



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-2010/19**

### **Carte CC IDEal Citiz (sur composant SB23YR80B), version 1.4.5 Application IAS**

*Paris, le 9 avril 2010,*

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

Patrick Pailloux  
[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.anssi@ssi.gouv.fr](mailto:certification.anssi@ssi.gouv.fr)

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



## 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](http://www.ssi.gouv.fr).



# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Identification du produit</i> .....	6
1.2.2. <i>Services de sécurité</i> .....	7
1.2.3. <i>Architecture</i> .....	7
1.2.4. <i>Cycle de vie</i> .....	8
1.2.5. <i>Configuration évaluée</i> .....	9
<b>2. L’EVALUATION .....</b>	<b>10</b>
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
<b>3. LA CERTIFICATION .....</b>	<b>12</b>
3.1. CONCLUSION .....	12
3.2. RESTRICTIONS D’USAGE.....	12
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> .....	13
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>14</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>16</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>18</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la « Carte CC IDEal Citiz (sur composant SB23YR80B), IDEAL/ST23YR80/1.4.5, 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 :
  - o 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) ;
  - o 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) ;
  - o l'application IAS (Identité Authentification Signature), qui permet de générer, détruire et charger des clés pour créer des signatures électroniques ;
- et 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 conforme aux profils de protection [PP0005] et [PP0006], adaptés à la version 3.1 des CC (ces PP ayant été rédigés selon la version 2.1 des CC).

### 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 : SB23YR80B ;
- référence commerciale du produit (SAGEM) : IDEAL/ST23YR80/1.4.5 ;
- référence complète du logiciel embarqué (SAGEM ORGA) OFFICIEL\_IDEAL\_ST23YR80\_1\_4\_50 ;
- référence fondeur (ST Microelectronics) : SB23YR80 QPX (puce masquée).

La version de chaque composant logiciel de la version certifiée du produit peut être vérifiée, selon les commandes et réponses identifiées dans le guide d'installation du produit (voir [GUIDES]).

### 1.2.2. Services de sécurité

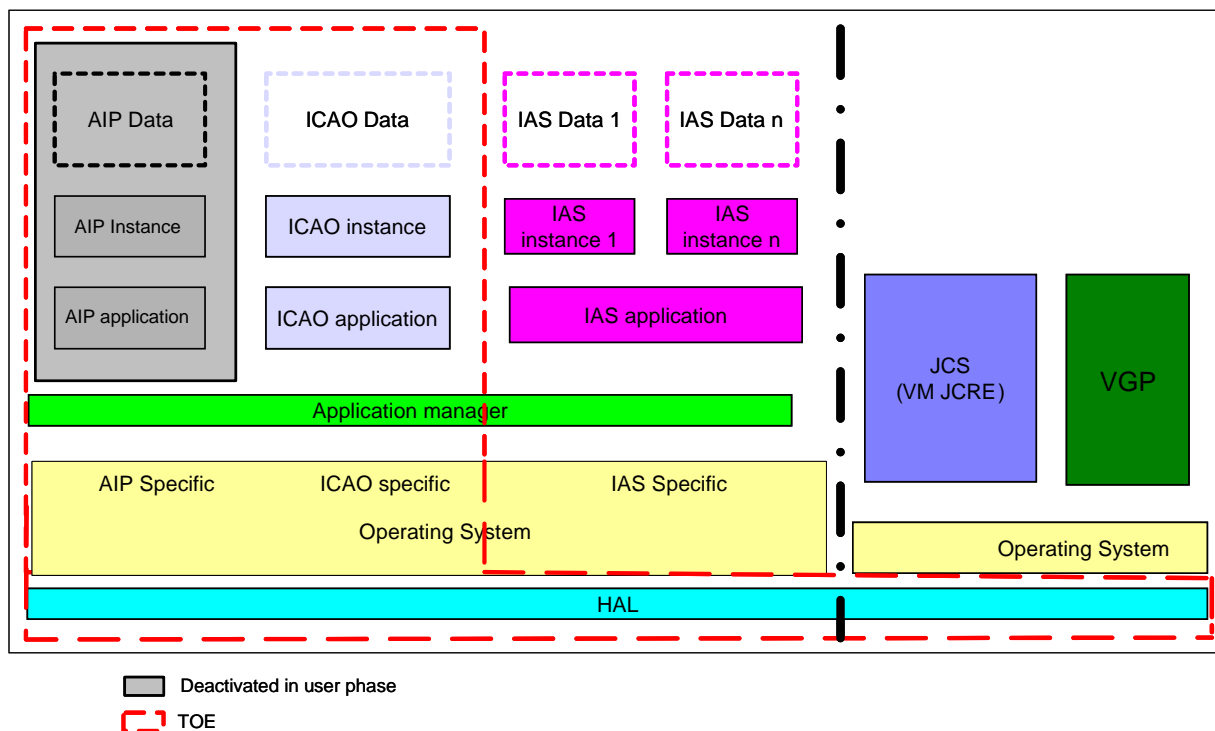
Les principaux services de sécurité évalués fournis par la TOE sont :

- la génération de bi-clés de signature ;
- la destruction de bi-clés de signature
- l'import de clés privées de signature ;
- la création de signature (basés sur des mécanismes RSA ou courbes elliptiques) ;
- et l'authentification du signataire par un PIN.

### 1.2.3. Architecture

Le produit est constitué :

- du microcontrôleur SB23YR80B, 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 :
  - o du système d'exploitation OPUCE ;
  - o de la couche d'abstraction du matériel HAL (Hardware Abstract Layer) ;
  - o du JavaCard System ;
  - o de l'application d'initialisation et de personnalisation de la carte AIP ;
  - o des l'application IAS et ICAO ;
- du patch de l'application IAS, version 5.0, développé par SAGEM Sécurité et chargé en EEPROM.

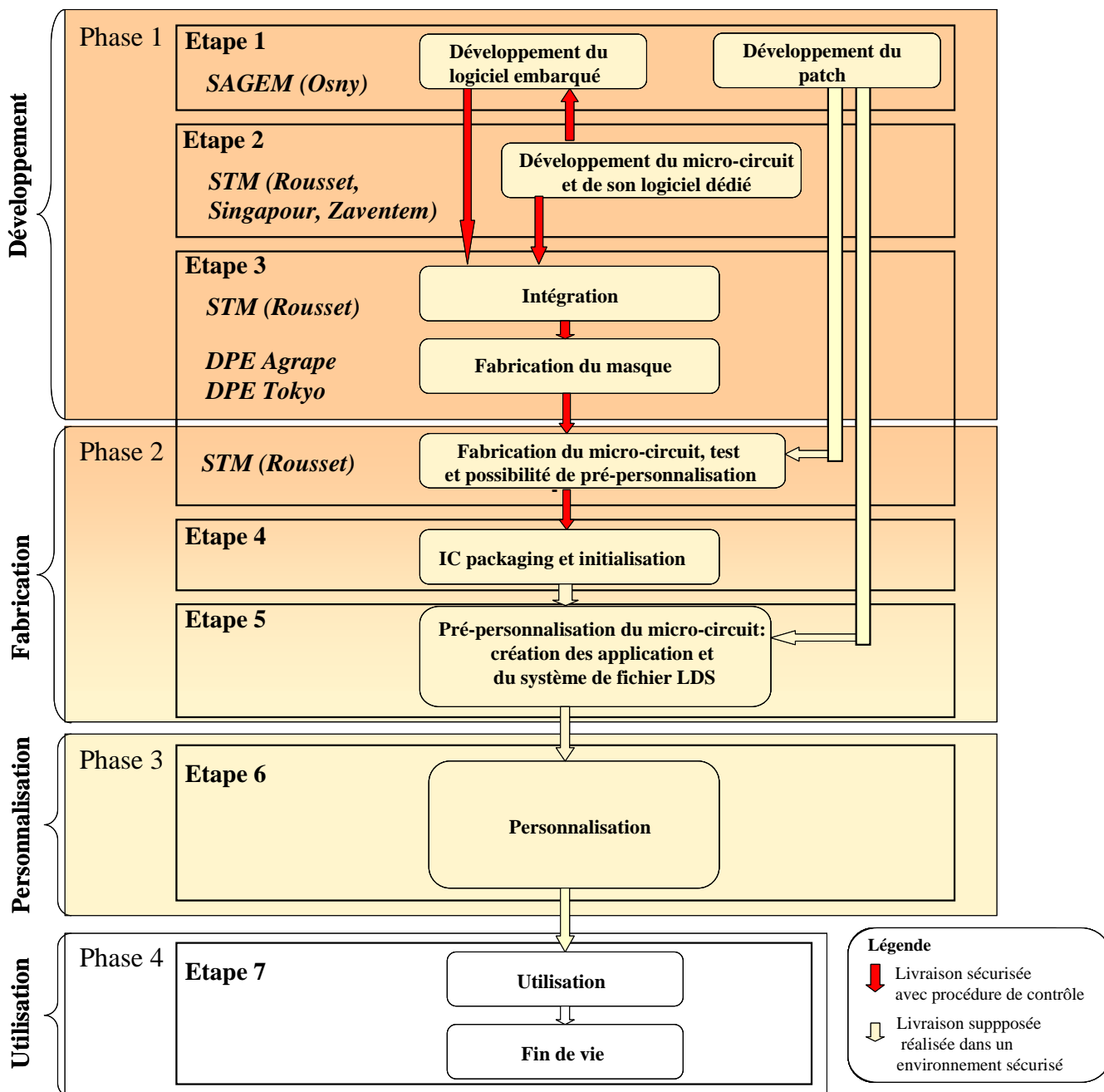


La TOE correspond à l'application IAS, associée aux fonctionnalités et services du système d'exploitation et du microcontrôleur requis pour mettre en œuvre les fonctionnalités de cette application.

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].

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. Il a fait également l'objet du rapport de maintenance ANSSI-CC-2010/02-M01 publié le 19 mars 2010.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 2 avril 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] et donnent lieu aux conclusions suivantes :

- le schéma de signature ECDSA de ce produit n'est pas reconnu conforme au référentiel ;
- les signatures électroniques doivent être générées en utilisant la fonction SHA-256 ;
- le dimensionnement des modules RSA et des courbes elliptiques doivent suivre les règles du référentiel ;
- pour le schéma de signature RSA , il est recommandé d'utiliser un exposant public supérieur à  $2^{16}$ .

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 SB23YR80B), 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 5 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] au paragraphe 4.2 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 1999 permet la reconnaissance, par les pays signataires de l'accord<sup>1</sup>, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



---

<sup>1</sup> Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, 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<sup>1</sup>, 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 :



---

<sup>1</sup> 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 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

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
<b>AVA</b> <b>Estimation des vulnérabilités</b>	AVA_VAN	1	2	2	3	4	5	5	5	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"> <li>- « Common Criteria security target – IAS ECC – Secure Signature Creation Device – CC IDEal Citiz », référence SSE-0000067225, révision 07,</li> </ul> <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"> <li>- « Common Criteria security target lite – IAS ECC – Secure Signature Creation Device – CC IDEal Citiz », référence SSE-0000078618, révision 03.</li> </ul>
[RTE]	<p>Rapports techniques d'évaluation :</p> <ul style="list-style-type: none"> <li>- « EOS - Rapport Technique d'Evaluation », référence LETI.CESTI.EOS.RTE.001, édition 1.0,</li> <li>- « Réévaluation EOS - Rapport Technique d'Evaluation », référence LETI.CESTI.EOS.RTE.002, édition 2.1.</li> </ul>
[ANA-CRY]	<p>« Cotation de mécanismes cryptographiques- Qualification EOS », n° 805/ANSSI/ACE/LCC du 2 avril 2010.</p>
[CONF]	<p>« IDEAL_ – Software Release Sheet – V1.4.50 », référence SSE-0000075528, révision 14.</p>
[GUIDES]	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none"> <li>- « IDEAL 1.4 procédure d'installation », référence SSE-0000076822, version 01,</li> </ul> <p>Guide d'administration du produit :</p> <ul style="list-style-type: none"> <li>- « ICAO Application Pre-personalization manual - Project : CC Ideal Pass », référence SSE-0000074722, version 02,</li> <li>- « IDEAL IAS ECC Personalization Guidance », référence : SSE-0000064845, version 02,</li> <li>- « ICAO Application Personalization manual - Project : CC Ideal Pass », référence SSE-0000074723, version 04,</li> </ul> <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> <li>- « ICAO Application User manual - Project : CC Ideal Pass », référence SSE-0000074862, version 01,</li> <li>- « IDEAL IAS ECC Operational User Guidance », référence : SSE-0000065958, version 01.</li> </ul>
[PP0005]	<p>Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0005-2002.</i></p>
[PP0006]	<p>Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0006-2002.</i></p>





[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 « Microcontrôleur sécurisé SB23YR80A incluant la bibliothèque cryptographique NesLib v3.0 en configuration SB ».
[2010/02-M01]	Rapport de maintenance ANSSI-2010/02-M01, délivré le 19 mars 2010, relatif au certificat ANSSI-CC-2010/02.

### Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.</p>
[CC]	<p>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.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation :          Evaluation Methodology,          September 2007, version 3.1, revision 2, ref CCMB-2007-09-004.</p>
[CC AP]	<p>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.</p>
[COMP]	<p>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.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</p>
[SOG-IS]	<p>«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.</p>
[REF-CRY]	<p>Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.11 du 24 octobre 2008, voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>.</p>