Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/28

Application e-Passport AXSEAL CC V2 72K embarquée sur le microcontrôleur Philips P5CD072 V0Q

Paris, le 12 décembre 2006

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ Ti 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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), 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
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr

Référence du rapport de certification

2006/28

Nom du produit

Application e-Passport AXSEAL CC V2 72K embarquée sur le microcontrôleur Philips P5CD072 V0Q

Référence/version du produit

Référence développeur de l'application : Axseal V3, code révision 456

Référence complète du microcontrôleur : Philips P5CD072 V0Q - Part A1002922 (CHIP M576ICAOP3M P5CD072V3 MOB4)

Conformité à un profil de protection

PP BSI-PP-0017

Machine Readable Travel Document with ICAO Application, Basic Access Control

Critères d'évaluation et version

Critères Communs version 2.2

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, ALC_DVS.2

Développeurs

Gemalto

6 rue de la Verrerie,
92197 Meudon Cedex, France

Philips Semiconductors

Postfach 54 02 40,
22502 Hamburg, Allemagne

Commanditaire

Gemalto

6 rue de la Verrerie, 92197 Meudon Cedex, France

Centre d'évaluation

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Tél : +33 (0)5 61 27 40 29, mél : ceaci@cnes.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 :

- La direction centrale 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 l'application e-Passport AXSEAL CC V2 72K (code révision 456), développée par la société Gemalto, et embarquée sur le microcontrôleur Philips P5CD072 V0Q (identification fabriquant : Part A1002922 - CHIP M576ICAOP3M P5CD072V3 MOB4) développé et fabriqué par la société Philips Semiconductors.

Le produit évalué est de type carte à puce sans contact avec antenne. Il implémente les fonctionnalités de passeport 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 permettant :

- de stocker les données signées du futur porteur du passeport (nation ou organisation émettrice, n° de passeport, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, données d'informations optionnelles), une donnée biométrique du porteur (photo du visage), des données d'authentification optionnelles et diverses données permettant de gérer la sécurité du document ;
- de vérifier l'authenticité du passeport et d'identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce micro-circuit et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels.

1.2. Description du produit évalué

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 [PP MRTD].

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
En mode d'utilisation finale, la version certifiée du produit est identifiable à l'aide de la réponse initiale de la carte (*Answer to select* – ATS). On doit trouver dans la réponse les données suivantes :

- « 00 15 » pour le microcontrôleur P5CD072 ;
- « D0 00 42 » pour l'application Axseal V2 CC 72K (code révision 456) ;
- « 00 00 » voulant dire qu'il n'y a pas de patch, ce qui est le cas de la configuration certifiée.

D'autres commandes d'administration permettent d'identifier plus précisément le produit et sont détaillées dans les guides (cf. [GUIDES]).
Le microcontrôleur peut également être identifié visuellement avec l'élément suivant écrit à la surface du produit et visible au microscope : « Philips T023Q ».

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- auto-tests des fonctions de sécurité ;
- gestion sécurisée du cycle de vie ;
- gestion sécurisée du chargement d'applicatifs en mémoire non volatile ;
- vérification de l'intégrité des données sensibles ;
- identification et authentification basées sur une authentification mutuelle ;
- échanges de données par « secure messaging » ;
- identification et authentification basées sur une authentification externe ;
- vérification de l'authenticité de la puce ;
- protection des données sensibles.

1.2.3. Architecture

Le produit est constitué d'un microcontrôleur embarquant l'application e-Passport et les données du porteur. Ce dernier est inséré dans un film papier avec une antenne (inlay) et la feuille est insérée dans la couverture d'un passeport. La figure suivante résume cette description :

