



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-2018/09

IDEAL Pass v2.2-n -BAC JC ePassport v2.2.0.12

Paris, le 23 mars 2018

*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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

<i>Référence du rapport de certification</i>	ANSSI-CC-2018/09	
<i>Nom du produit</i>	IDEal Pass v2.2-n -BAC JC ePassport	
<i>Référence/version du produit</i>	v2.2.0.12	
<i>Conformité à un profil de protection</i>	Machine Readable Travel Document with “ICAO Application”, Basic Access Control Version 1.10, BSI-CC-PP-0055-2009	
<i>Critères d'évaluation et version</i>	Critères Communs version 3.1 révision 4	
<i>Niveau d'évaluation</i>	EAL 4 augmenté ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_DVS.2, ALC_CMS.5, ALC_TAT.2, ATE_DPT.3	
<i>Développeurs</i>	IDEMIA (ex SAFRAN I&S) 18 Chaussée Jules César, 95520 Osny, France	NXP Semiconductors BU Security & Connectivity Stresenmannellee 101 22505 Hamburg, Germany
<i>Commanditaire</i>	IDEMIA 420 rue d'Estienne d'Orves, 92700 Colombes, France	
<i>Centre d'évaluation</i>	CEA - LETI 17 rue des martyrs, 38054 Grenoble Cedex 9, France	
<i>Accords de reconnaissance applicables</i>		
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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	6
1.2.4. <i>Identification du produit</i>	7
1.2.5. <i>Cycle de vie</i>	7
1.2.6. <i>Configuration évaluée</i>	7
2. L’EVALUATION	9
2.1. REFERENTIELS D’EVALUATION	9
2.2. TRAVAUX D’EVALUATION	9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	9
2.4. ANALYSE DU GENERATEUR D’ALEAS	9
3. LA CERTIFICATION	11
3.1. CONCLUSION	11
3.2. RESTRICTIONS D’USAGE	11
3.3. RECONNAISSANCE DU CERTIFICAT	12
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	12
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	12
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	13
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	14
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	15

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « IDeal Pass v2.2-n -BAC JC ePassport, v2.2.0.12 » et a été développé par *IDEMIA* sur une plateforme Javacard de *NXP SEMICONDUCTORS*.

Le produit évalué est de type « carte à puce » pouvant être utilisé en mode avec et/ou sans contact. Il implémente des fonctions de document de voyage électronique qui se veulent répondre (1) aux spécifications de l'organisation de l'aviation civile internationale (ICAO), et (2) aux préconisations de la Commission Européenne pour les passeports européens biométriques (Décision d'exécution C(2013) 6181) et titres de séjour européens biométriques (Décision d'exécution C(2013) 6178). 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 ou la page de données des passeports traditionnels ou des cartes au format ID1. Ils peuvent être livrés sous forme de module, d'*inlay*, de page de données ou de couverture de passeport. Le produit final peut également être au format carte plastique pour des applications telles que carte d'identité ou carte de résident.

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 [PP0055]. Il s'agit d'une conformité stricte.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- 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 AA (*Active Authentication*) ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de *Secure Messaging*, des données lues.

1.2.3. Architecture

Le produit est constitué :



- de la plateforme « NXP JCOP 3 SECID P60 CS (OSB) », certifiée sous la référence [NSCIB-CC-98209] ;
- de l'applet IDEal Pass v2.2-n développée par IDEMIA, de type MRTD, en configuration SAC/EAC. Le code de l'applet peut se situer soit en ROM ou soit en EEPROM, selon la variante du cycle de vie choisie.

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Le protocole de commandes à exécuter afin d'identifier le produit est décrit dans le guide [AGD_PRE]. La version certifiée du produit est identifiable par les éléments suivants :

- platform ID : JxHyyy0019790400 ;
- platform patch level : 0x0000000000000000 ;
- applet info version : 7125-9301-0311-02.02.00.0012 (lorsque chargée en EEPROM) ou bien 7125-9301-0319-02.02.00.0012 (lorsque chargée en ROM).

1.2.5. Cycle de vie

Le cycle de vie du produit est présenté au chapitre 1.4.3 de la cible de sécurité [ST].

Le développement du produit, couvert par la classe d'assurance ALC de l'évaluation, s'effectue sur les sites suivants :

Nom du Site	Adresse	Phase
Voir [NSCIB-CC-98209]		<i>Development (Phase 1, step 1)</i>
<i>IDEMIA OSNY</i>	18 Chaussée Jules César 95520 Osny, France	<i>Development (Phase 1, step 2)</i>
<i>IDEMIA NOIDA</i>	Rooms D-217 & D-216, Sector 63, Noida 201301, Uttar Pradesh, Inde	<i>Development (Phase 1, step 2)</i>
Voir [NSCIB-CC-98209]		<i>Manufacturing (Phase 2, step 3)</i>
<i>IDEMIA HAARLEM NETHERLAND</i>	Oudeweg 32, 2031 CC Haarlem Pays-Bas	<i>Manufacturing (Phase 2, steps 4 & 5)</i>

Le point de livraison est situé entre la Phase 2 et la Phase 3. Les phases *Personalization of the travel document* (Phase 3) et *Operational use* (Phase 4) sont couvertes par la classe d'assurance AGD de l'évaluation.

1.2.6. Configuration évaluée

Le certificat porte sur la configuration de l'applet IDEal Pass v2.2-n qui inclut les mécanismes suivants, après personnalisation par l'émetteur :

- *Basic Access Control*;

– *Active Authentication.*

Le présent rapport de certification porte également sur la configuration du produit obtenue sans activer le mécanisme optionnel *Active Authentication*.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [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 « NXP JCOP 3 SECID P60 CS (OSB) » au niveau EAL5 augmenté des composants AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 et ALC_FLR.1, conforme au profil de protection [PP-JC]. Cette plateforme a été certifiée le 2 août 2017 sous la référence [NSCIB-CC-98209]. Le microcontrôleur a été certifié sous la référence [BSI-DSZ-CC-0973-2016] ; sa librairie cryptographique a été certifiée sous la référence [NSCIB-CC-15-67206].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 20 décembre 2017, 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 pour cette configuration BAC du produit. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN.3 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 la revendication PTG.2 de [BSI-DSZ-CC-0973-2016]). 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 (voir la revendication DRG.3 de [NSCIB-CC-98209]).

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 « IDeal Pass v2.2-n -BAC JC ePassport, v2.2.0.12 » 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 ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_DVS.2, ALC_CMS.5, ALC_TAT.2, ATE_DPT.3.

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'accord¹, 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].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², 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 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 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	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	Implementation representation of 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	3	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - Security Target, IDeal Pass v2.2-n – BAC JC ePassport, 2016_2000020128 v1.1, 4 décembre 2017, <i>IDEMIA</i>. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Security Target Lite IDeal Pass v2.2-n – BAC JC ePassport, 2017_2000032442 v1.0, 5 décembre 2017, <i>IDEMIA</i>.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report (full ETR) TOUCAN, LETI.CESTI.TOU.RTE.001-v1.0, 8 décembre 2017, <i>CEA-LETI</i>.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - Software release sheet for IDeal Pass v2.2-n, 2016_2000021801, v1.0, 5 décembre 2017, <i>IDEMIA</i>.
[GUIDES] [AGD_PRE] [AGD_OPE]	<p>Preparative procedures for IDeal Pass v2.2-n, 2016_2000021062, v1.8, 9 novembre 2017, <i>IDEMIA</i> ;</p> <p>Operational procedures for IDeal Pass v2.2-n, 2016_2000021061, v1.5, 18 septembre 2017, <i>IDEMIA</i>.</p>
[PP-JC]	<p>Java Card Protection Profile – Open Configuration, version 3.0, May 2012, Oracle Corporation. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01</i>.</p>
[PP0055]	<p>Protection Profile, Machine Readable Travel Document with “ICAO Application”, Basic Access Control, version 1.10, 25 mars 2009. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0055-2009</i>.</p>
[BSI-DSZ-CC-0973-2016]	<p>NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software, BSI-DSZ-CC-0973-2016, 17 juin 2016, mise à jour BSI-DSZ-CC-0973-V2-2016, 11 octobre 2016.</p>
[NSCIB-CC-15-67206]	<p>Certification Report Crypto Library V3.1.x on P6022y VB, NSCIB-CC-15-67206-CR, 28 juillet 2016 ; mise à jour NSCIB-CC-17-67206-CR2, novembre 2017.</p>
[NSCIB-CC-98209]	<p>Certification Report, NXP JCOP 3 SECID P60 CS (OSB), NSCIB-CC-98209, 1 août 2017, mise à jour NSCIB-CC-98209-CR2, 15 janvier 2018.</p>

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 : <ul style="list-style-type: none"> - Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[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 1.4, août 2015.
[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.