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 DCSSI-2008/45

« eTravel EAC version 1.1 (version 01 02) sur composants P5CD080 et P5CD144 »

Paris, le 18 décembre 2008

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.gouv.fr

Référence du rapport de certification

DCSSI-2008/45

Nom des produits

eTravel EAC v1.1 80K (version 01 02) sur le composant P5CD080

et

eTravel EAC v1.1 144K (version 01 02) sur le composant P5CD144

Référence/version des produits

sur P5CD080 V0B : T1003327 version 1.1

et

sur P5CD144 V0B : T1003883 version 1.1

Conformité à un profil de protection

BSI-PP-0026 version 1.2

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

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeur(s)

Gemalto SA

6 rue de la verrerie, 92197 Meudon, France

NXP Semiconductors GmbH

Box 54 02 40, D-22502 Hamburg, Allemagne

Commanditaire

Gemalto SA

6 rue de la verrerie, 92197 Meudon, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

Accords de reconnaissance applicables

CCRA

SOG-IS

Ces produits sont reconnus 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. Les produits

1.1. Présentation des produits

Les produits évalués sont les cartes « eTravel EAC v1.1 (version 01 02) sur composants P5CD080 et P5CD144 » développés par les sociétés Gemalto et NXP Semiconductors, et fabriqués par la société NXP Semiconductors.

Ces produits sont de type carte à puce sans contact avec antenne. Ils implémentent les fonctionnalités de document de voyage électronique conformément aux spécifications de l'Organisation de l'Aviation Civile Internationale et à l'Extended Access Control. Il s'agit de microcontrôleurs à interface sans contact avec un logiciel embarqué destiné à vérifier l'authenticité du document de voyage et à 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 du porteur du document de voyage : nation ou organisation émettrice, numéro de document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, photo du visage du porteur, données d'information optionnelles, données biométriques complémentaires du porteur et diverses données permettant de gérer la sécurité du document ;
- 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 les données lues à l'aide du mécanisme « secure messaging » ;
- de vérifier l'authenticité de la puce à l'aide du mécanisme « Active Authentication » (si celui-ci a été activé en phase de pré-personnalisation à la demande du client) ;
- de réaliser une authentification forte de la puce et du système d'inspection, préalablement à toute lecture des données biométriques, à l'aide du mécanisme « Extended Access Control ».

Ces microcontrôleurs et les logiciels embarqués ont vocation à être insérés dans la couverture des passeports traditionnels. Ils peuvent être intégrés sous forme de module, d'inlay ou de datapage. Les produits finaux peuvent être un passeport, une carte plastique, etc.

1.2. Description des produits évalués

La cible de sécurité [ST] définit les produits évalués, leurs fonctionnalités de sécurité évaluées et leurs environnements d'exploitation.
Cette cible de sécurité est conforme au profil de protection [PP EAC].

1.2.1. Identification des produits

Les éléments constitutifs de ces produits sont identifiés dans la liste de configuration [CONF]. La version certifiée de ces produits est identifiable par les éléments suivants :

	Nom	**Référence**	**Version**
Sur P5CD080 V0B	eTravel EAC v1.1 80K	T1003327	1.2
Sur P5CD144 V0B	eTravel EAC v1.1 144K	T1003883	1.2

Ces éléments sont identifiables à l'aide de la commande « GET DATA » comme indiqué dans le guide d'administration (cf. [GUIDES]) et dans la liste de configuration (cf. [CONF]) :

- Pour P5CD080 :
  - IC TYPE = **50 80**
  - OPERATING SYSTEM IDENTIFIER= **D0 00 67**
  - OPERATING SYSTEM RELEASE LEVEL= **01 02**

- Pour P5CD144 :
  - IC TYPE = **51 44**
  - OPERATING SYSTEM IDENTIFIER= **D0 00 68**
  - OPERATING SYSTEM RELEASE LEVEL= **01 02**

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par ces produits sont :
- fiabilité ;
- contrôle d'accès ;
- mécanisme d'authentification mutuelle ;
- mécanisme « secure messaging » ;
- authentification du microcontrôleur ;
- validité de la chaine de certificats ;
- mécanisme d'authentification asymétrique.

