PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2003/12

ICitizen Tachograph :
Carte tachygraphique version 0.9.0
(référence : M256LFCHRON_SI_A5_05_01)

Paris, le 27 août 2003

Le Directeur central de la sécurité des systèmes d'information

Henri Serres

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 terme d'objectifs de sécurité.
Toutefois, la certification ne constitue pas en soi une recommandation du produit par l'organisme de certification, et ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables.

Avant-propos

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 rendu public (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 selon les ITSEC et les Critères Communs sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Le site international concernant la certification selon les Critères Communs est accessible à l'adresse Internet :

www.commoncriteria.org

Accords de reconnaissance des certificats

L'**accord de reconnaissance** européen du SOG-IS de 1999 permet la reconnaissance entre les états signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle 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 :

La direction centrale de la sécurité des systèmes d'information passe aussi des **accords de reconnaissance** avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de la Communauté européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties.

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, le Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

L'accord du Common Criteria Recognition Arrangement, permet la reconnaissance, par les pays signataires de l'accord[1], des certificats délivrés dans le cadre du schéma Critères Communs. La reconnaissance mutuelle s'applique au niveau EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

Les sites des organismes nationaux de certification des pays signataires de l'accord Common Criteria Recognition Arrangement sont :

Pays	Organisme certificateur	Site web
France	DCSSI	www.ssi.gouv.fr
Royaume-Uni	CESG	www.cesg.gov.uk
Allemagne	BSI	www.bsi.bund.de
Canada	CSE	www.cse-cst.gc.ca
Australie-Nouvelle Zélande	AISEP	www.dsd.gov.au/infosec
Etats-Unis	NIAP	www.niap.nist.gov

[1] En janvier 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada et l'Australie-Nouvelle Zélande ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Espagne, la Finlande, la Grèce, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, l'Autriche et le Japon.

Table des matières

1. Le produit évalué

1.1. Contexte

Le règlement de la commission européenne (CEE) 3821/85 sur l'appareil de contrôle dans le domaine des transports par route sert de base à l'actuel tachygraphe analogique qui enregistre le temps de conduite, les arrêts, les temps de repos ainsi que les temps consacrés aux autres travaux.
La Commission s'est efforcée de renforcer l'application dans ce secteur en modifiant le règlement (CEE) 3821/85 par le règlement (CE) 2135/98, qui introduit une nouvelle génération de tachygraphes entièrement électroniques. Ce tachygraphe électronique est un appareil d'enregistrement et de stockage plus sûr et plus précis que l'appareil actuel. Ce nouveau dispositif peut enregistrer l'ensemble des activités du véhicule, comme par exemple la distance, la vitesse ou les temps de conduite et de repos du conducteur. Il sera équipé d'une imprimante, pour permettre les contrôles en bord de route et le conducteur recevra une carte à microprocesseur qu'il devra introduire dans le tachygraphe lors de la prise des commandes du véhicule.
Le règlement (CE) 1360/2002 de la commission [EC 1360/2002] et son annexe 1B [EC/A1B], publié le 5 août 2002 au journal officiel de la commission européenne définit les spécifications techniques pour le tachygraphe numérique.
Quatre types de cartes seront disponibles : les cartes des conducteurs, les cartes d'atelier, les cartes d'entreprise et les cartes de contrôle.

1.2. Identification du produit

Le produit évalué est le composant masqué **ICitizen Tachograph version 0.9.0** développé par Schlumberger Systèmes et Infineon Technologies AG, composé des éléments suivants :

Element	Version	Développeur
Application Tachograph	SC_V0.9.0	Schlumberger Systèmes
GEOS – Generic Operating System	PLATFORM_T_SC_04_02;9	Schlumberger Systèmes
Librairie ACE	1.0	Infineon Technologies AG
Librairie RMS	1.3	Infineon Technologies AG
Micro-circuit SLE66CX322P	GC/B14	Infineon Technologies AG

La référence du composant masqué évalué est **M256LFCHRON_SI_A5_05_01**.
La référence donnée par Infineon à Schlumberger Systèmes pour le masque constitué du système d'exploitation GEOS et de l'application Tachograph est SB102.
Le composant masqué sert de base aux différents types de carte. Le choix du type de carte se fait en phase de personnalisation (Figure 2).

1.3. Les développeurs

Schlumberger Systèmes

36-38 rue de la Princesse
BP45

78431 Louveciennes Cedex
France

Infineon Technologies AG

Postfach 80 17 60
81617 München
Allemagne

1.4. Description du produit évalué

1.4.1. Architecture

Le produit évalué peut être schématisé de la manière suivante :

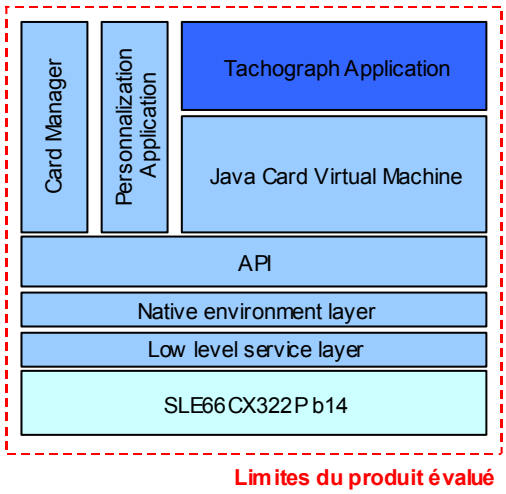

Figure 1 - Architecture du produit évalué

Une description détaillée de l'architecture de l'application se trouve dans le document [HLD].

1.4.2. Cycle de vie

Le cycle de vie du produit évalué s'inscrit dans le cycle de vie à 7 phases d'une carte à puce :

- Le développement du système d'exploitation GEOS et de l'application Tachoghaph, sur le site de développement de Louveciennes (cf §2.5.4) (phase 1) ;
- Le développement du micro-circuit SLE66CX322P par Infineon (phase 2) ;
- La création du masque par Infineon puis la fabrication du micro-circuit masqué par les logiciels de Schlumberger Systèmes (phase 3) ;
- La mise en micro-module des micro-circuits, et la pré-personnalisation de chacun des micro-modules, sur le site d'Orléans de Schlumberger Systèmes (cf §2.5.4) (phase 4) ;
- L'encartage des micro-modules (phase 5). Ces derniers sont livrés par Schlumberger Systèmes de manière sécurisée entre les phases 4 et 5 ;
- La personnalisation des cartes (phase 6) ;

- Et l'utilisation de la carte par son porteur (phase 7). La fin de vie de la carte (correspondant à la destruction de la carte) est aussi comprise dans cette phase.

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.

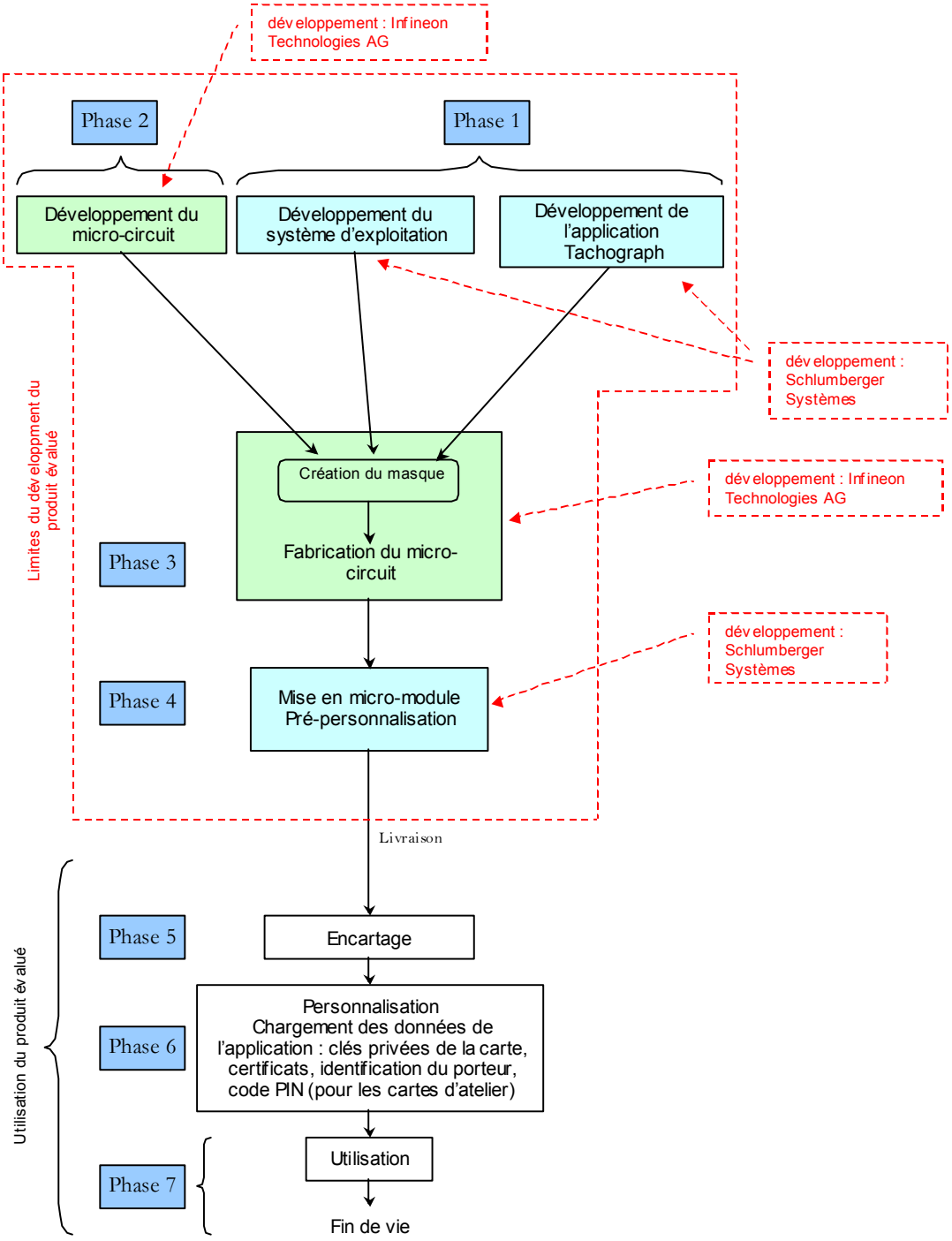

Figure 2 - Cycle de vie du produit évalué dans celui de la carte à puce

1.4.3. Périmètre et limites du produit évalué

Le produit évalué est le composant masqué constitué du micro-circuit SLE66CX322P/b14 développé par Infineon Technologies AG incluant les librairies RMS version 1.3 et ACE version 1.0, du système d'exploitation GEOS référence PLATFORM_T_SC_04_02;9 et de l'application Tachograph référence SC_V0.9.0 développés par Schlumberger Systèmes. Le produit évalué est le produit sortant de la phase de pré-personnalisation, phase 4 (Figure 2).

1.5. Utilisation et administration

1.5.1. Utilisation

L'utilisateur du produit est le porteur de la carte à puce contenant le composant évalué. Le guide pour les porteurs de carte à puce est le guide [USR].

1.5.2. Administration

L'administrateur est le personnalisateur (phase 6). Le guide pour le personnalisateur est le guide [ADM].

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 (objectif de sécurité sur l'environnement O.TEST_OPERATE, § 3.11.4).

2. L'évaluation

2.1. Centre d'évaluation

SERMA Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Téléphone : +33 (0)5 57 26 08 64

Adresse électronique : m.dus@serma.com

L'évaluation s'est déroulée de **novembre 2002** à **juillet 2003**.

2.2. Commanditaire

Schlumberger Systèmes

36-38 rue de la Princesse
BP45
78431 Louveciennes Cedex
France

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation respectent les exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].
L'évaluation de ce produit s'appuie sur le certificat du micro-circuit «Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, a27 and b14» émis par le BSI en août 2003 sous la référence : BSI-DSZ-CC-0223-2003 [322P-B14]. Ce certificat atteste que le micro-circuit SLE66CX322P atteint le niveau EAL 5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 et qu'il est conforme au profil de protection référencé PP/BSI-0002 «Smartcard Integrated Circuit Protection Profile v2.0» [SSVG]. La validité de ce certificat est reconnue par le schéma français en vertu de l'accord de reconnaissance du SOG-IS [SOG-IS]. Le micro-circuit étant certifié par le schéma allemand, les travaux effectués dans

le cadre de cette évaluation ont porté sur l'évaluation du masque et sur son intégration sûre dans le micro-circuit conformément aux interprétations sur la composition d'un circuit intégré et d'un logiciel embarqué [JIL-Comp].

2.5.1. Développement du produit

La classe d'assurance ADV – développement – définit les exigences de raffinement pas à pas des fonctions de sécurité du produit depuis ses spécifications globales dans la cible de sécurité [ST] jusqu'à l'implémentation. Chacune des représentations des fonctions de sécurité du produit qui résulte de ce processus fournit des informations qui aident l'évaluateur à déterminer si les exigences fonctionnelles du produit ont été satisfaites.
L'analyse des documents associés à la classe ADV montre que les exigences fonctionnelles sont correctement et complètement raffinées dans les différents niveaux de représentation du produit (spécifications fonctionnelles (FSP), sous-systèmes (HLD), modules (LLD) et implémentation (IMP)), jusqu'à l'implémentation de ses fonctions de sécurité.
Les documents fournis pour la classe ADV – développement – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.2. Documentation

Du point de vue de l'évaluation, l'administrateur est le personnalisateur, et les utilisateurs sont les porteurs des cartes tachygraphes. Quatre types de cartes sont disponibles : les cartes des conducteurs, les cartes d'atelier, les cartes d'entreprise et les cartes de contrôle.
Les guides utilisateur [USR] et administrateur [ADM] répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.3. Livraison et installation

Deux livraisons sont considérées. La première est la livraison du code des applications au fondeur Infineon : Schlumberger Systèmes fournit au fondeur (phase 1 à 3) le code source du système d'exploitation et de l'application Tachograph afin que tous deux soient masqués sur le composant SLE66CX322P. La seconde livraison est celle de Schlumberger Systèmes vers l'encarteur du micro-module (phase 4 à phase 5). Cette livraison correspond à la transition entre le développement du produit évalué et l'utilisation du produit évalué, au sens Critères Communs [CC]. Schlumberger Systèmes offre deux possibilités de livraison des micro-modules : le transport sécurisé vers le site de l'encarteur ou la mise à disposition des micro-modules sur son quai d'expédition afin que le client puisse lui-même procéder au transport sécurisé des micro-modules.
La procédure [DEL] de livraison est suffisante pour répondre aux exigences demandées : elle permet de connaître l'origine de la livraison et de détecter une modification du produit pendant la livraison.
L'installation du produit correspond à la phase de pré-personnalisation (phase 4). Les procédures d'installation, de génération et de démarrage [IGS] permettent d'obtenir une configuration sûre de l'application. De plus, les informations enregistrées dans un fichier log sur le site de pré-personnalisation permettent de retrouver et de déterminer quand et comment chaque micro-module a été pré-personnalisé.
Les documents fournis pour la classe ADO – livraison et opération – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.4. L'environnement de développement

Le système de gestion de configuration est utilisé conformément au plan de gestion de configuration [ACM].
La liste de configuration [LGC] identifie les éléments tracés par le système de gestion de configuration. Les éléments de configuration identifiés dans la liste de configuration sont maintenus par le système de gestion de configuration. Les procédures de génération de l'application sont efficaces pour s'assurer que les bons éléments de configuration sont utilisés pour générer l'application.
Le système d'exploitation et l'application Tachograph sont développés sur le site de Schlumberger Systèmes situé :

36-38 rue de la Princesse
78431 Louveciennes
France

Le micro-circuit est mis en micro-module et pré-personnalisé sur le site de Schlumberger Systèmes situé :

284, avenue de la Pomme de Pin
45060 Saint-Cyr-En-Val
France

Les mesures de sécurité décrites dans les procédures fournissent le niveau nécessaire de protection pour maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.
La vérification de la mise en œuvre des procédures de développement et de gestion de configuration a été effectuée lors de l'audit des sites ci-dessus (Annexe 1 et Annexe 2). Le rapport d'audit se trouve sous la référence [Audit].
Les documents fournis pour la classe ACM – gestion de la configuration – et ALC – support au cycle de vie – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.5. Tests fonctionnels

L'évaluateur a vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit sont reliées à au moins un test fonctionnel dans la documentation de test. Il a vérifié aussi que toutes les caractéristiques fonctionnelles de chaque fonction de sécurité, telle qu'elles sont décrites dans la conception de haut niveau [HLD] et dans la conception de bas niveau [LLD], sont couvertes par les tests du développeur.
Les tests ont été réalisés sur la version du produit identifiée au paragraphe 1.2, dans les configurations suivantes :

- le composant masqué pré-personnalisé ;
- la carte à puce contenant le micro-module personnalisé (c'est-à-dire en phase 7) suivant l'un des quatre types de configuration possibles : conducteur, entreprise, atelier et contrôle.

2.5.6. Estimation des vulnérabilités

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement couvertes.

L'évaluateur a réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités supplémentaires.
Le produit, dans son environnement d'exploitation, est résistant à des attaquants disposant d'un potentiel d'attaque **élevé**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du produit ICitizen Tachograph version 0.9.0.

3.2. Niveau d'évaluation

Le produit ICitizen Tachograph version 0.9.0 a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL4**[1] **augmenté** des composants d'assurance suivants, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADO_IGS.2	Generation log
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
ATE_DPT.2	Testing: low-level design
AVA_MSU.3	Analysis and testing for insecure states
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

Pour tous les composants du niveau d'évaluation du produit, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	Réussite

[1] En Annexe 5 se trouve un tableau récapitulant les différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.2	Generation log	Réussite
Class ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
ADV_SPM.1	Informal TOE security policy model	Réussite
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
Class ALC	**Life cycle support**	
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.2	Testing: low-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_MSU.3	Analysis and testing for insecure states	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** [ST] suivantes[1] :

- Potential violation analysis (FAU_SAA.1)
- Selective proof of origin (FCO_NRO.1)
- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key distribution (FCS_CKM.2)

[1] En Annexe 4 se trouve un tableau complet explicitant les exigences fonctionnelles de sécurité du produit évalué.

- Cryptographic key access (FCS_CKM.3)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Basic data authentication (FDP_DAU.1)
- Export of user data without security attributes (FDP_ETC.1)
- Export of user data with security attributes (FDP_ETC.2)
- Import of user data without security attributes (FDP_ITC.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Authentication failure handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- Unforgeable authentication (FIA_UAU.3)
- Single-use authentication mechanisms (FIA_UAU.4)
- Timing of identification (FIA_UID.1)
- User-subject binding (FIA_USB.1)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Management of TOE security functions data (FMT_MTD.1)
- Specification of management functions (FMT_SMF.1)
- Security roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Resistance to physical attack (FPT_PHP.3)
- TOE security functions domain separation (FPT_SEP.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)
- TOE security functions testing (FPT_TST.1)
- Inter-TSF trusted channel (FTP_ITC.1)

3.4. Résistance des fonctions

Seule la fonction d'authentification (code PIN) pour la carte atelier a fait l'objet d'une estimation du niveau de résistance.
Le niveau de résistance de cette fonction de sécurité est jugé **élevé** (**SOF-High**).

3.5. Analyse des mécanismes cryptographiques

A la demande du commanditaire, les mécanismes cryptographiques du composant masqué ICitizen Tachograph version 0.9.0 ont été analysés par le laboratoire d'analyse cryptographique de la DCSSI. Les résultats de cette analyse sont résumés en Annexe 3.

3.6. Conformité à l'annexe 1B du règlement EC 1360/2002

Conformément au document d'interprétation de l'annexe 1B du règlement EC 1360/2002 [JIL-Tacho], l'évaluateur a vérifié la conformité de la cible de sécurité du produit [ST] à l'appendice 10 de l'annexe 1B du règlement EC 1360/2002 [EC/A1B].
Le niveau d'évaluation atteint par le produit est **EAL4 augmenté** des composants ADO_IGS.2, ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_MSU.3 et AVA_VLA.4 (Tableau 1). Ce niveau d'évaluation **correspond** au niveau **E3hAP** définit dans le document [JIL-Tacho], augmenté des composants ACM_AUT.1, ADV_SPM.1, ALC_DVS.2, ALC_LCD.1, AVA_MSU.3.
L'évaluateur a vérifié que la cible de sécurité [ST] du produit respecte les interprétations des annexes A et B du document [JIL-Tacho], concernant le niveau d'évaluation et les exigences fonctionnelles de sécurité. Par conséquent, conformément à ce document, le niveau de sécurité de ICitizen Tachograph version 0.9.0 peut être considéré comme atteignant le niveau **ITSEC E3 fort**, niveau d'évaluation requis par l'annexe 1B du règlement EC 1360/2002 [EC/A1B].

3.7. Conformité à un profil de protection

Le certificat du micro-circuit SLE66CX322P/b14 [322P-B14] émis par le BSI atteste que sa cible de sécurité est conforme au profil de protection BSI-PP-0002 [SSVG].

3.8. Reconnaissance européenne (SOG-IS)

Ce certificat a été émis dans les conditions de l'accord du SOG-IS. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité.

3.9. Reconnaissance internationale (CC RA)

Ce certificat a été émis dans les conditions de l'accord du CC RA. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité.
Les augmentations suivantes ne sont par reconnues dans le cadre du CC RA [CC RA] : ADO_IGS.2, ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_MSU.3 et AVA_VLA.4 (Tableau 1).

3.10. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.11) ainsi que les recommandations se trouvant dans les guides utilisateur [USR] et administrateur [ADM].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

3.11. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST] :

3.11.1. Objectifs de sécurité sur la phase 1

- Le logiciel embarqué sur le micro-circuit doit être développé de manière sécurisée, en utilisant des outils de développement logiciel et des outils de tests d'intégration matériel-logiciel qui permettront de garder l'intégrité du programme et des données (O.DEV_TOOLS) ;
- Le développeur du logiciel embarqué doit utiliser des procédures pour contrôler l'enregistrement et l'utilisation des outils de développement et des documentations. Ces procédures doivent permettre de garantir l'intégrité et la confidentialité des biens du composant masqué. De plus, les outils de développement doivent être accessibles uniquement aux personnes autorisées. Les informations confidentielles sur les biens du composant masqué sont accessibles aux personnes autorisées uniquement (O.DEV_DIS_ES) ;
- Le logiciel embarqué sur le micro-circuit doit être livré de manière sécurisé entre le développeur du logiciel embarqué et le fondeur, à l'aide de procédures garantissant l'intégrité du logiciel et sa confidentialité (si nécessaire) (O.SOFT_DLV) ;
- Les données d'initialisation doivent être accessibles uniquement aux personnes autorisées (O.INIT_ACS) ;
- Les échantillons du composant masqué utilisés pour les tests doivent être accessibles uniquement aux personnes autorisées (O.SAMPLE_ACS) ;

3.11.2. Objectifs de sécurité sur la livraison du produit (phases 4 à 7)

- Les procédures de livraison doivent assurer la protection du composant masqué (protection matérielle 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 à 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 doivent assurer que des actions correctives sont prises dans le cas d'opérations erronées durant une livraison (O.DLV_AUDIT) ;
- Des procédures 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) ;

3.11.3. Objectifs de sécurité sur la livraison de la phase 1 à 4,5 et 6

- Les données de l'application doivent être livrées entre le développeur du logiciel embarqué et la mise en micro-module, ou l'encarteur, ou le personnalisateur de

manière sécurisée, avec des procédures permettant de garantir l'intégrité et la confidentialité des données de l'application (O.DLV_DATA) ;

3.11.4. Objectifs de sécurité sur les phases 4 à 6

- Les tests appropriés des fonctionnalités du composant masqué doivent être effectués dans les phases 4 à 6. Durant toute les phases de fabrication et de tests, des procédures de sécurité doivent être utilisées dans les phases 4, 5 et 6 pour garantir la confidentialité et l'intégrité du composant masqué et de ses données (O.TEST_OPERATE) ;

3.11.5. Objectifs de sécurité sur la phase 7

- Des protocoles et des procédures de communication sécurisées doivent être utilisés entre la carte à puce et le terminal (O.USE_DIAG) ;

3.11.6. Objectifs de sécurité supplémentaires

- 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).

3.12. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que ICitizen Tachograph version 0.9.0 identifié au paragraphe 1.2 et décrite au paragraphe 1.4 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

De plus, le centre de certification atteste que le composant ICitizen Tachograph version 0.9.0 satisfait aux exigences de sécurité définies à l'appendice 10 de l'annexe 1B du règlement EC 1360/2002 [EC/A1B] concernant les objectifs généraux de sécurité de la carte tachygraphique. Le certificat de sécurité est délivré conformément aux dispositions cet appendice et le niveau de sécurité du produit atteint le niveau d'évaluation ITSEC E3 fort requis par l'annexe 1B [EC/A1B].

Annexe 1. rapport de visite du site de Louveciennes relatif à l'environnement de développement

Le site de développement de **Schlumberger Systèmes situé 36-38, rue de la princesse, BP 45, 78431 Louveciennes Cedex**, a fait l'objet, dans le cadre de l'évaluation du produit ICitizen Tachograph version 0.9.0, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4, ACM_SCP.2)
- la livraison : **ADO** (ADO_DEL.2)
- le support au cycle de vie : **ALC** (ALC_DVS.2)

Le développement du système d'exploitation GEOS et de l'application Tachograph s'effectue sur le site de Louveciennes. Une fois son développement terminé, le code source de ces logciels est transmis de manière sécurisée à Infineon Technologies AG, pour la phase 3 (Figure 2).
La visite par le centre d'évaluation accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 2. rapport de visite du site d'Orléans relatif à l'environnement de développement

Le site de développement de **Schlumberger Systèmes situé 284, avenue de la Pomme de Pin 45060 Saint-Cyr-En-Val**, a fait l'objet, dans le cadre de l'évaluation du produit ICitizen Tachograph version 0.9.0, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4, ACM_SCP.2)
- la livraison : **ADO** (ADO_DEL.2)
- le support au cycle de vie : **ALC** (ALC_DVS.2)

Le micro-circuit masqué est envoyé par Infineon sur le site d'Orléans de Schlumberger Systèmes. Sur ce site, le composant est mis en micro-module et pré-personnalisé puis le livre à un client final.
La visite par le centre d'évaluation accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 3. Analyse des mécanismes cryptographiques

Les Critères Communs [CC] ne requièrent pas l'estimation de la résistance des mécanismes cryptographiques présents dans les fonctions de sécurité spécifiées dans la cible de sécurité du produit en évaluation. Toutefois, considérant qu'ils représentent une part importante du niveau de sécurité du produit, le centre de certification propose au commanditaire de l'évaluation l'analyse de ce type de mécanismes, dont les résultats figurent ci-après. Ces résultats ne remettent pas en cause le certificat Critères Communs de conformité du produit à sa cible de sécurité.

- Mécanismes en phase de **personnalisation** :
  - **Authentification mutuelle**

    Ce mécanisme est coté de niveau élevé.
  - **Protection des données en intégrité**

    En mode *secure channel MAC* seule l'intégrité des données est assurée. Le mécanisme d'intégrité utilisé est coté de niveau faible. Toutefois, l'utilisation d'un environnement sécurisé et le respect de procédures de sécurité durant la phase de personnalisation permet de contrer cette faiblesse. Ces recommandations sont cependant déjà requises dans le profil de protection 99/11 [PP/9911] et reprises dans la cible de sécurité [ST] du produit au travers de l'objectif de sécurité sur l'environnement O.TEST_OPERATE (cf § 3.11.4).
  - **Protection des données en confidentialité et en intégrité**

    En mode *secure channel ENC*, la confidentialité et l'intégrité des données sont assurés. Ce mécanisme est coté de niveau élevé.
- Mécanismes en phase d'**utilisation** :
  - **Authentification mutuelle**

    Ce mécanisme est conforme aux spécifications décrites dans l'annexe 1B [EC/A1B] du règlement EC 1360/2002.
  - **Protection des données en intégrité**

    Ce mécanisme est conforme aux spécifications décrites dans l'annexe 1B.
  - **Protection des données en confidentialité et en intégrité**

    Ce mécanisme est conforme aux spécifications décrites dans l'annexe 1B.
- Mécanisme de **retraitement d'aléa** :

  Ce mécanisme est coté de niveau faible. Il n'apporte aucune sécurité supplémentaire, toutefois, il n'altère pas la qualité du générateur de nombre aléatoire du composant SLE66CX322P, certifié par ailleurs.

Annexe 4. Exigences fonctionnelles de sécurité du produit evalué

Attention : les descriptions des composants fonctionnels suivants sont donnés à titre indicatif. Seule une lecture attentive de la cible de sécurité [ST] peut apporter la description exacte des exigences fonctionnelles auxquelles répond le produit.

Class FAU	**Security audit**
Security audit analysis	
FAU_SAA.1	*Potential violation analysis* Le produit doit implémenter un seuil de détection élémentaire, défini selon une règle fixée (spécifiée dans la cible de sécurité [ST]).
Class FCO	**Communication**
Non-repudiation of origin	
FCO_NRO.1	*Selective proof of origin* Le produit doit, suite à la requête du destinataire et/ou de l'émetteur, donner la preuve de l'origine des informations (spécifiées dans la cible de sécurité [ST]).
Class FCS	**Cryptographic support**
Cryptographic key management	
FCS_CKM.1	*Cryptographic key generation* Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiés qui peuvent être basés sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.2	*Cryptographic key distribution* Le produit doit distribuer des clés cryptographiques conformément à une méthode de distribution spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.3	*Cryptographic key access* Les accès aux clés cryptographiques doivent être effectués conformément à une méthode d'accès spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.4	*Cryptographic key destruction* Le produit doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée

	(spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Data authentication	
FDP_DAU.1	*Basic data authentication* Le produit doit être capable de garantir l'authenticité des informations contenues dans des objets spécifiés dans la cible de sécurité [ST] (e.g. des documents).
Export to outside TSF control	
FDP_ETC.1	*Export of user data without security attributes* Le produit doit appliquer les règles de sécurité appropriées lors de l'exportation de données de l'utilisateur à l'extérieur. Les données de l'utilisateur exportées par cette fonction sont exportées sans les attributs de sécurité qui leur sont associés.
FDP_ETC.2	*Export of user data with security attributes* Le produit doit appliquer les règles de sécurité appropriées en utilisant une fonction qui associe précisément et sans ambiguïté les attributs de sécurité avec les données de l'utilisateur qui sont exportées.
Import from outside TSF control	
FDP_ITC.1	*Import of user data without security attributes* Les attributs de sécurité doivent représenter correctement les données de l'utilisateur et doivent être fournis séparément de l'objet.
Residual information protection	
FDP_RIP.1	*Subset residual information protection* Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets lors de l'allocation ou de la désallocation de la ressource.
Stored data integrity	
FDP_SDI.2	*Stored data integrity monitoring and action* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées et entreprendre des actions (spécifiées dans la cible de sécurité [ST]) suite à une détection d'erreur.
Class FIA	**Identification and authentication**
Authentication failures	
FIA_AFL.1	*Authentication failure handling* Le produit doit être capable d'arrêter le processus d'établissement d'une

	session après un nombre spécifié de tentatives d'authentification infructueuses d'un utilisateur. Il doit aussi, après la clôture du processus d'établissement d'une session, être capable de désactiver le compte de l'utilisateur ou le point d'entrée (e.g. station de travail) à partir duquel les tentatives ont été faites jusqu'à ce qu'une condition définie par un administrateur se réalise.
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
User authentication	
FIA_UAU.1	*Timing of authentication* Le produit autorise un utilisateur à exécuter certaines actions, spécifiées dans la cible de sécurité [ST], avant que son identité ne soit authentifiée.
FIA_UAU.3	*Unforgeable authentication* Le mécanisme d'authentification doit être capable de détecter et d'empêcher l'utilisation de données d'authentification qui ont été contrefaites ou copiées.
FIA_UAU.4	*Single-use authentication mechanisms* Le mécanisme d'authentification doit fonctionner avec des données d'authentification à usage unique.
User identification	
FIA_UID.1	*Timing of identification* Le produit autorise les utilisateurs à exécuter certaines actions, identifiées dans la cible de sécurité [ST], avant d'être identifiés.
User-subject binding	
FIA_USB.1	*User-subject binding* La relation entre les attributs de sécurité de l'utilisateur et un sujet agissant pour le compte de cet utilisateur doit être maintenue.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.2	*Secure security attributes* Le produit doit garantir que les valeurs assignées aux attributs de sécurité sont valides par rapport à l'état sûr.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Management of TSF data	
FMT_MTD.1	*Management of TSF data* Les utilisateurs autorisés peuvent gérer les données des fonctions de sécurité du produit.
Specification of Management Functions	

FMT_SMF.1	*Specification of Management Functions* Le produit doit fournir les fonctions de gestion de la sécurité spécifiées dans la cible de sécurité [ST].
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiées dans la cible de sécurité [ST]).
Class FPR	**Privacy**
Unobservability	
FPR_UNO.1	*Unobservability* Le produit n'autorise pas certains utilisateurs (spécifiées dans la cible de sécurité [ST]) à déterminer si certaines opérations (spécifiées dans la cible de sécurité [ST]) sont en cours d'exécution.
Class FPT	**Protection of the TSF**
Fail secure	
FPT_FLS.1	*Failure with preservation of secure state* Le produit doit préserver un état sûr dans le cas de défaillances identifiées.
TSF physical protection	
FPT_PHP.3	*Resistance to physical attack* Le produit doit empêcher ou résister à certaines intrusion physique (spécifiées dans la cible de sécurité [ST]) sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
Domain separation	
FPT_SEP.1	*TSF domain separation* Le produit doit offrir un domaine protégé et distinct pour les fonctions de sécurité du produit et procurer une séparation entre sujets.
Inter-TSF TSF data consistency	
FPT_TDC.1	*Inter-TSF basic TSF data consistency* Le produit doit offrir la capacité de garantir la cohérence des attributs lors des échanges avec un autre produit de confiance.
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.
Class FTP	**Trusted path/channels**
Inter-TSF trusted channel	
FTP_ITC.1	*Inter-TSF trusted channel* Le produit doit offrir un canal de communication de confiance entre lui-même et un autre produit TI de confiance.

Annexe 5. Niveaux d'assurance prédéfinis IS 15408 ou CC

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 6. Références documentaires du produit évalué

[322P-B14]	Rapport de certification Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, a27 and b14 Référence BSI-DSZ-CC-0223-2003 Août 2003 Bundesamt für Sicherheit in der Informationstechnik
[ACM]	Configuration Management Plan Référence MRD11SCM023011 Version1.1 Schlumberger Systèmes
[ADM]	Administrator Manual Référence MRD11GUI023007 Version 1.4 Schlumberger Systèmes
[Audit]	Classes ALC ACM ADO evaluation report Version 2.0 Juillet 2003 Serma Technologies
[DEL]	Delivery and Operation Reference MRD11DEL023012 Version 1.2 Schlumberger Systèmes
[EC 1360/2002]	Règlement numéro 1360/2002 de la Commision des Communautés Européennes du 13 juin 2002 et publié le 5 août 2002, concernant l'appareil de contrôle dans le domaine des transports par route
[EC/A1B]	Annexe 1B du règlement 1360/2002 Exigences applicables à la construction, aux essais, à l'installation et à l'inspection
[HLD]	High Level Design Référence MRD11HLD023014 Version 1.1 Schlumberger Systèmes
[IGS]	Les guides pour l'installation, la génération et l'initialisation sont : ▪ Pre-personnalization procedure Référence MRD11IGS023013 Version 1.3 Schlumberger Systèmes ▪ Initialization procedure for Cyberflex Palmera

	Référence MITPRO023022 Version 1.0 Schlumberger Systèmes
[JIL-Comp]	Les guides pour la composition sont : ▪ ETR-lite for composition version 1.0 mars 2002 Joint Interpretation Library ▪ ETR-lite for composition : Annex A, Composite smartcard evaluation : Recommended best practice version 1.2 mars 2002 Joint Interpretation Library
[JIL-Tacho]	Security Evaluation and Certification of Digital Tachographs Version 1.12 Joint Interpretation Library
[LGC]	Configuration List Référence MRD11LIS0330071 Version 1.0 Schlumberger Systèmes
[LLD]	Low Level Design Référence MRD11LLD023015 Version 1.1 Schlumberger Systèmes
[PP/9806]	Smart Card Integrated Circuit Protection Profile Version 2.0 Septembre 1998
[PP/9911]	Smart Card Integrated Circuit with Embedded software Protection Profile Version 2.0 Juin 1999
[RTE]	Evaluation Technical Report Version Juillet 2003 Serma Technologies
[SSVG]	Profil de protection «Smartcard Integrated Circuit Protection Profile v2.0» Référence BSI-PP-0002 Bundesamt für Sicherheit in der Informationstechnik
[ST]	Security Target Référence MRD11STT023001 Version 1.5

	Schlumberger Systèmes
[USR]	User Manual Référence MRD11GUI023008 Version 1.3 Schlumberger Systèmes

Annexe 7. 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.	
Décret 2001-272 du 30 mars 2001- Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.	
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, august 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[IS 15408]	Norme IS/IEC 15408 :1999, comportant 3 documents : ▪ IS 15408–1: (Part 1) Introduction and general model ; ▪ IS 15408–2: (Part 2) Security functional requirements ; ▪ IS 15408–3: (Part 3) Security assurance requirements ;
[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.
[MQ]	Manuel qualité du centre de certification Référence SGDN/DCSSI/SDR/MQ.01 Version 1.0 SGDN/DCSSI
[CER/P/01]	Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information Référence CER/P/01.1 Version 1 SGDN/DCSSI

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
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr