PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-2009/20

ID ONE™ ePASS v2.1 en configuration BAC sur composants NXP P5CD040V0B, P5CD080V0B, P5CD144V0B

Paris, le 23 juillet 2009,

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

Le contre-amiral Michel Benedittini,
directeur général adjoint
[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 nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

UUcertification.dcssi@sgdn.gouv.fr

Référence du rapport de certification

ANSSI-2009/20

Nom du produit

ID ONE™ ePASS v2.1 en configuration BAC sur composants NXP P5CD040V0B, P5CD080V0B, P5CD144V0B

Référence/version du produit

Révision 1.0 avec code optionnel (patch) r2.0

Conformité à un profil de protection

[PP BAC] BSI-PP-0017

Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2

Développeurs

Oberthur Technologies[1]
50 quai Michelet
92300 Levallois-Perret, France

NXP Semiconductors GmbH[1]
Stresemannallee 101
D-22502 Hamburg, Germany

Commanditaire

Oberthur Technologies[1]
50 quai Michelet
92300 Levallois-Perret, France

Centre d'évaluation

CEACI (Thales Security Systems – CNES)
18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France
Tél : +33 (0)5 61 28 16 51, mél : nathalie.feyt@thalesgroup.com

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

1 : il s'agit des sites principaux.

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 à puce « ID ONE™ ePASS v2.1 en configuration BAC sur composants NXP P5CD040V0B, P5CD080V0B, P5CD144V0B », révision 1.0 avec code optionnel (patch) r2.0, développée par Oberthur Technologies et NXP Semiconductors.

Le produit évalué est de type carte à puce sans contact avec antenne. Il implémente les fonctionnalités de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (cf. [OACI]). Il s'agit d'un microcontrôleur à interface sans contact avec un logiciel embarqué destiné à vérifier l'authenticité du document de voyage et d'identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection, et permettant notamment :

- de protéger en intégrité les données stockées grâce à des moyens physiques et au contrôle d'accès qui ne permet d'écrire qu'une seule fois ;
- d'authentifier le porteur du document de voyage et le système d'inspection (terminal de lecture des documents de voyage) préalablement à tout contrôle aux frontières, à l'aide du mécanisme *Basic Access Control ;*
- de protéger en intégrité et en confidentialité la lecture des données à l'aide du mécanisme *secure messaging* ;
- d'authentifier l'authenticité de la puce à l'aide du mécanisme *Active Authentication* (si activé) ;

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels. Ils peuvent être intégrés sous forme de module ou d'*inlay*. Le produit final peut être un passeport, une carte plastique, etc.

1.2. Description du produit

La cible de sécurité [ST], au paragraphe 2, définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection [PP BAC]. L'évaluateur a considéré que c'est une conformité démontrable, la cible de sécurité ayant été élaborée suivant la version 3.1 des [CC] alors que le profil de protection [PP BAC] l'a été en version 2.3 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 par les éléments suivants :

Commande Vs. composant	**P5CD040**	**P5CD080**	**P5CD144**
ATS (Answer To Select)	4F 54 49 44 **25** 94 XX XX XX XX	4F 54 49 44 **28** 94 XX XX XX XX	4F 54 49 44 **2B** 94 XX XX XX XX

Par ailleurs, la lecture du fichier EF.TOE par la commande *Read Binary* permet d'obtenir les informations d'identification suivantes :

Informations d'identification	**Exemples de valeurs**
Identifiant du code ROM	04 03 06 95 91
Identifiant du patch	04 03 07 09 42
Identifiant du [PP EAC]	04 01 26
Identifiant du [PP BAC]	04 01 17
Indication du support de EAC / AA / BAC	04 01 0X, où X = b1|0|b2|b3 avec b1 = EAC, ici = 0 b2 = AA b3 = BAC, ici = 1

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- contrôle d'accès en lecture ;
- contrôle d'accès en écriture ;
- mécanisme BAC ;
- mécanisme *secure messaging* ;
- authentification de l'agent de personnalisation ;
- mécanisme A*ctive Authentication* à base de RSA et ECC ;
- auto-tests ;
- gestion de l'état sûr de la carte ;
- protection physique.

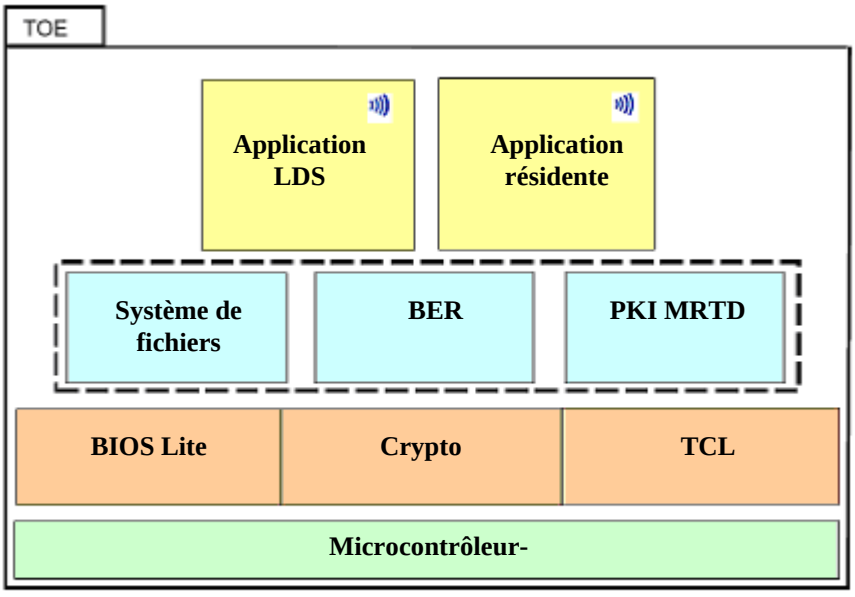
Les services de sécurité offerts par le microcontrôleur sont :
- génération de nombres aléatoires ;
- coprocesseur triple DES ;
- coprocesseur AES (n'est pas utilisé par le présent produit) ;
- contrôle des conditions de fonctionnement ;
- protection contre les modifications physiques ;
- protection logique ;
- protection du mode de contrôle ;
- contrôle d'accès aux mémoires ;
- fonctions spéciales de contrôle de l'accès aux registres.

1.2.3. Architecture

Le produit est constitué :

- d'une couche représentant le matériel (*IC*) ;
- d'une couche basse faisant l'interface entre la couche du dessus et le matériel :
  - *BIOS Lite* gère l'accès à la mémoire (lecture, écriture) ainsi que la manipulation d'autres éléments basiques du matériel ;
  - *Crypto* offre les services cryptographiques ;
  - *TCL* gère l'interface de communication qui est sans contact ici ;
- d'une couche de modules offrant des API génériques :
  - *File System* gère de façon sécurisée les données des applications ;
  - *BER* offre une boîte à outils pour gérer les formats APDU ;
  - *PKI MRTD* implémente les fonctions génériques pour l'*Active Authentication* et le *secure messaging* des données entrantes et sortantes ;
- D'une couche applicative :
  - *LDS Application* implémente les commandes du passeport électronique qui sont disponibles en phase opérationnelle ;
  - *Resident Application* implémente les commandes de pré-personnalisation et de personnalisation ;

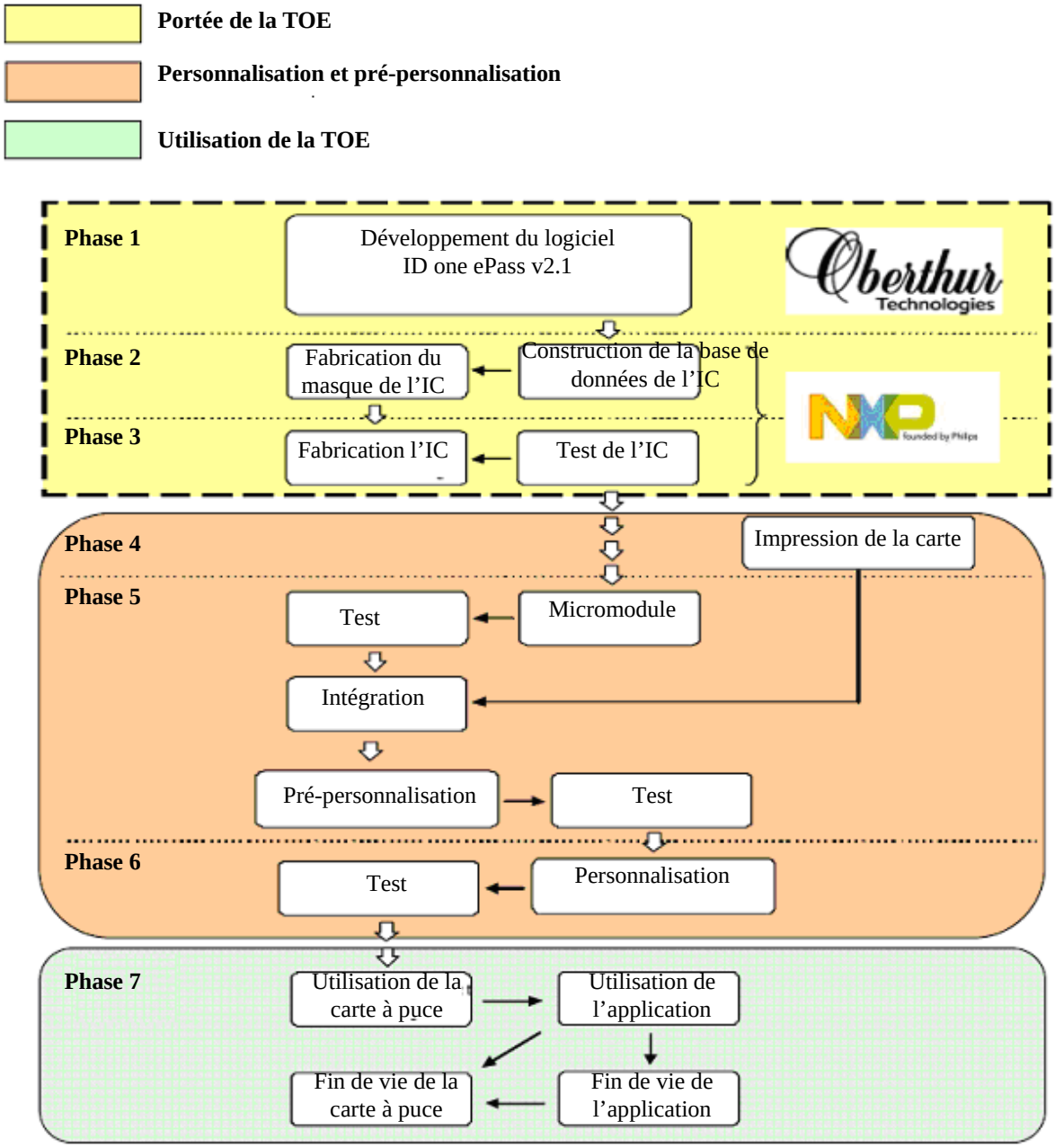
La figure suivante résume cette architecture :



Cette couche est perméable: les couches supérieurs peuvent également accéder directement à des couches lus basses pour un ensemble déterminé de services.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



La livraison du produit, depuis le fondeur jusqu'au pré-personnalisateur, est protégée par des mesures de sécurité spécifiques.

Le chargement de patch fonctionnel et la pré-personnalisation sont en dehors du périmètre de l'évaluation. Ces étapes sont couvertes par des guides et des mesures de protection spécifiques.

L'application a été développée par Oberthur Technologies sur les sites suivants :

Oberthur Technologies - Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies - Levallois

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies - Bordeaux

Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus - Porte 2

33 600 PESSAC
France

Le microcontrôleur a été développé et fabriqué par NXP sur ses sites (cf. [BSI-DSZ-CC-0404-2007] / [BSI-DSZ-CC-0410-2007] / [BSI-DSZ-CC-0411-2007]), dont le principal est :

NXP Semiconductors GmbH1

Stresemannallee 101
D-22502 Hamburg
Allemagne

Pour l'évaluation, l'évaluateur a considéré comme :
- administrateur du produit, les nations émettrices du passeport ;
- utilisateur du produit, les porteurs du passeport ainsi que les systèmes d'inspection qui interviennent en phase d'utilisation du produit.

