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 2005/01

# ACTIA L2000 Digital Tachograph – SMARTACH Famille Standard

(références 921435 Indice B, 921439 Indice B et 921463 Indice B)

*Paris, le 18 janvier 2005.*

*Le Directeur central de la sécurité des systèmes d'information*

*Henri Serres*
[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 le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

# Table des matières

# 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 publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

## Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats 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 suivante :


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 l'Union 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. (article 9 du décret 2002-535)

Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle s'applique

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

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

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. Le produit évalué

## 1.1. Contexte

Les véhicules (transport par route) mis en circulation pour la première fois après le 5 août 2004 devront être équipés d'un appareil de contrôle conforme aux prescriptions de l'annexe 1B du règlement (CE) n° 1360/2002[1] [CE 1360/2002]. Ces appareils, communément désignés par l'appellation « chrono-tachygraphes numériques » remplaceront les « chrono-tachygraphes analogiques » actuels.

Ces appareils de contrôle sont constitués de deux éléments : une unité embarquée sur le véhicule et un capteur de mouvement. Ce dernier est vissé puis scellé avec la boîte de vitesses. La fonction de ces appareils est d'enregistrer le temps de conduite, les arrêts, les temps de repos ainsi que les temps consacrés aux autres travaux. Une carte à microprocesseur est nécessaire à leur fonctionnement. Quatre types de cartes sont disponibles : les cartes des conducteurs, les cartes d'atelier, les cartes d'entreprise et les cartes de contrôle.

**Unité embarquée sur le véhicule L2000**

**Capteur de mouvement IS2000**

Ce rapport de certification ne porte que sur l'unité embarquée sur le véhicule.

Ce rapport de certification fait suite au rapport de certification [2004/16] portant sur une version précédente du même produit.

## 1.2. Identification du produit

Le produit évalué est l'unité embarquée sur le véhicule « ACTIA L2000 Digital Tachograph – SMARTACH Famille Standard » développée par ACTIA. Ce rapport de certification porte sur trois versions différentes de ce produit dont les références sont : 921435 Indice B, 921439 Indice B et 921463 Indice B.

## 1.3. Développeur

**ACTIA**
25 chemin de Pouvourville
B.P. 4215
31432 TOULOUSE CEDEX 04 (France)

[1] Ce règlement modifie le règlement (CEE) n° 2135/98 du Conseil du 24 septembre 1998.

## 1.4. Description du produit évalué

Le produit véhicule « ACTIA L2000 Digital Tachograph » est constitué :

- d'un processeur, d'une mémoire et d'une horloge,
- de deux lecteurs de cartes à puce,
- d'une imprimante,
- d'un écran,
- de connecteurs.

Le produit véhicule « ACTIA L2000 Digital Tachograph » est destiné à être installé dans les véhicules de transport par route. Il permet d'enregistrer, de stocker, d'imprimer et d'exporter les données relatives aux activités du conducteur.

### *1.4.1. Architecture*

Le produit évalué peut être schématisé de la manière suivante :

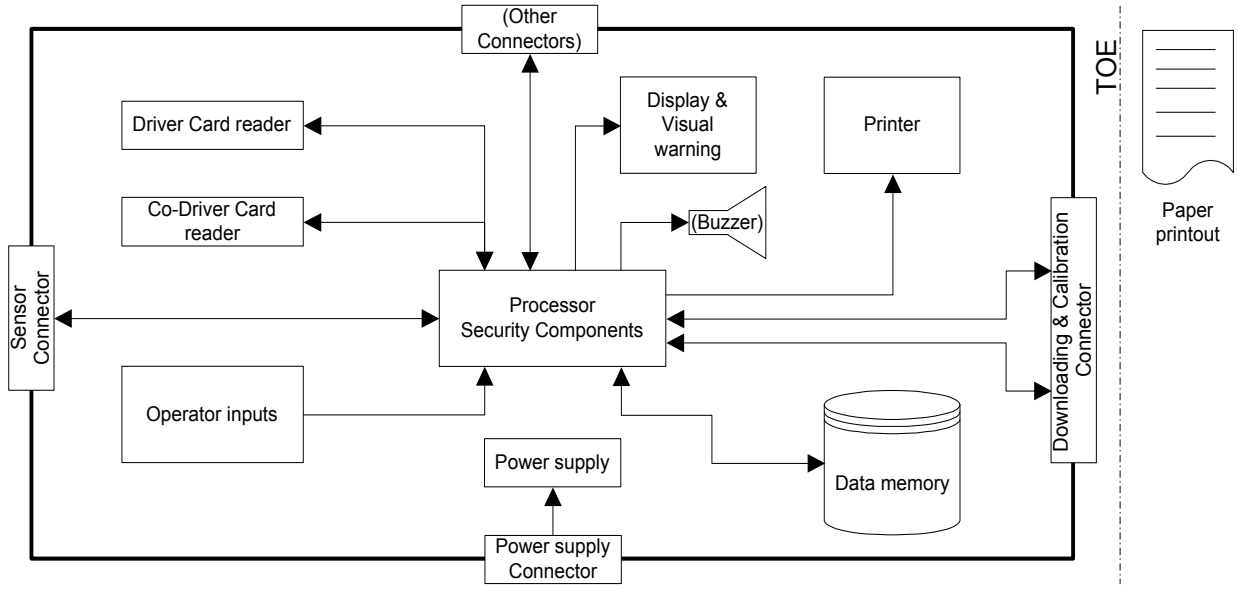


**Figure 1 - Architecture du produit évalué**

L'unité embarquée sur le véhicule est connectée au capteur de mouvement avec lequel il échange les données relatives au mouvement du véhicule.

Les utilisateurs s'identifient à l'aide d'une carte à puce tachygraphique. L'accès aux données et fonctionnalités du L2000 dépend des droits de chaque type d'utilisateur.

Le produit véhicule « ACTIA L2000 Digital Tachograph » enregistre et stocke les données relatives aux activités du conducteur dans sa mémoire et dans la carte à puce. Il exporte les données de l'utilisateur vers l'écran, l'imprimante et des dispositifs externes.

### *1.4.2. Cycle de vie*

Le cycle de vie du produit est détaillé dans la figure 2.

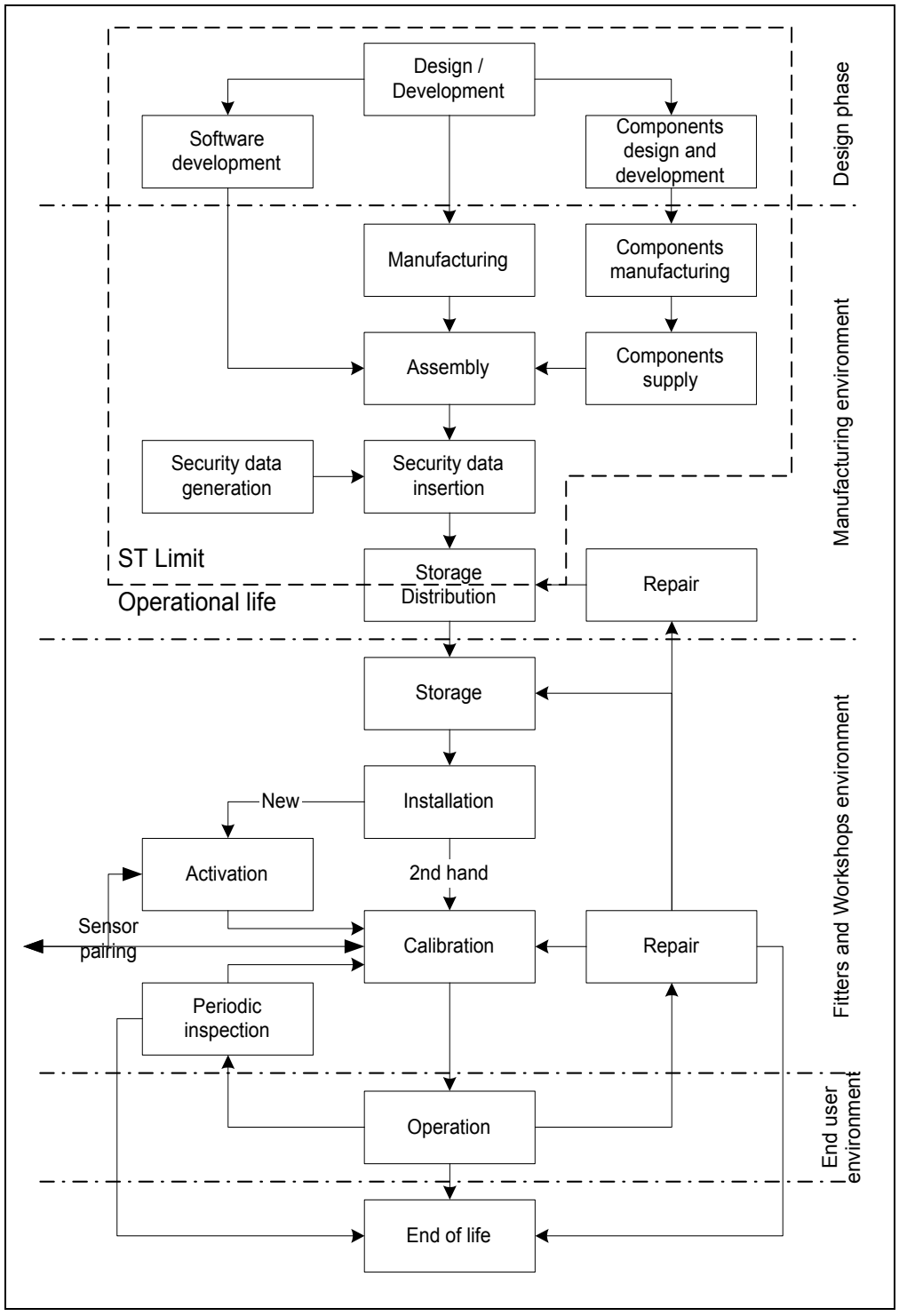


**Figure 2 - Cycle de vie du produit évalué**

Le produit évalué est le produit à la sortie de sa fabrication (fin de la phase de « manufacturing environment »). Les phases d'installation et d'opération sont considérées comme des phases d'utilisation.

La conception du produit, ainsi que le développement de l'application logicielle s'effectuent dans les locaux d'ACTIA.

Les opérateurs dans les ateliers et les conducteurs des véhicules ont été considérés, pour les besoins de l'évaluation, comme des utilisateurs. A ce titre, il n'y a pas d'administration du produit évalué.

# 2. L'évaluation

## 2.1. Commanditaire

**ACTIA**
25 chemin de Pouvourville
B.P. 4215
31432 TOULOUSE CEDEX 04
France

## 2.2. Référentiels d'évaluation

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

## 2.3. Centre d'évaluation

**CEACI (TES – CNES)**

18 Av Edouard BELIN
31 401 Toulouse Cedex 9
France

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : ceaci@cnes.fr

## 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 satisfont aux exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].

L'évaluation s'est déroulée de mai à décembre 2004.

L'évaluation des différents critères et les tests se sont déroulés sur la version 921435 indice B du produit en se fondant sur les résultats de l'évaluation ayant fait l'objet du rapport de certification 2004/16. En outre, le développeur a mené les analyses d'impact suivantes :

- analyse d'impact des évolutions de la version 921435 Indice B vers la version 921439 Indice B ;
- analyse d'impact des évolutions de la version 921439 Indice B vers la version 921463 Indice B.

L' évaluateur a confirmé que les modifications apportées n'ont pas d'impact sur la sécurité.

### *2.5.1. L'environnement de développement*

Le produit est développé sur les sites suivants :

- **ACTIA**
  25 chemin de Pouvourville
  B.P. 4215
  31432 TOULOUSE CEDEX 04
  France
- **CIPI**
  2 rue des Entrepeneurs
  Z.I. Charguia II
  Ariana Aéroport
  2035 TUNIS-CARTHAGE
  Tunisie

Les mesures de sécurité permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.
Un système de gestion de configuration est utilisé conformément au plan de gestion de configuration défini par le développeur du produit. La liste de configuration [LGC] identifie les éléments gérés par ce système. Les procédures de génération permettent par ailleurs de s'assurer que les bons éléments de configuration sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures de développement et de gestion de configuration a été effectuée par une visite du site de CIPI (cf annexe A).

### *2.5.2. La conception du produit*

La classe d'assurance ADV définit les exigences de raffinement des fonctions de sécurité du produit depuis les spécifications globales présentes dans la cible de sécurité [ST] jusqu'à l'implémentation de ces fonctions.

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit :

- spécifications fonctionnelles (FSP),
- conception de haut-niveau (HLD),
- conception de bas-niveau (LLD),
- implémentation des fonctions de sécurité (IMP).

### *2.5.3. La documentation d'exploitation*

Les opérateurs dans les ateliers et les conducteurs des véhicules ont été considérés, pour les besoins de l'évaluation, comme des utilisateurs. A ce titre, il n'y a pas d'administration du produit évalué.

Les guides livrés à ces utilisateurs [USR] ont été fournis pour évaluation.

### *2.5.4. Les 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, telles qu'elles sont décrites dans la conception de haut niveau [HLD], sont couvertes par les tests du développeur.
Les tests ont été réalisés sur la version 921435 indice B.

### *2.5.5. L'analyse de vulnérabilité*

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 prises en compte dans la conception du produit.
L'évaluateur a également réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré.
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 des trois versions du produit « ACTIA L2000 Digital Tachograph – SMARTACH Famille Standard ».

## 3.2. Niveau d'évaluation

Les trois versions du produit « ACTIA L2000 Digital Tachograph – SMARTACH Famille Standard » ont été évaluées selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **E3hAP** [JIL-Tacho].

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_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 |
| **Class AGD** | **Guidance** | |
| AGD_ADM.1 | Administrator guidance | Réussite |
| AGD_USR.1 | User guidance | Réussite |
| **Class ALC** | **Life cycle support** | |
| ALC_DVS.1 | Identification of security measures | 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.2 | Validation of analysis | Réussite |
| AVA_SOF.1 | Strength of TOE security function evaluation | Réussite |
| AVA_VLA.4 | Highly resistant | Réussite |

**Tableau 1 - Composants et verdicts associés**

## 3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** suivantes. Les opérations sur ces exigences sont décrites dans la cible de sécurité [ST].

- Audit data generation (FAU_GEN.1)
- Audit review (FAU_SAR.1)
- Guarantees of audit data availability (FAU_STG.2)
- Cryptographic key generation (FCS_CKM.1)
- Cryptographic key distribution (FCS_CKM.2)
- Cryptographic key access (FCS_CKM.3)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)
- Security attribute based access control (FDP_ACF.1)
- Basic data authentication (FDP_DAU.1)
- Export of user data with security attributes (FDP_ETC.2)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Import of user data with security attributes (FDP_ITC.2)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring (FDP_SDI.1)
- Data exchange integrity (FDP_UIT.1)
- Authentication failure handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- User authentication before any action (FIA_UAU.2)
- Unforgeable authentication (FIA_UAU.3)
- Re-authenticating (FIA_UAU.6)
- User identification before any action (FIA_UID.2)

- Abstract machine testing (FPT_AMT.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Passive detection of physical attack (FPT_PHP.1)
- TSF domain separation (FPT_SEP.1)
- Reliable time stamps (FPT_STM.1)
- TSF testing (FPT_TST.1)
- Limited priority of service (FRU_PRS.1)
- Inter-TSF trusted channel (FTP_ITC.1)

## 3.4. Résistance des fonctions

Seules les fonctions d'authentification ont fait l'objet d'une estimation du niveau de résistance. Le niveau de résistance des fonctions de sécurité est jugé **élevé** (**SOF-High**).

## 3.5. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI suivant l'instruction [CRY/I/01].

## 3.6. Conformité à l'annexe 1B du règlement (CE) n° 1360/2002

Une analyse de correspondance réalisée par l'évaluateur a permis de s'assurer de la conformité de la cible de sécurité ACTIA avec la cible de sécurité générique sur l'unité embarquée sur le véhicule de l'appendice 10 de l'annexe 1B du règlement (CE) n° 1360/2002 [CE 1360/2002]. En termes d'assurance, le document [JIL-Tacho] assure la correspondance entre les niveaux ITSEC E3 fort et CC E3hAP.

## 3.7. Reconnaissance européenne (SOG-IS)

Ce certificat a été émis dans les conditions de l'accord du SOG-IS [SOG-IS].

## 3.8. Reconnaissance internationale (CC RA)

Ce certificat a été émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, les augmentations suivantes n'entrent pas dans le cadre de l'accord : ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 et AVA_VLA.4.

## 3.9. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.10) ainsi que les recommandations se trouvant dans les guides utilisateur [USR].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

## 3.10. Objectifs de sécurité sur l'environnement

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

- les utilisateurs du produit doivent être informés de leur responsabilité. Les opérateurs dans les ateliers doivent être particulièrement informés de leur responsabilité relative à l'activation du L2000 après son installation ;
- le L2000 doit être activé par les opérateurs d'atelier après son installation, avant que le véhicule ne quitte les locaux où a lieu l'installation ;
- les cartes tachygraphiques doivent être livrées par les autorités des États membres seulement aux personnes autorisées ;
- la livraison des cartes doit être suivie (listes blanches, listes noires) et les listes doivent être utilisées durant les audits de sécurité ;
- un conducteur doit posséder, à un moment donné, seulement une carte de conducteur valide ;
- les conducteurs doivent suivre les règles et agir de manière responsable (c'est-à-dire, utiliser leur carte de conducteur, sélectionner correctement leur activité pour celles qui sont manuellement sélectables…) ;
- des contrôles doivent être réalisés régulièrement et aléatoirement, et doivent inclure des audits de sécurité aussi bien que des inspections visuelles de l'équipement* ;
- des inspections périodiques des équipements mis en place dans les véhicules doivent être réalisées après chaque appariement de l'équipement, ou après toute altération du coefficient caractéristique du véhicule ou de la circonférence effective des pneus, ou dès que le temps UTC est erroné de plus de 20 minutes, ou lorsque le VRN a changé, et au moins une fois tous les deux ans ;
- les États membres doivent approuver, contrôler régulièrement et certifier les opérateurs et les ateliers autorisés à mener les installations, les vérifications, les inspections et les réparations.

* Les inspections visuelles de l'équipement doivent permettre de s'assurer de l'intégrité physique du boîtier, en contrôlant les étiquettes de scellement.

## 3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que les trois versions du produit « ACTIA L2000 Digital Tachograph – SMARTACH Famille Standard » identifiées au paragraphe 1.1 et décrit au paragraphe 1.4 du présent rapport **sont conformes** 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, ce rapport de certification atteste que ces trois versions satisfont les exigences relatives à l'unité embarquée sur le véhicule définies à l'appendice 10 de l'annexe 1B du règlement (CE) n° 1360/2002 [CE 1360/2002]. Le certificat de sécurité est délivré conformément aux dispositions de cet appendice.

# Visite du site CIPI

Le site de développement de CIPI situé à Tunis a fait l'objet, dans le cadre de l'évaluation des produits ACTIA L2000 Digital Tachograph – SMARTACH Famille Standard (références 921435 Indice B, 921439 Indice B et 921463 Indice B), 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) ;
- la livraison : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.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. Le rapport de visite se trouve sous la référence [Visite].

# Références documentaires du produit évalué

| | |
|---|---|
| [CE 1360/2002] | Règlement (CE) n° 1360/2002 de la Commission du 13 juin 2002 portant septième adaptation au progrès technique du règlement (CEE) n° 3821/85 du Conseil concernant l'appareil de contrôle dans le domaine des transports par route. |
| [2004/16] | Rapport de certification "ACTIA L2000 Digital Tachograph P104194 – 100 Indice 7", référence 2004/16. |
| [RTE] | Rapport technique de l'évaluation<br>VIC_RTE version 3.0L du 05/01/05<br>CEACI |
| [ST] | Security Target – L2000<br>P204070 indice L du 08.12.2004<br>ACTIA |
| [ST Publique] | Security Target – L2000<br>P204070 indice L (public) du 08.12.2004<br>ACTIA |
| [USR] | 1. Notice Utilisateur L2000 Conducteur – P205549 – 07.05.2003<br>2. Notice Utilisateur L2000 ateliers – P205750 indice B – 16.09.2003<br>3. Notice Utilisateur L2000 Entreprises – P205552 – 16.05.2003<br>4. Notice Utilisateur L2000 Contrôleurs – P205551 indice A – 19.09.2003 |
| [Visite] | Rapport de visite<br>VIC_RDV_CIP version 1.0<br>CEACI |

# 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. |
| [CRY/I/01] | Instruction CRY/I/01 Analyse des mécanismes cryptographiques, DCSSI. |
| [CC] | Critères Communs pour l'évaluation de la sécurité des technologies de l'information:<br>• Part 1: Introduction and general model, January 2004, version 2.2 ;<br>• Part 2: Security functional requirements, January 2004, version 2.2 ;<br>• Part 3: Security assurance requirements, January 2004, version 2.2. |
| [CEM] | Méthodologie d'évaluation de la sécurité des technologies de l'information: Evaluation Methodology, January 2004, version 2.2. |
| [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. |
| [JIL-Tacho] | Security Evaluation and Certification of Digital Tachographs<br>Version 1.12<br>Joint Interpretation Library |

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