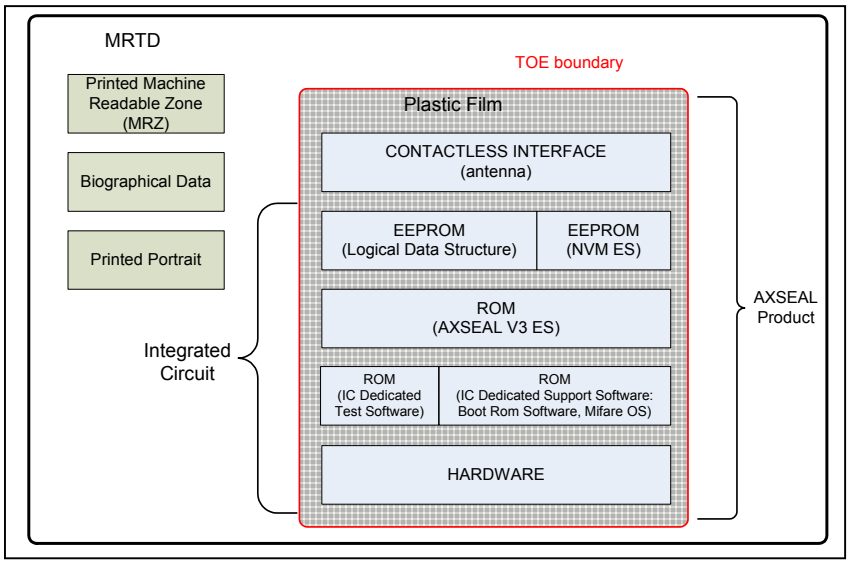

Figure 1 – Architecture du produit

Le produit dans sa configuration évaluée contient les structures de données et les clés nécessaires au chargement des données utilisateur dans la phase de personnalisation. Le produit a été fourni avec une application de personnalisation permettant le chargement des clés et des données utilisateurs lors de la phase de personnalisation et le passage en configuration d'usage conformément aux spécifications de l'Organisation de l'Aviation Civile Internationale (cf. [OACI]). Cette application a été utilisée et la configuration résultante a été testée pour s'assurer de la conformité aux exigences telles que définies dans le profil de protection.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

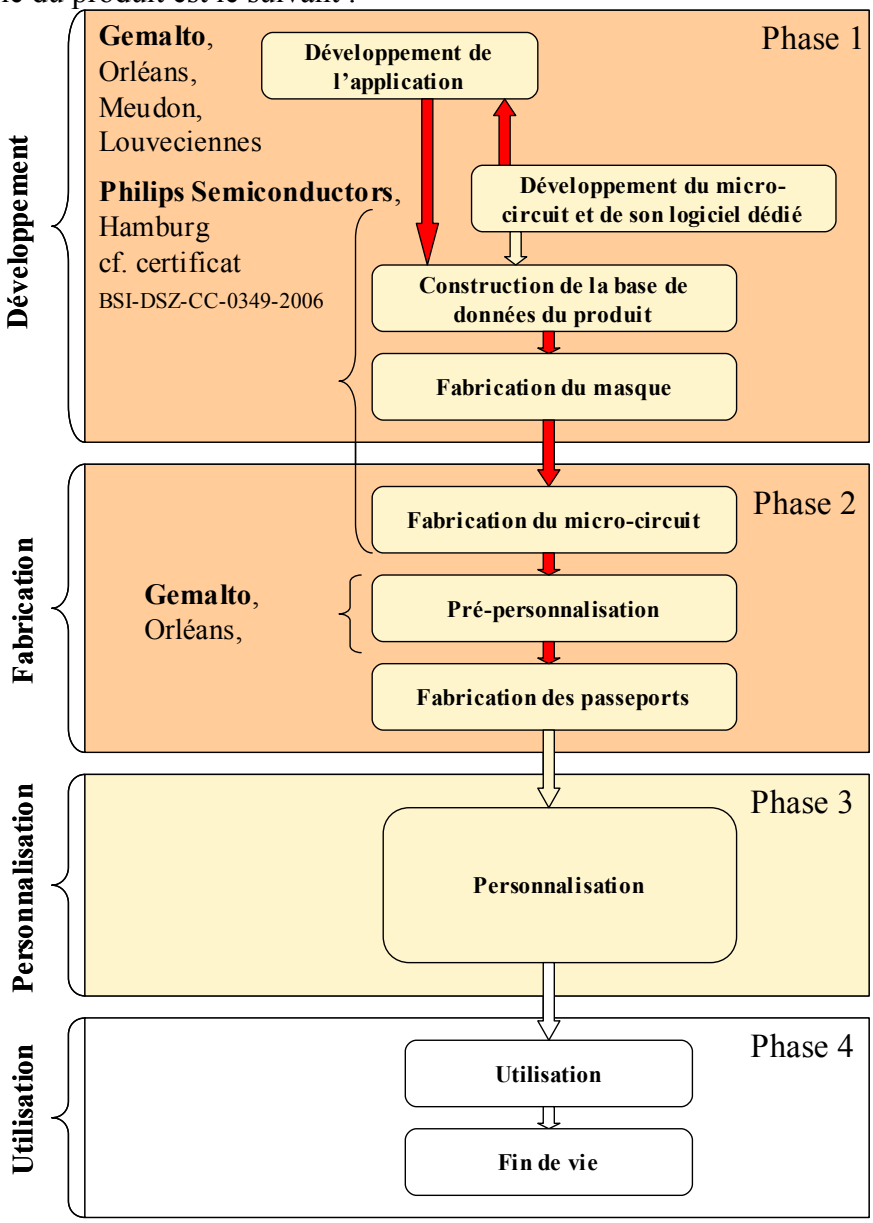

Figure 2 - Cycle de vie du produit

Le produit a été développé par Gemalto sur les sites suivants :

Gemalto Meudon

6 rue de la Verrerie,
92197 Meudon Cedex,
France.

Gemalto Louveciennes

36-38 route de la Princesse, BP 45
78431 Louveciennes Cedex
France.

Gemalto Orléans

284 avenue de la Pomme de Pin, BP-6021 St Cyr en Val,
45060 Orléans Cedex 2,
France.

Le microcontrôleur est développé et fabriqué par Philips Semiconductors sur le site suivant :

Philips Semiconductors

Postfach 54 02 40,
22502 Hamburg,
Allemagne.

La phase de fabrication du passeport (pré-personnalisation) est en partie réalisée par Gemalto sur son site d'Orléans.
Les phases de mise en inlay et d'intégration de l'inlay dans le livret du passeport ne sont pas couvertes par l'évaluation, mais n'ont de toute façon pas d'impact sécuritaire, le produit étant protégé durant ces phases.

1.2.5. Configuration évaluée

Le produit évalué est le microcontrôleur et son logiciel embarqué identifiés au §1.1. Le produit a été livré sous la forme d'Inlay au centre d'évaluation. La référence de l'Inlay identifiant l'antenne utilisée est « AWPFA 032/06-3 ». Le produit testé par le centre d'évaluation est représentatif du passeport final (produit sous forme d'inlay, en configuration pré-personnalisée et personnalisée).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.2** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et aux interprétations suivantes : 86, 137, 146, 175, 180, 192, 220, 227, 228, 232, 243, 254.
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par la DCSSI et compatibles avec le document [AIS34] ont été utilisées.

L'évaluation a été réalisée en composition 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 « P5CD072 V0Q » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002]. Ce microcontrôleur a été certifié le 28 mars 2006 sous la référence BSI-DSZ-CC-0349-2006.

Pour répondre aux spécificités des cartes à puce, les guides [CCIC] et [CCAP] ont été appliqués.

L'évaluation s'appuie sur les résultats d'évaluation du produit « Application e-Passport AXSEAL CC V2 36K (version 456) embarquée sur le microcontrôleur Philips P5CD036V0Q » certifié en date du 28 novembre 2006 sous la référence 2006/23 (cf. [2006/23]). L'application embarquée demeure identique. Seule la référence du composant change, en raison de taille mémoire différente.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], délivré à la DCSSI le 7 décembre 2006, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse et ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

3. La certification

3.1. Conclusion

L'évaluation, identifiée au chapitre 2 et décrite dans le rapport technique d'évaluation [RTE], a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises par 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 « Application e-Passport AXSEAL CC V2 72K embarquée sur le microcontrôleur Philips P5CD072 V0Q » 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 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 identifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- l'Etat émetteur ou l'organisation doit s'assurer que les utilisateurs agissant en tant qu'agents de personnalisation :
    - établissent l'identité correcte du porteur du passeport et identifient ses données biographiques pour le passeport électronique ;
    - enregistrent les données biométriques de référence du porteur, c'est-à-dire son portrait ;
    - personnalisent le passeport pour le porteur avec les mesures sécuritaires physiques et logiques requises (incluant la signature électronique des données du porteur dans le passeport). L'agent de personnalisation active la fonction de contrôle d'accès basique (BAC) et génère la clé de contrôle d'accès basique dans le passeport. L'agent de personnalisation doit générer des clés cryptographiques de 112 bits conformément à l'algorithme de dérivation des clés BAC spécifié dans l'annexe E du document [OACI] relatif à la PKI ;
- l'Etat émetteur ou l'organisation doit :
    - générer une bi-clé de signature nationale cryptographiquement sûre ;
    - garantir le secret de la clé privée de cette bi-clé nationale de signature et signer les certificats des signataires de document dans un environnement opérationnel sécurisé ;
    - distribuer un certificat de la clé publique nationale de signature aux Etats et organisations hôtes. Ce certificat assure l'intégrité et l'authenticité de cette clé.

  L'Etat émetteur ou l'organisation doit également :
    - générer une bi-clé de signature des documents cryptographiquement sûre ;
    - garantir le secret de la clé privée de cette bi-clé de signature de document, et signer les données sécuritaires d'un passeport authentique dans un environnement opérationnel sécurisé ;

  - distribuer aux Etats et organisations hôtes le certificat de la clé publique de signature de document signé avec la clé publique nationale, en maintenant son intégrité et son authenticité en utilisant l'infrastructure de clés décrite dans [OACI] ;
- l'Etat émetteur ou l'organisation doit :
  - générer une bi-clé d'authentification active du passeport ;
  - signer et stocker dans le passeport la clé publique d'authentification active ;
  - fournir un support aux systèmes d'inspection des Etats et organisations hôtes, pour vérifier l'authenticité des passeports électroniques en certifiant la clé publique d'Authentification Active (AA) ;
- l'Etat ou l'organisation émetteur doit garantir que les administrateurs agissant pour leur compte établissent correctement l'identité du porteur et mettent à jour les passeports avec les mesures physiques et logiques requises. Selon la décision de l'Etat ou l'organisation émetteur, l'administrateur peut par exemple désactiver l'application ou exécuter les commandes d'administration proposées par le produit ;
- le système d'inspection de l'Etat ou organisation hôte doit vérifier le passeport présenté par le voyageur pour vérifier son authenticité à l'aide de moyens physiques, et pour détecter toute manipulation physique du passeport. Le système d'inspection étendu utilise le mécanisme « Active authentication » pour vérifier l'authenticité de la puce du passeport présenté ;
- le système d'inspection doit vérifier la signature des données signées du passeport préalablement à leur utilisation pour identifier le porteur. Les Etats et organisations hôtes doivent maintenir l'authenticité et la disponibilité des clés publiques de signature nationales et de signature des documents au sein de tous les systèmes d'inspection ;
- le système d'inspection des Etats et organisations hôtes doit garantir la confidentialité et l'intégrité des données lues dans le passeport. Les Etats et organisations hôtes examinant le passeport en mettant en œuvre le protocole BAC doivent utiliser un terminal d'inspection implémentant la partie « terminal » du protocole BAC afin de chiffrer les communications et données transmises entre le passeport et le terminal. Les Etats et organisations hôtes utilisant le mode primaire (Primary inspection system) mettront en œuvre des mesures empêchant l'écoute passive des communications entre le terminal et le passeport ;
- le porteur ne doit pas divulguer les données de son passeport à des tiers non autorisés. Un attaquant connaissant la bande MRZ (données imprimées sur le passeport utilisées pour dériver la clé d'accès aux données stockées dans la puce) ou une partie de ces données aura plus de chance de réaliser une attaque par écoute passive ou par tentative de communication avec le passeport à l'insu de son porteur.

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 :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, il n'est reconnu qu'au niveau EAL4.

L'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], 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 SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

[2] Les pays signataires de l'accord sont : l'Allemagne, l'Australie, l'Autriche, le Canada, la Corée du Sud, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Nouvelle Zélande, la Norvège, 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
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**2**	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level design
	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_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Validation of analysis
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Axseal V2 CC 72K Security Target – HERMES, Référence : D1033361 Rev 1.4, Gemalto Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - e-Passport Axseal CC V2 72K Security Target Public Version, Référence : D1033361 Rev. 1.4, Gemalto
[RTE]	Evaluation Technical Report, Project: HERMES 72K, Référence : HER72_ETR_V1.0 CEACI
[CONF]	Liste de Configuration Axseal V3, Référence : D1028643 Rev 1.1 Gemalto
[GUIDES]	Guide d'installation du produit : - Pre-personalization Manual – Hermes ePassport Axseal V3, Référence : D1031012 Rev 1.3 Gemalto - Cards global personalization process for a new application, Référence : D1024364 Rev : B Gemalto Guide d'administration du produit : - Personalization Manual – Hermes ePassport Axseal V3, Référence : D1031013 Rev 1.3 Gemalto - AGD_ADM – Administrator manual Hermes ePassport Axseal V3 (V2 CC 36K and 72K), Référence : D1028647 Rev 1.2 Gemalto Guide d'utilisation du produit : - AGD_USR – User manual AXSEAL V3, Référence : D1028648 Rev : 1.1 Gemalto
[OACI]	- PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 1st 2004 International Civil Aviation Organization, - Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, May 18th 2004, International Civil Aviation Organization, Machine Readable Travel Documents, supplement 9303

	version 3.0, 12nd June 2005
[PP MRTD]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.0, 18 August 2005. *Certifié sous la référence* BSI-PP-0017
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié sous la référence BSI-PP-0002-2001.*

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, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[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 de niveau de robustesse standard, Version 1.02 du 19 novembre 2004, réf: 2791/SGDN/DCSSI/SDS/Crypto.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004 Bundesamt für Sicherheit in der Informationstechnik