Les services de sécurité offerts par les microcontrôleurs sont :
- génération de nombres aléatoires ;
- coprocesseur triple DES ;
- coprocesseur AES ;
- 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 du microcontrôleur, du logiciel embarqué comprenant les tests et la gestion des commandes et des données, et de la structure logique des données.

La figure suivante résume l'architecture des produits évalués :

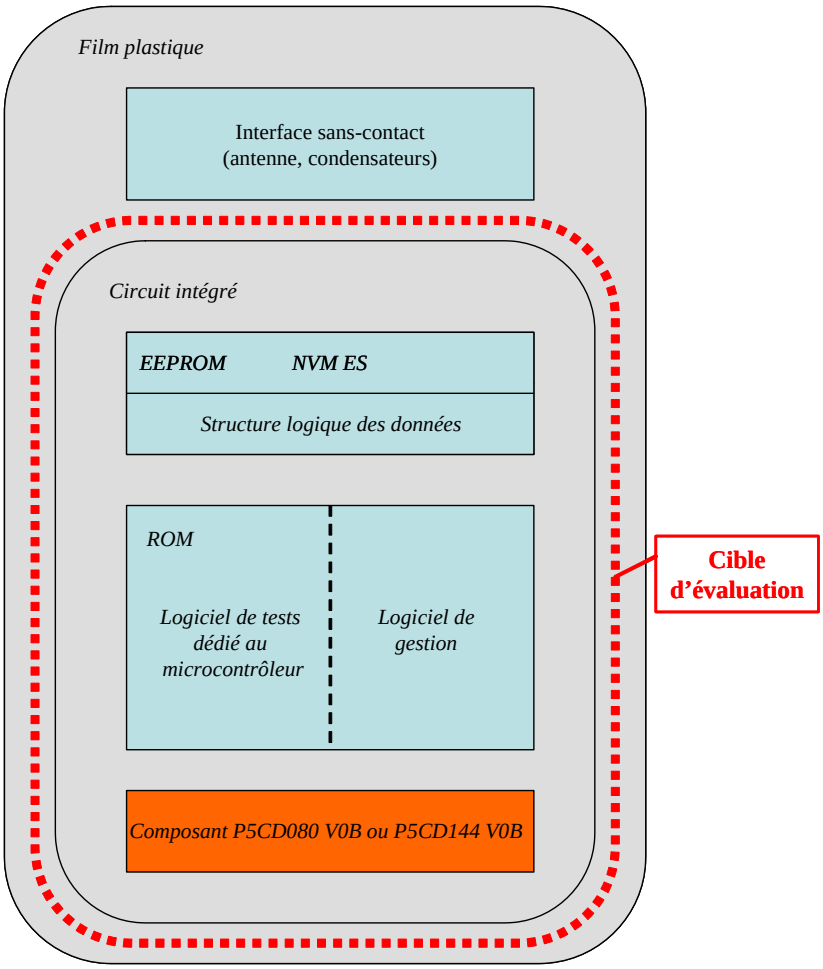

Figure 1 - Architecture du produit

1.2.4. Cycle de vie

Le cycle de vie des produits est le suivant :

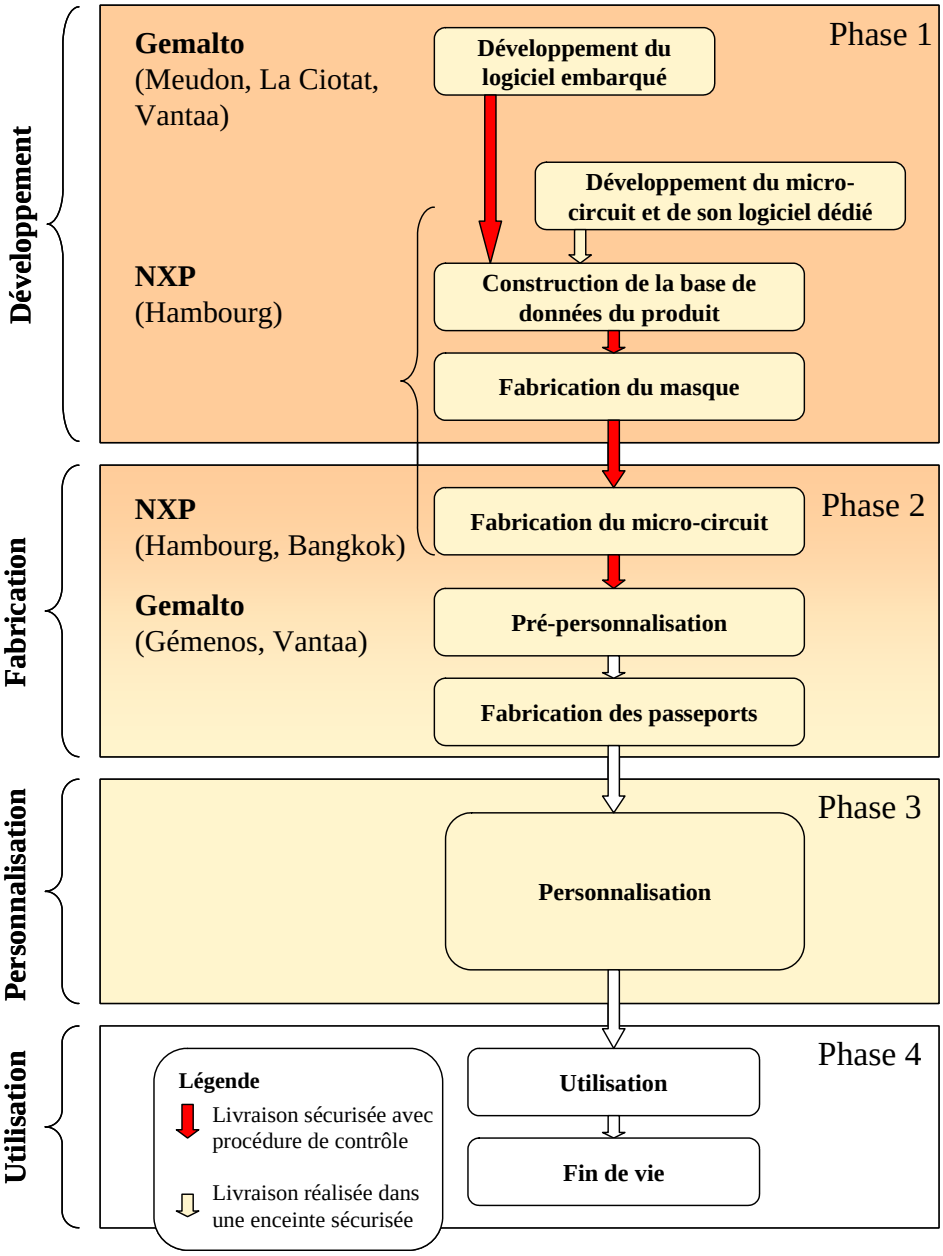

Figure 2 - Cycle de vie du produit

Les produits sont développés sur les sites suivants :

Gemalto

Turvalaaksonkaari 2
FI-01741 Vantaa
Finlande

Gemalto

6 rue de la verrerie
92190 Meudon
France

Gemalto

Avenue du Jujubier
ZI Athelia IV
13705 La Ciotat
France

Gemalto

Avenue du Pic de Bretagne
13881 Gémenos
France

Les microcontrôleurs sont développés et fabriqués par NXP Semiconductors sur les sites suivants :

NXP Semiconductors

GmbH Box 54 02 40,
D-22502 Hamburg,
Allemagne

NXP Semiconductors

303 Chaengwattana Road,
Laksi Bangkok 10210,
Thaïlande

Les « administrateurs du produit » sont les nations ou organisations émettrices du document de voyage.
Les « utilisateurs du produit » sont les voyageurs et les systèmes d'inspection pendant la phase d'utilisation.

