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-2007/20

Carte MultiApp ID Tachograph 36K : composant SLE66CX360PE masqué par la plate-forme GEOS et l'application TachographV1.1

Paris, le 16 novembre 2007,

Le Directeur central 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 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

DCSSI-2007/20

Nom du produit

Carte MultiApp ID Tachograph 36K : composant SLE66CX360PE masqué par la plate-forme GEOS et l'application TachographV1.1

Référence/version du produit

Ref. T1002264 A7 / version 1.1

Conformité à un profil de protection

BSI-PP-0002-2001 [PP0002]

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté

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

Développeurs

GEMALTO

6 rue de la verrerie 92197 Meudon, FRANCE

Infineon Technologies AG

Postfach 80 09 49, D-81609 München, ALLEMAGNE

Commanditaire

GEMALTO

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

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 la « Carte MultiApp ID Tachograph 36K : composant SLE66CX360PE masqué par la plate-forme GEOS et l'application TachographV1.1, Ref. T1002264 A7 / version 1.1 » développé par GEMALTO et INFINEON.

Ce produit est une carte à puce destinée à être utilisée par les tachygraphes électroniques (équipements d'enregistrement des activités d'un véhicule de transport routier) ou par des ordinateurs personnels (pour réaliser les opérations de contrôle de l'activité du véhicule).
Les principales fonctions de cette carte sont :

- le stockage des identifiants de la carte et de son porteur en vue de l'identification du porteur de la carte afin de fournir les droits d'accès appropriés aux fonctions et aux données, et d'assurer l'imputation des activités ;
- le stockage des informations relatives à l'activité du porteur de la carte.

Les exigences fonctionnelles de cette carte sont spécifiées par [EEC/A1B].
En phase 7, seule l'unité véhicule est autorisée à écrire des données « utilisateur » dans la carte.

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.
La cible de sécurité s'inspire du profil de protection [PP/9911].
Cette cible de sécurité est conforme au profil de protection [PP0002].

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 octets T1 à T7 de son ATR (Answer To Reset) :

ATR: 3B 97 95 C0 2A 31 FE 35 **D0 00 48 01 05 A3 11**

Les octets T1 à T7 de cet ATR ont la signification suivante :

- T1= code composant (D0)
- T2= référence du hardmask sur ce composant (00)
- T3= version du hardmask (48)
- T4= référence du softmask sur ce hardmask (01)
- T5= version du softmask (05)
- T6= référence de l'applet sur ce hardmask (A3)
- T7= version de l'applet (11)

1.2.2. Services de sécurité

Les services de sécurité évalués fournis par le produit sont :

- Services de sécurité basiques :
  - auto-test à l'ouverture de session ;
  - gestion des messages d'erreur et des exceptions ;
  - effacement de données ;
  - intégrité de données ;
  - protections contre les observations extérieures ;
  - protections liées au Card Manager ;
- Services cryptographiques :
  - génération de clés RSA et 3DES ;
  - création et vérification de signatures ;
  - chiffrement/déchiffrement 3DES ;
  - hachage de messages ;
  - génération et vérification de MAC ;
  - canal de confiance ;
  - gestion des PIN ;
- Services de gestion de la sécurité :
  - gestion des accès aux fichiers ;
  - séparation des domaines ;
- Services de surveillance physique.

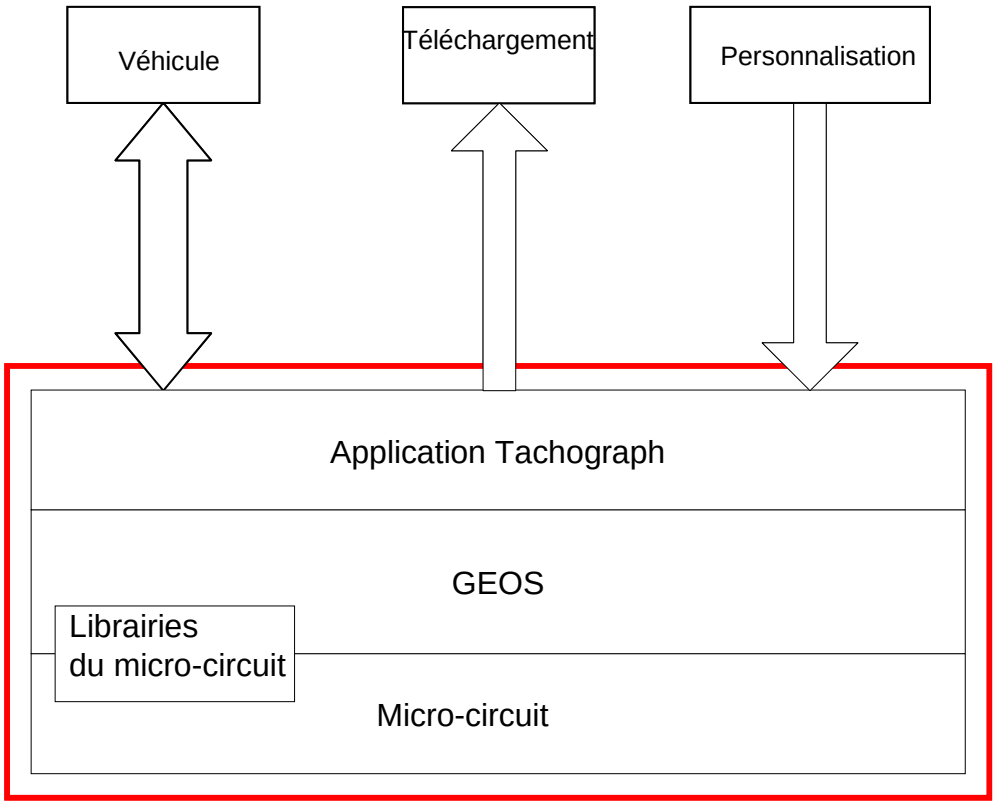
Ces services sont plus précisément décrits au chapitre 6 de [ST].

1.2.3. Architecture

Le produit est constitué :

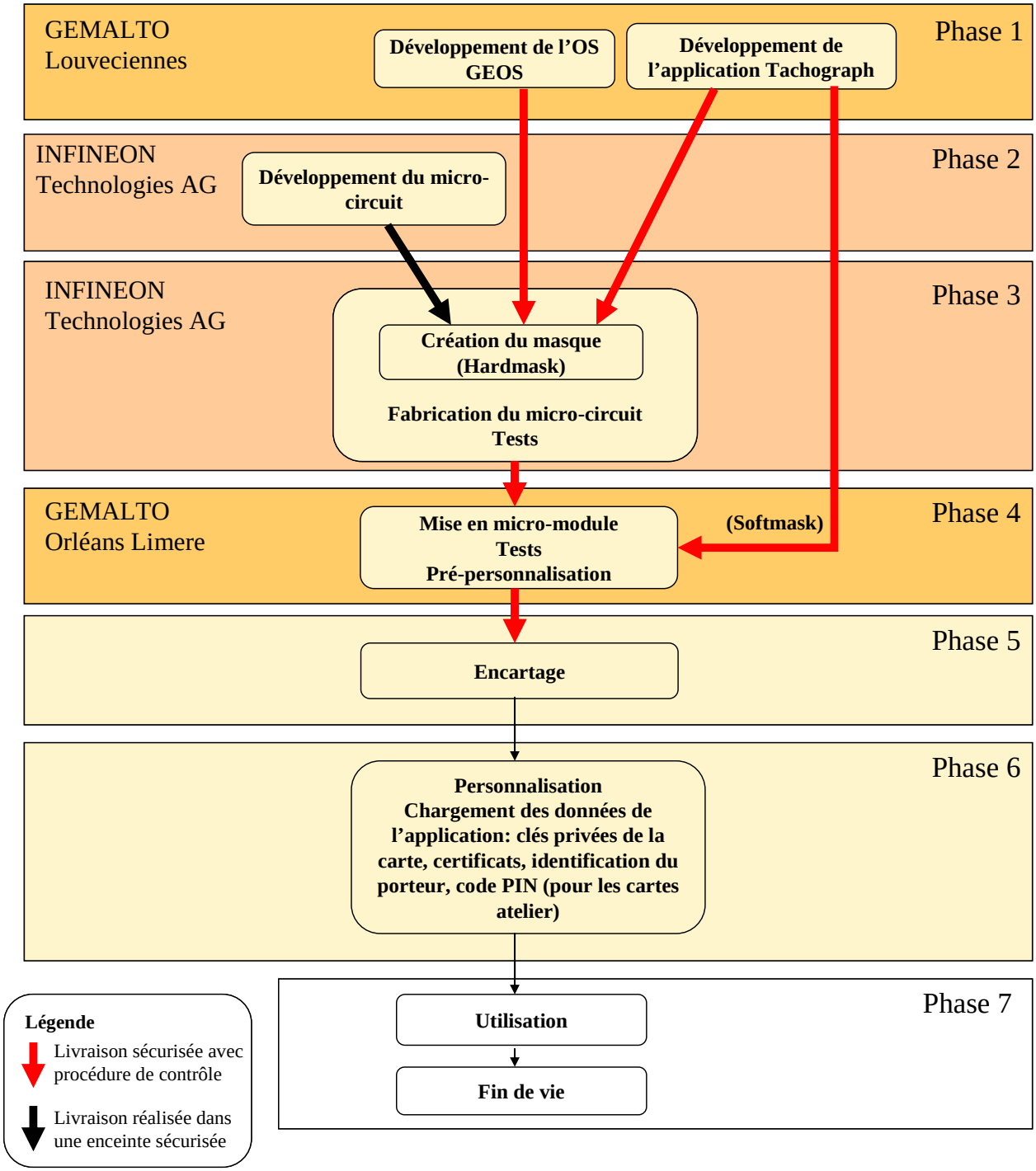
- du microcontrôleur SLE66CX360PE/ m1536a13 (version A13) et de ses bibliothèques cryptographiques RSA2048 (version 1.4) et RMS (version 2.5), développés et fabriqués par INFINEON ;
- du système d'exploitation GEOS, développé par GEMALTO, masqué dans la ROM du microcontrôleur (référence : S1021079 A7, version : 23) ;
- de l'application tachygraphique TachographV1.1, version 1.1, développée par GEMALTO, masquée dans la ROM du microcontrôleur (référence : S1022443 A9, version : 3) ;
- du code correctif (softmask) développé par GEMALTO, chargé en EEPROM (référence : S1025378 A4, version : 12).

L'architecture de cette carte est décrite dans la figure suivante (produit évalué en rouge) :



1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Du point de vue de l'évaluation, les phases 1 à 4 correspondent au développement du produit, la livraison se fait entre la phase 4 et 5, l'installation, la génération et le démarrage se font en phase 4, enfin, les phases 5 à 7 correspondent à l'utilisation du produit évalué.

Le produit a été développé sur le site suivant :

GEMALTO Louveciennes

36-38, route de la Princesse
78431 Louveciennes
France

La conception et la fabrication du micro-circuit sont réalisées par Infineon Technologies AG sur le site suivant :

INFINEON Technologies AG

CCM MTH, Postfach 80 09 49
D-81609 München
Allemagne

Le micro-module est fabriqué par Gemalto sur le site d'Orléans-Limere :

GEMALTO Limere

Avenue de la Pomme de Pin,
45590 Saint Cyr En Val
France

L'utilisateur du produit est le porteur de la carte à puce.
L'administrateur est le personnalisateur (phase 6). Il est recommandé au personnalisateur d'opérer dans un environnement sécurisé et d'utiliser des procédures de sécurité permettant de maintenir la confidentialité et l'intégrité du produit évalué ainsi que de ses données de fabrication et de test (voir O.TEST_OPERATE,en 3.2).

1.2.5. Configuration évaluée

Le produit évalué est le microcontrôleur et son logiciel embarqué identifié au chapitre 1.1.
Le certificat porte sur la configuration « fermée » du produit (les commandes GlobalPlatform pour charger, installer et effacer des applications sont désactivées de façon permanente).
Le certificat porte sur les quatre configurations suivantes (positionnées en phase de personnalisation) :

- carte conducteur,
- carte entreprise,
- carte atelier,
- carte de contrôle.

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 2.3** [CC], 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, ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CCIC] et [CCAP] 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 « SLE66CX360PE/m1536a13 with RSA 2048 V1.4 and specifc IC dedicated software » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002][1]. Ce microcontrôleur a été certifié le 14 septembre 2005 sous la référence BSI-DSZ-CC-0322-2005.
Le niveau de résistance du microcontrôleur a été confirmé en septembre et octobre 2006 dans le cadre du processus de surveillance.

L'évaluation s'appuie sur les résultats d'évaluation du produit « Java Card Open Platform (référence T100921) » certifié le 10 mai 2006 sous la référence 2006/08 (voir [2006/08]).

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 9 novembre 2007, 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 n'a pas été analysée par la DCSSI.

[1] Bien que le certificat du microcontrôleur ne couvre pas le composant ADO_IGS.2, il a été considéré ici que, ce composant ne comprenant pas d'application (IC générique), il satisfaisait par défaut à cette exigence d'assurance. Les règles de composition sont alors satisfaites dans le cadre de la présente évaluation.

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 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 « Carte MultiApp ID Tachograph 36K : composant SLE66CX360PE masqué par la plate-forme GEOS et l'application TachographV1.1, Ref. T1002264 A7 / version 1.1» 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- des procédures de livraison entre les phases 5 à 7 doivent assurer la protection du composant masqué (protection du matériel et des informations du composant masqué) de manière à respecter les objectifs suivants (O.DLV_PROTECT) :
    - non-divulgation des informations relevant de la sécurité ;
    - identification des éléments livrés ;
    - règles de confidentialité (niveau de confidentialité, bordereau de livraison, accusé de réception) ;
    - protection physique pour prévenir tout dommage physique ;
    - stockage sécurisé et procédures de stockage (incluant aussi les composants masqués rejetés) ;
    - traçabilité du composant masqué durant les livraisons (origine de la livraison et moyen d'expédition, accusés de réception, localisation du matériel et des informations) ;
- des procédures entre les phases 5 à 7 doivent assurer que des actions correctives sont prises dans le cas d'opérations erronées durant une livraison (O.DLV_AUDIT) ;
- des procédures entre les phases 5 à 7 doivent assurer que les personnes impliquées dans la livraison du composant masqué possèdent les connaissances suffisantes et ont suivi des formations afin de satisfaire aux exigences des procédures (O.DLV_RESP) ;
- les données de l'application doivent être livrées entre les phases 5 à 7 de manière sécurisée, avec des procédures permettant de garantir l'intégrité et la confidentialité des données de l'application (O.DLV_DATA) ;
- les tests appropriés des fonctionnalités du composant masqué doivent être effectués dans les phases 5 et 6. Durant toutes les phases de fabrication et de tests, des

procédures de sécurité doivent être utilisées dans les phases 5 et 6 pour garantir la confidentialité et l'intégrité du composant masqué et de ses données (O.TEST_OPERATE) ;
- en phase 7, des protocoles et des procédures de communication sécurisés doivent être utilisés entre la carte à puce et le terminal (O.USE_DIAG) ;
- l'émetteur doit s'assurer que les clés secrètes et les clés privées à l'extérieur du composant masqué sont gardées de manière sécurisée. Les clés privées incluent la clé privée européenne, la clé privée du pays et la clé privée du véhicule (OE.Secret_Private_Keys) ;
- l'émetteur doit s'assurer que tous les certificats utilisés dans le système du tachygraphe sont gardés par une IGC (Infrastructure de Gestion de Clés) de confiance. Ceci inclut la révocation de certificats lorsque les clés correspondantes ne sont plus sécurisées (OE.Qualified certificates).

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].

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, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.
[2] 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 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	**2**	Generation log
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**	**2**	Testing: low-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 du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - PHAESTOS-2 Security Target, référence ST_D1038709, version 1.2, Août 2007 Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MultiApp ID Tachograph 36K: Security Target, référence ST_D1038709_public, version 1.2, Août 2007
[RTE]	Rapport technique d'évaluation : - PHAESTOS-2 project - Evaluation Technical Report, référence Phaestos-2_RTE_v1.2.fm, version 1.2 du 9 novembre 2007
[CONF]	PHAESTOS2: Configuration List, référence LIS_06-000407, version 1.4, septembre 2007
[GUIDES]	Guide d'administration du produit (guide de personnalisation) : - PHAESTOS2: Administrator Guide, référence GUI_06-000409, version 1.0, Juillet 2007 Guide d'utilisation du produit : - PHAESTOS2: User Guide, référence GUI_06-000410, version 1.0, Juillet 2007
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI sous la référence BSI-PP-0002-2001.*
[PP/9911]	Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999. *Certifié par la DCSSI sous la référence PP/9911.*
[2006/08]	Rapport de certification 2006/08 - Java Card Open Platform (référence T100921), 10 mai 2006, SGDN/DCSSI
[EEC/A1B]	Council Regulation No 3821/85 on recording equipment in road transport – Annex 1B Requirements for construction, Installation and Inspection

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, SGDN/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, 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.