



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-2016/80

Applet MICA0 v1.1.3 sur la plateforme IdealCitiz v2.1, en configuration SAC/EAC

Paris, le 13 décembre 2016

*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.

Référence du rapport de certification	ANSSI-CC-2016/80	
Nom du produit	Applet MICA0 v1.1.3 sur la plateforme IdealCitiz v2.1, en configuration SAC/EAC	
Référence/version du produit	Applet v1.1.3, plateforme v2.1, configuration SAC/EAC	
Conformité à un profil de protection	Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP) Version 1.3.2, BSI-CC-PP-0056-V2-2012-MA-02 Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) Version 1.0, BSI-CC-PP-0068-V2-2011	
Critères d'évaluation et version	Critères Communs version 3.1 révision 4	
Niveau d'évaluation	EAL 5 augmenté ALC_DVS.2, AVA_VAN.5	
Développeurs	MORPHO 18 Chaussée Jules César, 95520 Osny, France	INFINEON Technologies AG AIM CC SM PS – Am Campeon 1-12, 85579 Neubiberg, Allemagne
Commanditaire	Safran Identity & Security (anciennement MORPHO) 18 Chaussée Jules César, 95520 Osny, France	
Centre d'évaluation	CEA - LETI 17 rue des martyrs, 38054 Grenoble Cedex 9, France	
Accords de reconnaissance applicables		
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	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>	8
1.2.6. <i>Configuration évaluée</i>	8
2. L’EVALUATION	10
2.1. REFERENTIELS D’EVALUATION	10
2.2. TRAVAUX D’EVALUATION	10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	10
2.4. ANALYSE DU GENERATEUR D’ALEAS	11
3. LA CERTIFICATION	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS D’USAGE	12
3.3. RECONNAISSANCE DU CERTIFICAT	13
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	13
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	13
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	14
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	15
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	17

1. Le produit

1.1. Présentation du produit

Le produit évalué est l'Applet MICA0 v1.1.3 sur la plateforme IdealCitiz v2.1, en configuration SAC/EAC ; l'applet et la plateforme ont été développées par *MORPHO* sur un microcontrôleur d'*INFINEON*.

Le produit évalué 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 (OACI¹). 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. Ils peuvent être livrés sous forme de module, d'*inlay*, de couverture de passeport ou de passeport. Le produit final peut également être au format carte plastique.

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 [PP0056V2]. Il s'agit d'une conformité stricte. Le profil de protection [PP0056V2] est strictement conforme au profil de protection [PP0068V2]. La cible de sécurité est donc également strictement conforme à [PP0068V2].

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*) ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme SAC (*Supplemental Access Control*) ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de *Secure Messaging*, des données lues ;

¹ Encore appelé ICAO pour *International Civil Aviation Organization*.

- l'authentification forte (avec validation de la chaîne de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme EAC (*Extended Access Control*) préalablement à tout accès aux données biométriques.

1.2.3. Architecture

Le produit est constitué :

- de la plateforme ouverte cloisonnante « IDEal Citiz v2.1 Open platform » (voir [ANSSI-CC-2015/45]) ;
- de l'application MICA0 procurant les services eMRTD ;
- d'une autre application, nommée ID.me, évaluée par ailleurs (voir [ANSSI-CC-2016/64]).

La cible d'évaluation (TOE) est constituée de l'application MICA0 v1.1.3 sur la plateforme Ideal Citiz v2.1.

Par ailleurs, l'application ID.me de type SSCD a été prise en compte dans le processus d'évaluation conformément aux prescriptions de [JIL_OPEN] applicables aux *known applications*. Cette application ID.me v1.12 a été vérifiée conformément aux contraintes de développements d'applications décrites dans le guide [PLF_BADR] de la plateforme.

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 suivants :

- 1) La méthode d'identification de la plateforme est présentée dans [PLF_AGD_PRE] :
 - les *Card Production and Life Cycle (CPLC) Data* indiquent les valeurs suivantes :

Donnée	Valeur attendue
IC Fabricator	0x8100
IC Type	0x7805
Operating System Identifier	0x4921
Operating System Release Date	0x5079
Operating System Release Level	0x2101

- la valeur de la donnée *Hardware security integrity* est 0x448C448C48C6.
- 2) La méthode d'identification de l'applet MICA0 est présentée dans le guide [MICA0_AGD_PRE] :

- les Executable Load Files et Executable Module suivants sont présents :

Objet	AID
MICA0 Executable Load File	A00000024710
MICA0 Executable Module	A0000002471001

- la version de l'applet MICA0 est 01.01.03.0001 (dans la réponse à la commande Get Info Version).

3) La méthode d'identification de l'applet ID.me est présentée dans le guide [ID.me_AGD_PRE] :

- les Executable Load Files et Executable Module suivants sont présents :

Objet	AID
ID.me Executable Load File	A0000000024349444D45
LJFS Executable Load File	A000000002434C4A4653
ID.me Executable Module	A0000000024349444D4501

- la version de l'applet ID.me est 1.12 (0x01 0x0C dans la réponse à la commande GetDataForID.MeVersion).

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 [BSI-0782-V2]		<i>Development (Phase 1, step 1)</i>
<i>MORPHO OSNY</i>	18 Chaussée Jules César 95520 Osny, France	<i>Development (Phase 1, step 2)</i>
Voir [BSI-0782-V2]		<i>Manufacturing (Phase 2, step 3)</i>
<i>MORPHO CARDS CZECH</i>	Jelinkova 1174/3A 72100 Ostrava République Tchèque	<i>Manufacturing (Phase 2, steps 3, 4 & 5)</i>

Le point de livraison est situé entre la Phase 2 et la Phase 3. Les phases *Personalisation of the travel document* (Phase 3) et *Operational use* (Phase 4) sont couvertes par la classe d'assurance AGD de l'évaluation. Les applications ID.me et MICA0 sont chargées avant le point de livraison. Aucune autre *known application* n'est considérée.

Si des applications supplémentaires sont chargées en phase *Personalization of the travel document* (Phase 3), ces applications doivent avoir été développées et être chargées en respectant les contraintes de la plateforme (voir guides [PLF_BADR], [PLF_SADR], [PLF_VAR], [PLF_AGD_PRE]).

1.2.6. Configuration évaluée

La configuration ouverte du produit a été évaluée conformément à [JIL_OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification et réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.

Le présent rapport de certification porte également sur la configuration du produit obtenue sans embarquer l'application ID.me.

Le certificat porte sur la configuration de l'applet MICA0, après personnalisation par l'émetteur, qui inclut les mécanismes suivants :

- *Extended Access Control*;
- *Supplemental 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 [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 « Ideal Citiz v2.1 Open Platform » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP-JC]. Cette plateforme ouverte a été certifiée le 2 octobre 2015 sous la référence [ANSSI-CC-2015/45].

Le niveau de résistance du microcontrôleur a été confirmé le 3 novembre 2015, voir [BSI-0782-V2]. Le niveau de résistance de la plateforme ouverte a été confirmé le 29 janvier 2016 dans le cadre du processus de surveillance, voir [ANSSI-CC-2015/45-S01].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 1^{er} décembre 2016, 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 a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations données au chapitre 6 du guide [MICA0_AGD_PRE] doivent être suivies.

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.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI ([RTE]) sur le code développé par *MORPHO* ; elle se base sur la certification *AVA_VAN.5* du microcontrôleur et de ses bibliothèques cryptographiques ([BSI-0782-V2]). Ces 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.

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 [BSI-0782-V2]). 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 « Applet MICA0 v1.1.3 sur la plateforme IdealCitiz v2.1, en configuration SAC/EAC » 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 :

- dans le cadre de la qualification renforcée du produit, les recommandations au chapitre 6 du guide [MICA0_AGD_PRE] doivent être suivies ;
- toutes les futures applications chargées sur ce produit doivent respecter les contraintes de développement de la plateforme (guides [PLF_BADR] et [PLF_SADR] selon la sensibilité de l'application considérée) ;
- les autorités de vérification doivent appliquer le guide [PLF_VAR] ;
- la protection du chargement de toutes les applications sur ce produit doit être activée conformément aux indications de [PLF_AGD_PRE].

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 puces 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.

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 lorsque les dépendances CC sont satisfaites.

Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



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.

² 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, le Qatar, 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 5+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical 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 for Product Citiz 2.1 : Micao 1.1.3 on Ideal Citiz OS 2.1, SAC/EAC configuration, 2014_0000002308, v08, 30 novembre 2016, Morpho. <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 for Micao 1.1.3 on IdealCitiz OS v2.1, SAC/EAC configuration, 2016_2000022974, v1.0, 6 décembre 2016, Morpho.
[RTE]	Evaluation Technical Report -LETI.CESTI.FAL.RTE.026 - v1.1 – 1 ^{er} décembre 2016, CEA Leti
[ANA-CRY]	Cotation des mécanismes cryptographiques Application MICA0, LETI.CESTI.FAL.RT.011, v1.0, 20 octobre 2016
[CONF]	Software Release Sheet for MICA0, 2015_2000008933, version 3.4, 30 novembre 2016, Morpho.
<p>[GUIDES]</p> <p>[MICA0_AGD_PRE]</p> <p>[MICA0_AGD_OPE]</p> <p>[ID.me_AGD_PRE]</p> <p>[PLF_BADR]</p> <p>[PLF_SADR]</p> <p>[PLF_VAR]</p> <p>[PLF_AGD_PRE]</p> <p>[PLF_AGD_OPE]</p>	<p>MICA0 Preparative procedures, 2015_2000006884, v7.0, 25 octobre 2016, Morpho.</p> <p>MICA0 Operational Guidance, 2015_2000006882, v3.0, 1 décembre 2016, Morpho.</p> <p>ID.me Preparative Guide, 2014_2000002907, v1.3, 20 octobre 2015, Morpho.</p> <p>Ideal Citiz v2.1 – Basic Applet Development Recommendations, réf. 2014_2000001499, version 1.0, 7 juillet 2014, Morpho.</p> <p>Ideal Citiz v2.1 – Secure Applet Development Recommendations, réf. 2014_2000001501, version 1.3, 3 décembre 2015, Morpho.</p> <p>Ideal Citiz v2.1 – Verification Authority Rules, réf. 2014_2000001513, version 1.0, 7 juillet 2014, Morpho.</p> <p>Preparative procedure for IDEalcitiz v2.1, réf 2014_2000003597, version 07, 31 juillet 2015, Morpho.</p> <p>Operational user guidance IDEalcitiz_v2.1, réf 2014_2000004459, version 03, 31 juillet 2015, Morpho.</p>
[PP-JC]	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>

[PP0068V2]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, 2 novembre 2011. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011.</i>
[PP0056V2]	Protection Profile - Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), version 1.3.2, 5 décembre 2012. <i>Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.</i>
[ANSSI-CC-2015/45]	IDEal Citiz v2.1 Open platform, Rapport de certification ANSSI-CC-2015/45, 2 octobre 2015.
[BSI-0782-V2]	Rapport de certification BSI-DSZ-CC-0782-V2-2015 for Infineon M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware), 3 novembre 2015, BSI.
[ANSSI-CC-2015/45-S01]	IDEal Citiz v2.1 Open platform, Rapport de surveillance ANSSI-CC-2015/45-S01, 29 janvier 2016.
[ANSSI-CC-2016/64]	Applet ID.me v1.12 sur la plateforme IDEal Citiz v2.1, Rapport de certification ANSSI-CC-2016/64, 11 octobre 2016.

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, 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 1.2, janvier 2012.
[JIL_OPEN]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013.
[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]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), 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.