1.2.5. Configuration évaluée

Les produits évalués correspondent à une plate-forme e-Passport générique, qui peut être personnalisée sous différentes configurations. Ce rapport de certification porte sur la configuration incluant les mécanismes suivants :

- « Basic Access Control » ;
- « Extented Access Control » avec algorithme RSA ou ECDSA ;
- « Active Authentication ».

L'antenne et la phase de fabrication du document de voyage lui-même ne sont pas incluses dans le périmètre d'évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
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 [AIS 34], 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 les microcontrôleurs déjà certifiés par ailleurs.

Cette évaluation a ainsi pris en compte les résultats des évaluations des microcontrôleurs « P5CD080 V0B » et « P5CD144 V0B » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conformes au profil de protection [PP0002]. Les microcontrôleurs « P5CD080 V0B » et « P5CD144 V0B » ont été certifiés le 5 juillet 2007 sous les références respectives BSI-DSZ-CC-0410-2007 et BSI-DSZ-CC-0411-2007.

L'évaluation s'appuie sur les résultats de l'évaluation du produit « eTravel EAC v1.1 sur composants P5CD080 et P5CD144 » certifié le 14 août 2008 sous la référence DCSSI-2008/28 [2008_28].

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 8 août 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

L'addendum au rapport technique d'évaluation [RTE_ADD], remis à la DCSSI le 25 novembre 2008, détaille les travaux complémentaires menés par le centre d'évaluation.

2.3. 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 [ANA-CRY] et ont été pris en compte par l'évaluateur.

Les mécanismes analysés atteignent le niveau standard défini dans le référentiel cryptographique de la DCSSI (cf. [REF-CRY]).

2.4. Analyse du générateur d'aléas

Les valeurs aléatoires nécessaires aux mécanismes cryptographiques sont générées par un générateur d'aléa disponible sur la carte.
Le générateur d'aléa est un générateur physique couplé avec un générateur logiciel.

Le générateur matériel n'a pas fait l'objet d'une analyse par la DCSSI.

Le générateur logiciel consiste en un retraitement logiciel des aléas issus du générateur matériel de la carte. Le mécanisme de retraitement d'aléa atteint le niveau standard de la DCSSI (cf. [REF-CRY]). Il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléa n'a pas révélé de faiblesse.

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 les produits « eTravel EAC v1.1 80K (version 01 02) sur P5CD080 » et « eTravel EAC v1.1 144K (version 01 02) sur P5CD144 » soumis à l'évaluation répondent aux caractéristiques de sécurité spécifiées dans leur cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur les produits spécifiés au chapitre 1.2 du présent rapport de certification.

L'utilisateur de ces produits certifiés devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] au chapitre 4 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[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, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation des produits

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**	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**3**	Analysis and testing for insecure states
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**4**	Highly resistant

Annexe 2. Références documentaires des produits évalués

[ST]	Cible de sécurité de référence pour l'évaluation : - MAÏA EAC security target, Référence: ST_D1069147, version 0.7, Gemalto Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MAÏA EAC Security target, Référence : ST_D1093538, version 1.0, Gemalto
[RTE]	Evaluation Technical Report – MAÏA project, Référence : MAÏA_ETR_v1.1, version 1.1, Serma Technologies
[RTE_ADD]	Evaluation Technical Report – Addendum – MAÏA project, Référence : MAÏA_ETR_ADD_v1.0, version 1.0, Serma Technologies
[2008_28]	Rapport de certification DCSSI-2008/28 – « eTravel EAC version 1.1 sur composants P5CD080 et P5CD144 », 14 août 2008 SGDN/DCSSI
[CONF]	Class ACM : Configuration list, référence D1086734, version 0.5
[GUIDES]	Guide d'administration du produit : - MAÏA – Administrator guide, référence GUI_D1074871, version 1.2, Gemalto Guide d'utilisation du produit : - MAÏA – User guide, référence GUI_D1074872, version 1.1, Gemalto
[ANA-CRY]	Cotation de mécanismes cryptographiques – Projet MAÏA, N°2630/SGDN/DCSSI/SDS/DR du 20 novembre 2008 SGDN/DCSSI
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001*.
[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*

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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[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 de niveau de robustesse standard, version courante, voir www.ssi.gouv.fr.

[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik)