



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-2012/28

MultiApp ID Tachograph V1.3 sur composant P5CC081 Version (MPH117/FILTER2.2)

Paris, le 05 juillet 2012

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

[Original signé]

Patrick Pailloux



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

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

<i>Référence du rapport de certification</i>	ANSSI-CC-2012/28	
<i>Nom du produit</i>	MultiApp ID Tachograph V1.3 sur composant P5CC081	
<i>Référence/version du produit</i>	T1018062 / Version (MPH117/FILTER2.2)	
<i>Conformité à un profil de protection</i>	Néant	
<i>Critères d'évaluation et version</i>	CC version 3.1 révision 3	
<i>Niveau d'évaluation</i>	EAL4 Augmenté ALC_DVS.2 et AVA_VAN.5	
<i>Développeurs</i>	Gemalto 6 rue de la Verrerie, 92197 Meudon Cedex France	NXP Stresemannallee 101, D-22502 Hamburg Allemagne
<i>Commanditaire</i>	Gemalto 6 rue de la Verrerie, 92197 Meudon Cedex France	
<i>Centre d'évaluation</i>	SERMA Technologies 30 Avenue Gustave Eiffel, 33608 Pessac France	
<i>Accords de reconnaissance applicables</i>	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 modifié. 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	6
1.1. PRÉSENTATION 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>	6
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Cycle de vie</i>	8
1.2.5. <i>Configuration évaluée</i>	10
2. L'ÉVALUATION	11
2.1. RÉFÉRENTIELS D'ÉVALUATION	11
2.2. TRAVAUX D'ÉVALUATION	11
2.3. COTATION DES MÉCANISMES CRYPTOGRAPHIQUES SELON LES RÉFÉRENTIELS TECHNIQUES DE L'ANSSI	11
2.4. ANALYSE DU GÉNÉRATEUR D'ALÉAS.....	11
3. LA CERTIFICATION	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS D'USAGE.....	12
3.3. RECONNAISSANCE DU CERTIFICAT	13
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	13
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	13
ANNEXE 1. NIVEAU D'ÉVALUATION DU PRODUIT.....	14
ANNEXE 2. RÉFÉRENCES DOCUMENTAIRES DU PRODUIT ÉVALUÉ	15
ANNEXE 3. RÉFÉRENCES LIÉES À LA CERTIFICATION	16

1. Le produit

1.1. Présentation du produit

Le produit évalué est une carte à puce, nommée « MultiApp ID Tachograph V1.3 sur composant P5CC081 », référence T1018062, en version (MPH117/FILTER2.2), développée par Gemalto et NXP.

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.

1.2. Description du produit

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

Elle est basée sur la cible de sécurité générique de la directive européenne [EEC/A1B].

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 présents dans la réponse que donne le produit suite à la commande SELECT FILE et READ BINARY (cf. [GUIDES]).

La réponse est :

Fabricant circuit	4790
Type circuit	5081
Version OS	1291
Date OS	1102
Os Release	0201
Données CPLC d'initialisation	XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
Version de filtre OS	22
Application Tachygraphe	A3
Version de l'application	13

1.2.2. Services de sécurité

Les services de sécurité évalués fournis par le produit sont :

- les services de sécurité basiques :

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

1.2.3. Architecture

Le produit « MultiApp ID Tachograph V1.3 sur composant P5CC081 » est constitué des éléments suivants :

- des fonctionnalités matérielles du microcontrôleur (CPU, RAM, ROM, EEPROM, I/O, coprocesseurs cryptographiques) ;
- d'une partie native composée elle-même :
 - d'un gestionnaire de mémoire *Memory Manager* ;
 - d'un gestionnaire de communication *Communication* ;
 - de bibliothèques cryptographiques *Cryptography* ;
- d'une plateforme Java Card MultiAppV2.1 ;
- d'une application Tachograph v1.3;
- d'autres applications.

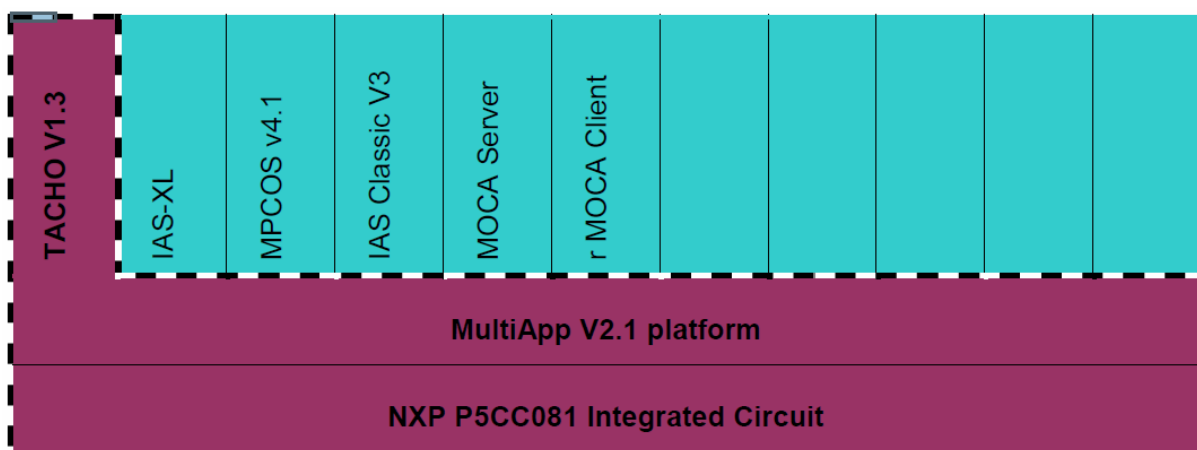
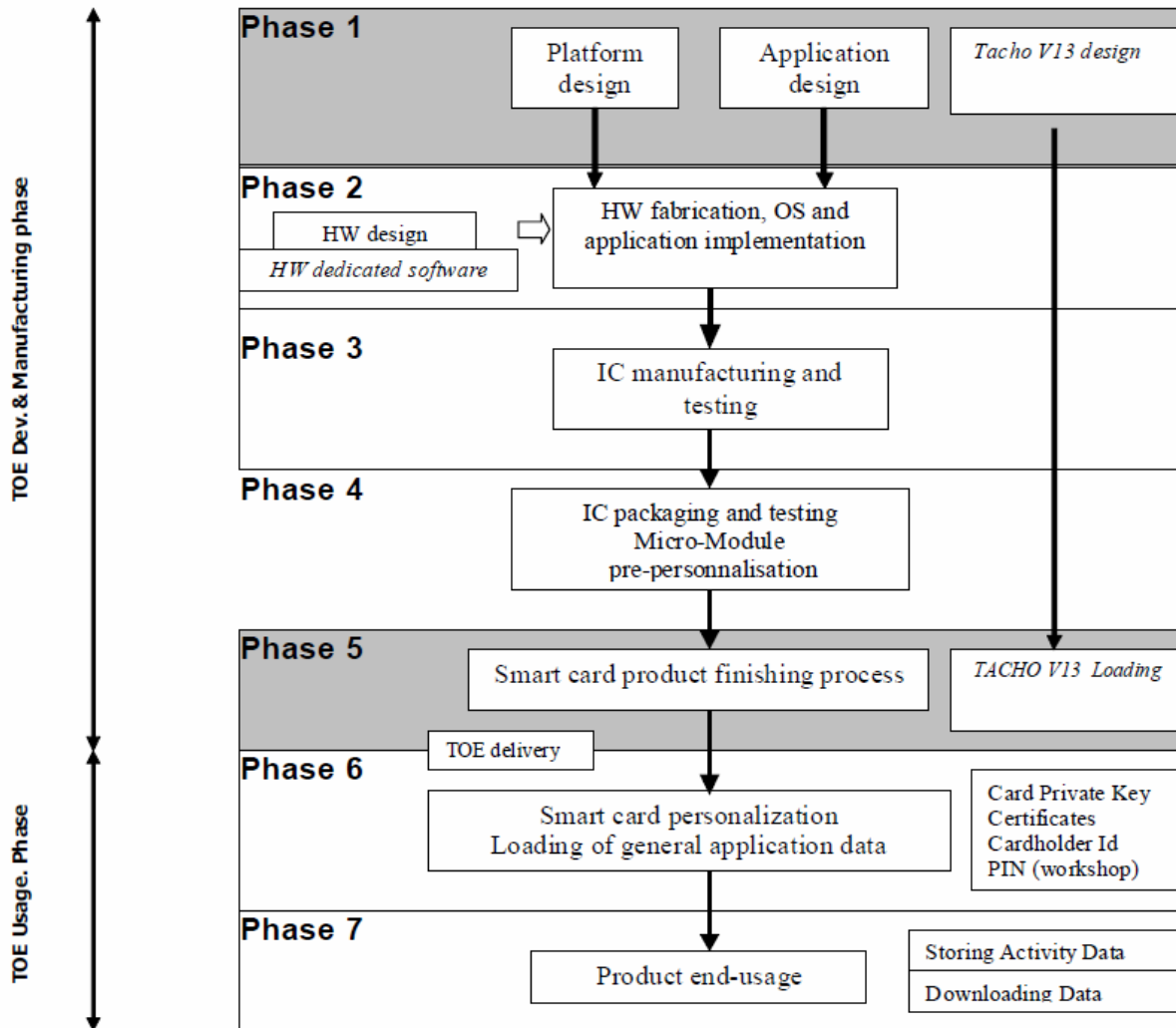


Figure 1 – Architecture et périmètre de la TOE

1.2.4. Cycle de vie

Le circuit est fabriqué chez NXP. Il est ensuite envoyé sur le site de Gemalto où il est initialisé et pré-personnalisé. Le produit est ensuite verrouillé par une clé diversifiée et envoyé au personnalisateur.





Le produit a été développé sur les sites suivants :

Développement (phase 1)	Gemalto Meudon Gemalto La Ciotat Gemalto Gémenos Gemalto Pte Ltd Singapore
Fabrication du micromodule, initialisation et encartage (phase 4)	Gemalto Gémenos Gemalto Pte Ltd Singapore
Pré-personnalisation (phase 5)	Gemalto Gémenos Gemalto Pte Ltd Singapore Gemalto Vantaa

Gemalto

6 Rue de la verrerie
92190 Meudon
France

Gemalto

La Vigie Avenue du Jujubier, ZI Athélia IV BP 90
13702 La Ciotat
France

Gemalto

525 Avenue du Pic de Bertagne
13420 Gémenos
France

Gemalto Pte Ltd

12 Ayer Rajah Crescent, Singapore 139941
Singapore

Gemalto

Turvalaaksonkaari 2
FI-01741 Vantaa
Finlande

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit : le personnalisateur, le gestionnaire de la carte chargé de l'administration de la carte, et comme utilisateur du produit : l'utilisateur du produit final sur le terrain.

1.2.5. Configuration évaluée

Le certificat porte sur l'application tachygraphe version v1.3 sur la plateforme MultiApp ID v2.1, telle que présentée plus haut, au paragraphe 1.2.1, et configurée conformément au guide de personnalisation (cf. [GUIDES]).

Aucune application autre que l'application tachygraphe v1.3 n'est considérée active dans le cadre de cette évaluation. Les autres applications présentes sur le produit ont été prises en compte dans l'analyse de vulnérabilité et ne dégradent pas la sécurité du produit.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

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 P5CC081 au niveau EAL5 augmenté des composants ALC_DVS.2, ASE_TSS.2 et AVA_VAN.5, conforme au profil de protection [PP035]. Ce microcontrôleur a été certifié le 10 novembre 2009 sous la référence [BSI-DSZ-CC-0555-2009].

Le niveau de résistance du microcontrôleur a été confirmé le 3 novembre 2011 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 juin 2012, 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 selon les référentiels techniques de l'ANSSI [REF-CRY] et [REF-KEY] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était dans le périmètre de l'évaluation et a été analysé par le centre d'évaluation. L'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

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 « MultiApp ID Tachograph V1.3 sur composant P5CC081 », référence T1018062, version (MPH117/FILTER2.2) soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

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].

3.3. Reconnaissance du certificat

Ce certificat fait l'objet d'une reconnaissance internationale

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 2010 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé 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 CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², 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'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

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, 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 4+	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	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic 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	4	4	Problem tracking 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	1	1	Well-defined development tools
ASE Security Target Evaluation	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	1	1	Testing: basic 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
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical 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">- PHAESTOS V3 Security Target référence D1189203, version v1.1 du 5 avril 2012 éditée par Gemalto. <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">- PHAESTOS3 Public Security Target référence D1189203, version v1.1p de juin 2012 éditée par Gemalto.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none">- Evaluation Technical Report PHAESTOS-3 Project référence PHAESTOS3_ETR_v1.1, version v1.1 du 28 juin 2012 édité par Serma Technologies.
[CONF]	<p>Liste de configuration :</p> <ul style="list-style-type: none">- PHAESTOS3: Configuration List référence D1128599, version v1.2 du 15 juin 2012, édité par Gemalto.
[GUIDES]	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none">- PREPARATIVE PROCEDURE PHAESTOS3 référence D1190960, version v1.2 du 1^{er} juin 2012 édité par Gemalto. <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none">- OPERATIONAL USER GUIDANCE PHAESTOS3 référence D1190958, version v1.1 du 1er juin 2012 édité par Gemalto.
[BSI-DSZ-CC-0555-2009]	<p>NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 10 novembre 2009 sous la référence BSI-DSZ-CC-0555-2009.</i></p>
[EEC/A1B]	<p>COMMISSION REGULATION (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport.</p>

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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC AP]	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.
[CC GSE]	Common Criteria Supporting Document - Guidance Technical Document – Guidance for smartcard Evaluation, reference CCDB-2010-03-001 version 2.0 revision 1, February 2010.
[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 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr .
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr .