_ePass_ETR_v1.1, version 1.1, 19 mars 2019, *SERMA SAFETY & SECURITY*.
[CER-PTF]	Rapport de certification ANSSI-CC-2019/11, J-SAFE3 sur ST31G480, Version 1.2.5. *Certifié par l'ANSSI le 27 février 2019 sous la référence ANSSI-CC-2019/11*.
[CONF]	Liste de configuration du produit : - icao_mrtd_ConfigList, référence icao_mrtd_ConfigList.txt, *STMICROELECTRONICS S.R.L.*
[GUIDES]	Guides d'installation et d'utilisation du produit : - JSAFE3-EPASS - Operational User Guidance, référence JSAFE3_EPASS_OPE , Rev E, 10 janvier 2019, *STMICROELECTRONICS S.R.L.* ; - JSAFE3-EPASS - Preparative Procedure, référence JSAFE3_EPASS_PRE , Rev F, 15 janvier 2019, *STMICROELECTRONICS S.R.L.*
[SITE]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - 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*.
[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.*

[PP BAC]	Protection Profile, Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.10, 25 mars 2009. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0055-2009.*
[CER-IC]	ST31G480 A02 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X. *Certifié par l'ANSSI le 25 août 2016 sous la référence ANSSI-CC-2016/58.*

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.

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