1.2.5. Configuration évaluée

Le produit peut être personnalisé sous différentes configurations.

Le certificat porte sur la configuration suivante :
- mécanisme BAC activé ;
- mécanisme EAC désactivé ;
- mécanisme *Active Authenticate* activé (ECC ou RSA) ou désactivé ;
- interface de contact désactivée ;
- commande *Get Data* désactivée.

2. L'évaluation

2.1. R éférentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
Pour les composants d'assurance qui ne seraient pas couverts par [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 [CC IC] et [CC AP] 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, conforme au profil de protection [PP0002], des microcontrôleurs P5CD040V0B, P5CD080V0B, P5CD144V0B au niveau EAL5 augmenté des composants ALC-DVS.2, AVA_MSU.3, AVA_VLA.4. Ces microcontrôleurs ont été certifiés par le BSI (cf. [BSI-DSZ-CC-0404-2007] / [BSI-DSZ-CC-0410-2007] / [BSI-DSZ-CC-0411-2007]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 12 mai 2009, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par l'ANSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et ont été pris en compte par l'évaluateur.

Les mécanismes analysés contiennent, pour certains d'entre eux, des implémentations qui ne sont pas conformes au référentiel cryptographique de l'ANSSI (Cf. [REF-CRY]).

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation allemand T-Systems (cf. [BSI-DSZ-CC-0404-2007] / [BSI-DSZ-CC-0410-2007] / [BSI-DSZ-CC-0411-2007]). Le générateur atteint le niveau *P2 – High* selon [AIS 31].

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 « ID ONE™ ePASS v2.1 en configuration BAC sur composants NXP P5CD040V0B, P5CD080V0B, P5CD144V0B », révision 1.0 avec code optionnel (patch) r2.0, développé par Oberthur Technologies et NXP Semiconductors, soumis 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 paragraphe 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] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment les paragraphes 7.4, 7.5, 9.3, 9.4 et 9.5.

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[1], 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 :

[1] 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[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, la République de Corée, le Pakistan, les Pays-Bas, 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**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	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 procedure
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
	ADO_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 Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component 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 specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**2**	Testing: security enforcing modules
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independant 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 : - HEIMDALL – Security Target – BAC référence FQR: 110 4292, révision 3 Oberthur Technologies Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ID One™ ePass v2.1 with BAC configuration - Public Security Target FQR 110 4641, révision 1 Oberthur Technologies
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: HEIMDALL référence HEI_ETR, révision 1.0 Thales Security Systems – CEACI business activity
[ANA-CRY]	Rapport d'analyse cryptographique de la DCSSI : - Cotation de mécanismes cryptographiques Qualification HEIMDALL N°1469SGDN/DCSSI/DR du 9 juin 2009 SGDN/DCSSI
[CONF]	Liste de configuration du produit - HEIMDALL – configuration List FQR: 110 4535, révision 1 Oberthur Technologies
[GUIDES]	Guide d'administration et d'utilisation du produit : - HEIMDALL - Administration and User Guidance Document FQR 110 4404, révision 5 Oberthur Technologies
[PP BAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.0, 18 August 2005. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0017*
[PP EAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control, version 1.2 du 19 November 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0026*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0002-2001.*

[OACI]	ICAO Doc 9303, Sixth Edition, 2007
[BSI-DSZ-CC-0404-2007]	NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-DSZ-CC-0404-2007*
[BSI-DSZ-CC-0410-2007]	NXP Secure Smart Card Controller P5CD080V0B, P5CN080VOB and P5CC080VOB each with specific IC Dedicated Software. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-DSZ-CC-0410-2007*
[BSI-DSZ-CC-0411-2007]	NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-DSZ-CC-0411-2007*

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, révision 2, ref CCMB-2007-09-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[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 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version courante, voir www.ssi.gouv.fr
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik)