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-2010/35

Carte CC IDeal Citiz (sur composant SB23YR48B), version 1.4.5 Application ICAO BAC

Paris, le 9 juin 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

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-2010/35

Nom du produit

Carte CC IDeal Citiz (sur composant SB23YR48B)

Référence, version du produit

IDEAL/ST23YR48/1.4.5, Version 1.4.5

Conformité à un profil de protection

[PP BAC]
Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.10

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 4 augmenté

ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3

Développeurs

SAGEM Sécurité
Etablissement d'Osny, 18 Chaussée Jules César, 95520 Osny, France

ST Microelectronics
29 Boulevard Romain Rolland, 75669 Paris cedex 14, France

Commanditaire

SAGEM Sécurité
Etablissement d'Osny, 18 Chaussée Jules César, 95520 Osny, France

Centre d'évaluation

CEA - LETI
17 rue des martyrs, 38054 Grenoble Cedex 9, France
Tél : +33 (0)4 38 78 40 87, mél : cesti.leti@cea.fr

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, publié au Journal officiel de la République française. 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 CC IDeal Citiz (sur composant SB23YR48B), IDEAL/ST23YR48/1.4.5, Version 1.4.5 » développée par SAGEM Sécurité et ST Microelectronics.

Le produit évalué est de type carte à puce duale, avec et sans contact. Il est composé :

- de trois applications :
  - l'application AIP qui permet de réaliser les opérations de pré-personnalisation et de personnalisation de la carte. Cette application n'est plus accessible une fois la TOE en phase opérationnelle (étape 7 du cycle de vie du produit) ;
  - l'application ICAO qui réalise les fonctions du passeport électronique et qui peut être instanciée plusieurs fois (plusieurs jeux de données architecturés en autant d'arborescences de données distinctes) ;
  - l'application IAS (Identité Authentification Signature), qui permet de générer, détruire et charger des clés pour créer des signatures électroniques ;
- d'une plateforme ouverte Java qui permet de charger des applets, durant la phase opérationnelle.

1.2. Description du produit

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]. Cette évaluation n'a donc porté que sur l'application ICAO BAC.

1.2.1. Identification du produit

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

La version certifiée du produit est identifiable à partir des éléments suivants :

- nom et version du produit : CC IDeal Citiz, version 1.4.5 ;
- nom et version du microcontrôleur : SB23YR48B ;
- référence commerciale du produit (SAGEM) : IDEAL/ST23YR48/1.4.5 ;
- référence complète du logiciel embarqué (SAGEM ORGA) OFFICIEL_IDEAL_ST23YR80_1_4_50 ;
- référence fondeur (ST Microelectronics) : SB23YR48 QPX (puce masquée).

La version certifiée du produit peut être vérifiée :

- en mode contact :
  - par les octets T3 à T11 suivants des 15 octets d'historique de l'ATR[1] :
    « 49 44 65 61 6C 5F 31 2E 34 » en héxadécimal => « IDeal 1.4 »;
  - ou par les octets en position 8 et 9 du CPLC[2] (obtenu après ouverture du BAC, en mode s*ecure messaging* par la commande GET DATA avec un tag égal à « 9F7F ») :

    « 14 50 » =>« 1.4.5 » ;
- en mode sans contact :
  - par les octets 3 et 4 suivants de l'ATQB[3] :

    « 14 50 » => « 1.4.5 » ;
  - ou par les octets en position 8 et 9 du CPLC (cette lecture étant dans ce cas conditionnée par un paramètre de la carte) :

    « 14 50 » =>« 1.4.5 ».

1.2.2. Services de sécurité

Les principaux services de sécurité évalués fournis par la TOE sont :

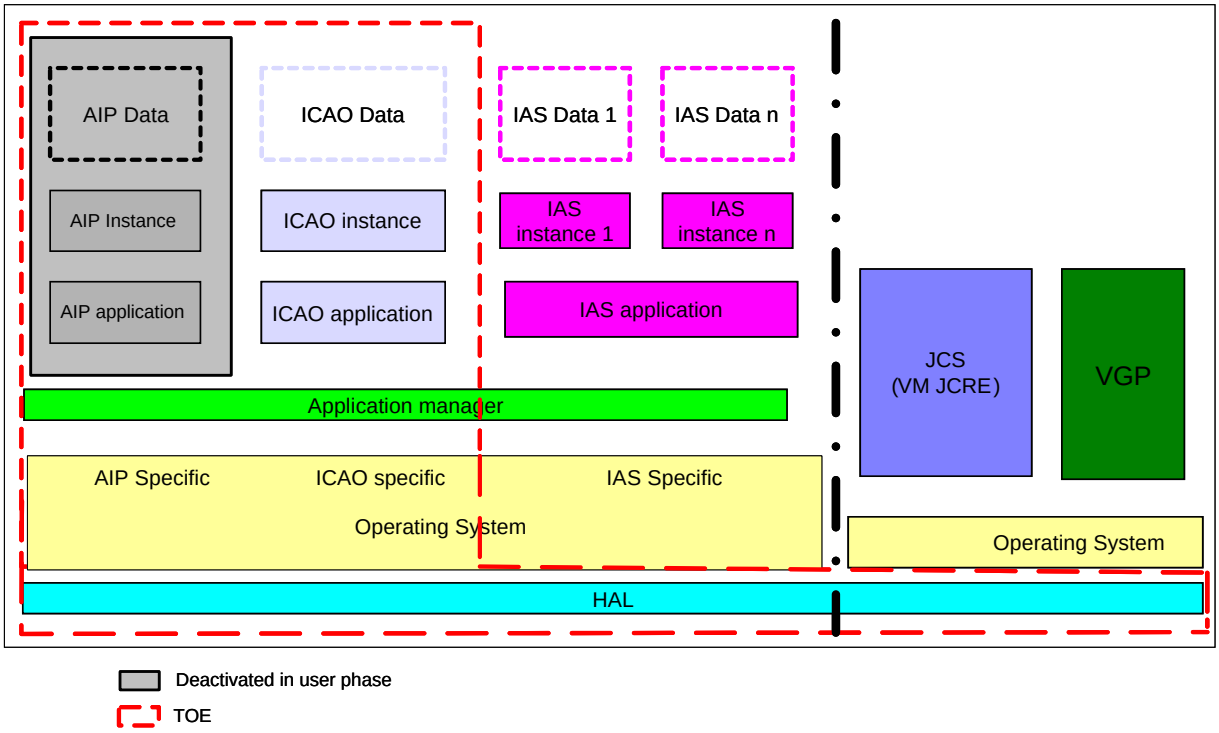
- la protection de l'intégrité des données du porteur stockées dans la carte : pays ou organisation de délivrance, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait du porteur, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme BAC (*Basic Access Control*) ;
- la protection de l'intégrité et de la confidentialité des données lues à l'aide du mécanisme *secure messaging*.

1.2.3. Architecture

Le produit est constitué :

- du microcontrôleur SB23YR48B, développé et fabriqué par ST Microelectronics ;
- des parties logicielles, développées par SAGEM Sécurité, de référence CVS OFFICIEL_IDEAL_ST23YR80_1_4_00, et masquées dans la ROM du microcontrôleur, composé :
  - du système d'exploitation OPUCE ;
  - de la couche d'abstraction du matériel HAL (Hardware Abstract Layer) ;
  - du JavaCard System ;
  - de l'application d'initialisation et de personnalisation de la carte AIP ;
  - des applications IAS et ICAO ;
- du patch de l'application IAS, version 5.0, développé par SAGEM Sécurité et chargé en EEPROM.

[1] Answer To Reset
[2] Card Production Life Cycle
[3] Answer to reQuest type B

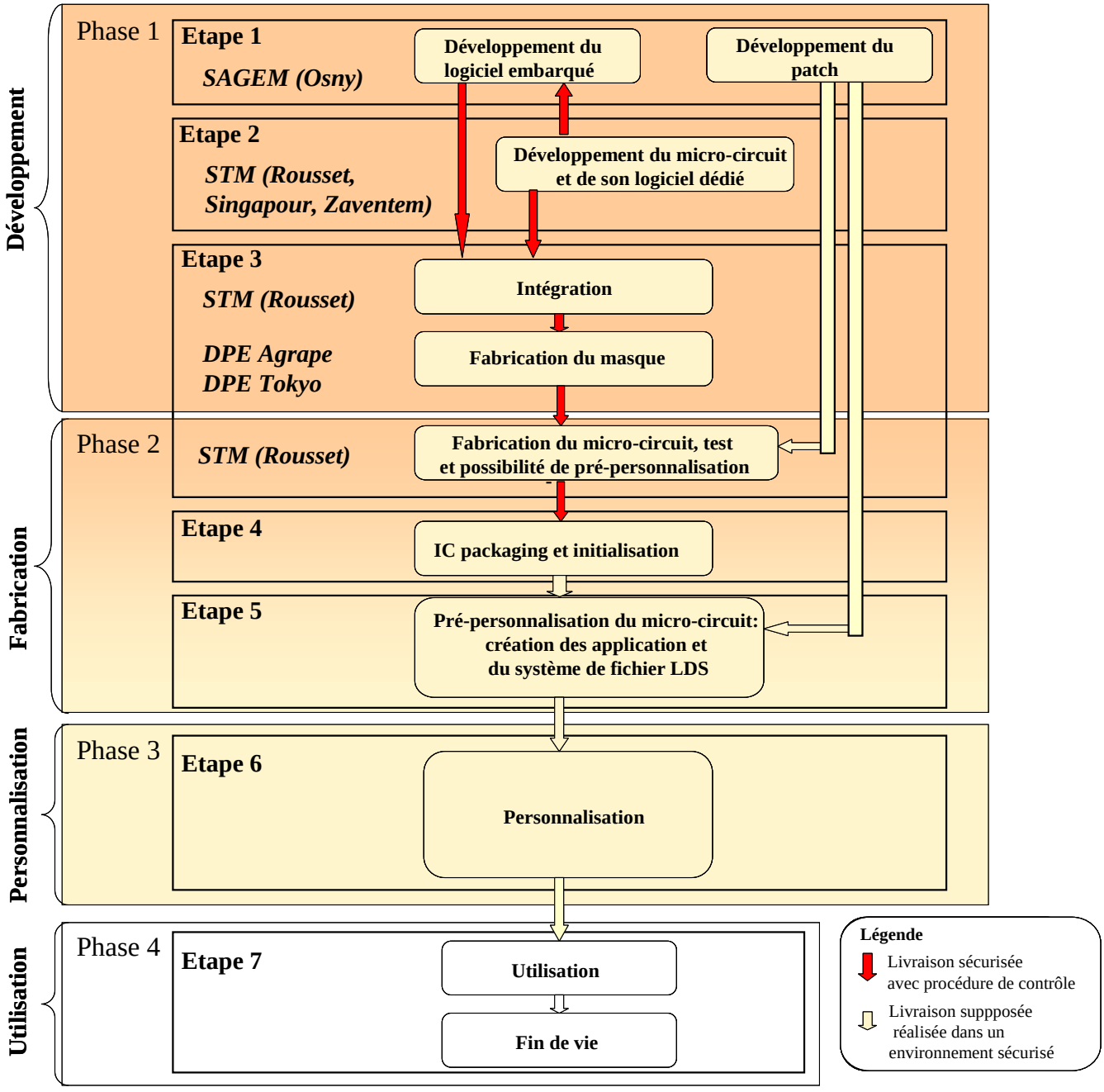


La TOE correspond à l'application ICAO, associée aux fonctionnalités et services du système d'exploitation et du microcontrôleur requis pour mettre en œuvre les fonctionnalités de cette application.

Le CESTI a vérifié l'étanchéité entre les différentes applications, et notamment entre celles de la TOE et celles n'en faisant pas partie. En particulier, le CESTI a vérifié qu'une applet Java ne peut accéder qu'à ses propres données et pas à celles d'une autre applet, ni à celles des applications de la TOE.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le chargement des patchs est protégé par l'application AIP.

Le logiciel embarqué du produit a été développé sur le site suivant :

SAGEM Sécurité - Etablissement d'Osny
18 Chaussée Jules César
95520 Osny
France

Les sites de développement du microcontrôleur sont identifiés dans le rapport de certification [2010/02].

1.2.5. Configuration évaluée

Le certificat porte sur la configuration « ouverte » du produit (des applets peuvent être chargés dans le produit en phase opérationnelle).
Le produit testé par le centre d'évaluation est représentatif du produit final.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM], avec l'interprétation suivante :

- le composant d'assurance ATE_DPT.2 est remplacé par le composant ATE_DPT.1 au niveau EAL4 dans la révision 3 des CC version 3.1 (publiée après le démarrage de cette évaluation).

Pour répondre aux spécificités des cartes à puce, les guides [CC AP] et [COMP] ont été appliqués.

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 « SB23YR80B avec sa librairie cryptographique Neslib version 3.0 », conforme au profil de protection [PP0035], au niveau EAL6 augmenté du composant ALC_FLR.1. Ce microcontrôleur a été certifié le 10 février 2010 sous la référence ANSSI-CC-2010/02 ([2010/02]). Il a également fait l'objet du rapport de maintenance ANSSI-CC-2010/02-M01 ([2010/02-M01]) publié le 19 mars 2010.

L'évaluation s'appuie sur les résultats d'évaluation du produit « Carte CC IDeal Citiz (sur composant SB23YR48B), version 1.4.5 », selon le [PP BAC], certifié le 9 avril 2010, sous la référence ANSSI-CC-2010/21 ([2010/21].)

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 3 juin 2010, 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 par l'ANSSI conformément à [REF-CRY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY].
Ce rapport d'analyse établit que les mécanismes analysés ne sont pas conformes aux exigences du référentiel cryptographique de l'ANSSI [REF-CRY], du fait de faiblesses cryptographiques inhérentes aux spécifications ICAO [ICAO] auxquelles le développeur est contraint de se conformer.

Ces résultats ont été pris en compte dans l'analyse de vulnérabilités indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilités exploitables pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas utilisé par le produit est celui du microcontrôleur (voir le rapport de certification [2010/02]).

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 la « Carte CC IDeal Citiz (sur composant SB23YR48B), version 1.4.5 » soumise à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

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 spécifiés dans la cible de sécurité [ST], aux paragraphes 4.2 et 4.3, 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 :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

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 signataires[1], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[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**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the 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**	**2**	**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]	Cible de sécurité de référence pour l'évaluation : - « Common Criteria Security Target - Machine Readable Travel Document – Basic Access Control – CC IDeal Citiz », référence SSE-0000078636, révision 03, Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Common Criteria Security Target Lite - Machine Readable Travel Document – Basic Access Control – CC IDeal Citiz », référence SSE-0000078637, révision 03.
[RTE]	Rapports techniques d'évaluation : - « Réévaluation EOS - Rapport Technique d'Evaluation », référence LETI.CESTI.EOS.RTE.002, édition 3.2.
[ANA-CRY]	« Cotation de mécanismes cryptographiques- Qualification EOS », n° 805/ANSSI/ACE/LCC du 2 avril 2010.
[CONF]	« IDEAL_– Software Release Sheet – V1.4.50», référence SSE-0000075528, révision 19.
[GUIDES]	Guide d'installation du produit : - « IDEAL 1.4 procédure d'installation », référence SSE-0000076822, version 02, Guide d'administration du produit : - « ICAO Application Pre-personalization manual - Project : CC Ideal Pass », référence SSE-0000074722, version 02, - « IDEAL IAS ECC Personalization Guidance », référence : SSE-0000064845, version 02, - « ICAO Application Personalization manual - Project : CC Ideal Pass », référence SSE-0000074723, version 04, Guide d'utilisation du produit : - « ICAO Application User manual - Project : CC Ideal Pass », référence SSE-0000074862, version 01, - « IDEAL IAS ECC Operational User Guidance », référence : SSE-0000065958, version 01.
[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.*
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

[2010/02]	Rapport de certification ANSSI-CC-2010/02, délivré le 10 février 2010 pour les « Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB ».
[2010/02-M01]	Rapport de maintenance ANSSI-2010/02-M01, délivré le 19 mars 2010, relatif au certificat ANSSI-CC-2010/02.
[2010/21]	Rapport de certification ANSSI-CC-2010/21, délivré le 9 avril 2010 pour la « Carte CC IDeal Citiz (sur composant SB23YR48B), version 1.4.5- Application ICAO BAC ».

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001, Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002, Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, revision 2, ref CCMB-2007-09-004.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.11 du 24 octobre 2008, voir www.ssi.gouv.fr.