



PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/12

ACTIA IS2000 SRES (référence 921441 indice A)
ACTIA IS2000 SRES FIAT (référence 921492 indice A)

Paris, le 26 mai 2005.

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

Henri Serres
[Original signé]



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

Table des matières

1. LE PRODUIT EVALUE.....	6
1.1. CONTEXTE	6
1.2. IDENTIFICATION DU PRODUIT.....	6
1.3. DEVELOPPEUR.....	7
1.4. DESCRIPTION DU PRODUIT EVALUE	7
1.4.1. <i>Architecture</i>	7
1.4.2. <i>Cycle de vie</i>	8
2. L’EVALUATION	9
2.1. COMMANDITAIRE.....	9
2.2. REFERENTIELS D’EVALUATION	9
2.3. CENTRE D’EVALUATION	9
2.4. EVALUATION DE LA CIBLE DE SECURITE.....	9
2.5. EVALUATION DU PRODUIT	9
2.5.1. <i>L’environnement de développement</i>	9
2.5.2. <i>La conception du produit</i>	10
2.5.3. <i>La documentation d’exploitation</i>	10
2.5.4. <i>Les tests fonctionnels</i>	10
2.5.5. <i>L’analyse de vulnérabilité</i>	10
3. CONCLUSIONS DE L’EVALUATION.....	12
3.1. RAPPORT TECHNIQUE D’EVALUATION	12
3.2. NIVEAU D’EVALUATION	12
3.3. EXIGENCES FONCTIONNELLES	13
3.4. RESISTANCE DES FONCTIONS	14
3.5. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES	14
3.6. CONFORMITE A L’ANNEXE 1B DU REGLEMENT (CE) N° 1360/2002.....	14
3.7. RECONNAISSANCE EUROPEENNE (SOG-IS).....	14
3.8. RECONNAISSANCE INTERNATIONALE (CC RA).....	14
3.9. RESTRICTIONS D’USAGE	14
3.10. OBJECTIFS DE SECURITE SUR L’ENVIRONNEMENT	14
3.11. SYNTHESE DES RESULTATS	15
REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	16
REFERENCES LIEES A LA CERTIFICATION	17

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'accord¹, 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 signataires², 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

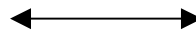
1.1. Contexte

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° 1360/2002¹ [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 SRES**

Ce rapport de certification ne porte que sur le capteur de mouvement.

Ce rapport de certification fait suite au rapport de certification [2005/02] portant sur une version précédente du même produit.

1.2. Identification du produit

Le produit évalué est le capteur « ACTIA IS2000 SMARTACH SRES » développé par ACTIA. Ce rapport de certification porte sur 2 versions différentes de ce produit dont les références sont :

- ACTIA IS2000 SRES : 921441 indice A ;
- ACTIA IS2000 SRES FIAT: 921492 indice A.

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

1.3. Développeur

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

1.4. Description du produit évalué

Le produit IS2000 est constitué:

- d'une cellule de détection, située dans la partie du produit plongeant dans la boîte de vitesses,
- de composants électroniques situés sur une carte électronique.

1.4.1. Architecture

Le produit évalué peut être schématisé de la manière suivante :

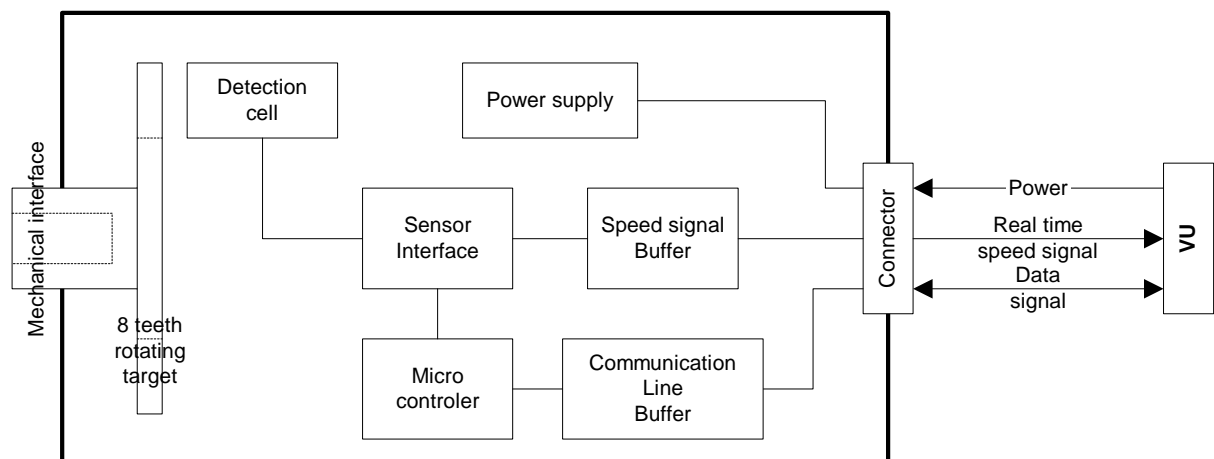


Figure 1 - Architecture du produit évalué

Les fonctionnalités offertes par le produit IS2000 sont les suivantes :

- détection et transmission des impulsions à l'unité embarquée,
- appariement avec l'unité embarquée,
- comptage des impulsions transmises,
- envoi de données sur demande de l'unité embarquée,
- autotests,
- gestion de l'alimentation.

1.4.2. Cycle de vie

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

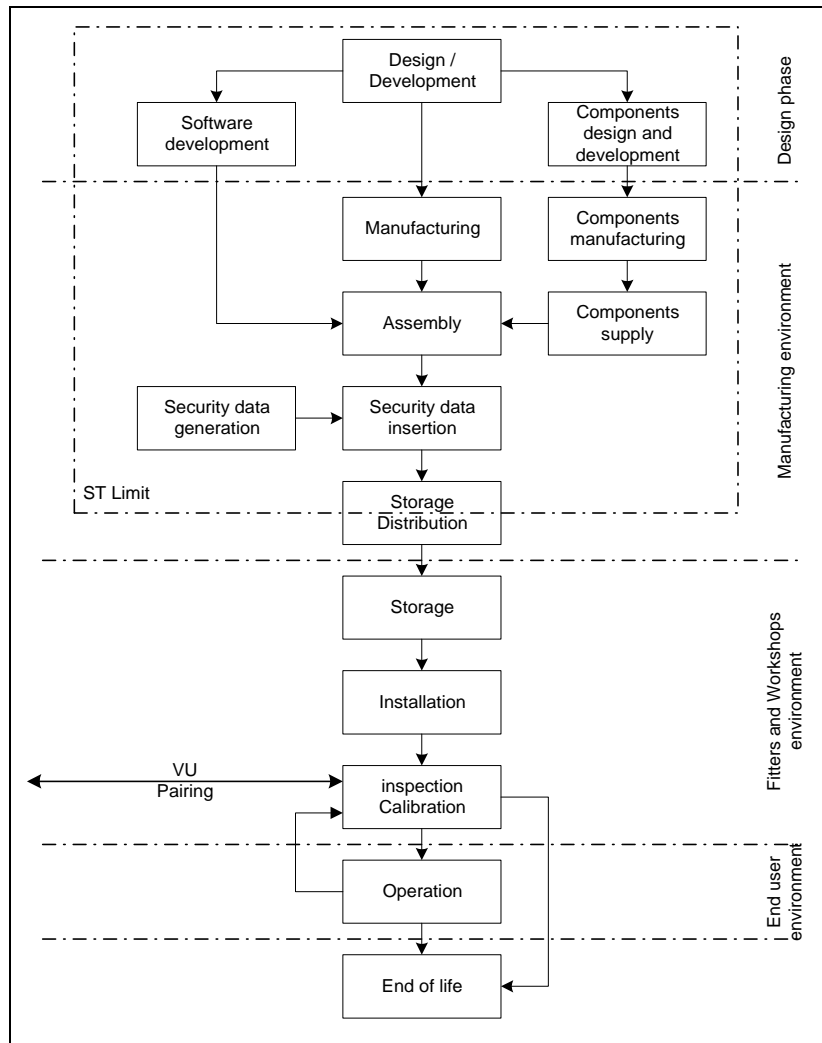


Figure 2 - Cycle de vie du produit évalué

Le produit évalué est le produit à la sortie de sa fabrication. Les phases d'installation et d'opération sont considérées comme des phases d'utilisation.

La conception du produit, le développement de l'application logicielle, l'assemblage des composants, le sertissage, l'industrialisation ainsi que la personnalisation (insertion des éléments de sécurité) sont effectuées par ACTIA.

Il n'y a pas d'administration du produit. Les opérateurs dans les ateliers sont seuls amenés à avoir une interaction (installation, inspection, calibrage) avec le capteur. Ils ont été considérés, pour les besoins de l'évaluation, comme des utilisateurs. Les conducteurs des véhicules n'ont accès à aucune fonctionnalité du capteur.

2. L'évaluation

2.1. Commanditaire

ACTIA
25 chemin de Pouvoirville
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 d'avril 2004 à avril 2005.

Les résultats de l'évaluation des deux versions faisant l'objet de ce rapport de certification sont fondés sur les résultats de l'évaluation des versions ayant fait l'objet du rapport de certification 2005/02.

2.5.1. L'environnement de développement

Le produit est développé sur les sites suivants :

ACTIA
25 chemin de Pouvoirville
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 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.

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, sont couvertes par les tests du développeur.

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 2 versions du produit « ACTIA IS2000 SMARTACH SRES ».

3.2. Niveau d'évaluation

Les 2 versions du produit « ACTIA IS2000 SMARTACH SRES » 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)
- 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)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Stored data integrity monitoring (FDP_SDI.1)
- Data exchange integrity (FDP_UIT.1)
- Authentication failure handling (FIA_AFL.1)
- User authentication before any action (FIA_UAU.2)
- Unforgeable authentication (FIA_UAU.3)
- 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 testing (FPT_TST.1)
- Inter-TSF trusted channel (FTP_ITC.1)

3.4. Résistance des fonctions

Le produit ne contient pas de fonction probabilistique ou permutacionnelle qui ne soit pas de nature cryptographique.

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 le capteur de mouvement 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 la qualité du scellement de l'interface mécanique.
- 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 assemblés aux véhicules doivent avoir lieu au moins une fois tous les deux ans.
- les Etats membres doivent approuver, contrôler régulièrement et certifier les opérateurs et les ateliers autorisés à mener les installations, vérifications, inspections et les réparations.

* Les inspections visuelles de l'équipement doivent permettre de s'assurer de l'intégrité physique du capteur, en particulier de l'intégrité du sertissage. L'intégrité du scellé entre la boîte de vitesses et le capteur de mouvement doit également être vérifié.

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 2 versions du produit « ACTIA IS2000 SMARTACH SRES » identifiées au paragraphe 1.1 et décrites 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 11 versions satisfont les exigences relatives au capteur de mouvement 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.

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.
[2003/13]	Rapport de certification « ACTIA IS2000 Motion Sensor 1426xy », référence 2003/13.
[RTE]	Rapport technique de l'évaluation SRS_ETR version 1.0 du 26/04/05 CEACI
[ST]	SECURITY TARGET IS2000 SMARTACH SRES P206412 indice B du 06/04/05 ACTIA
[ST Publique]	Security Target – L2000 P206412 indice B (public) du 03/05/05 ACTIA
[USR]	SMARTACH SENSOR SRES INSTRUCTIONS D'INSTALLATION P207565 version B du 23/02/2005 ACTIA

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]	<p>Critères Communs pour l'évaluation de la sécurité des technologies de l'information:</p> <ul style="list-style-type: none"> • Part 1: Introduction and general model, January 2004, version 2.2 ; • Part 2: Security functional requirements, January 2004, version 2.2 ; • 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 Version 1.12 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

La reproduction de ce document sans altérations ni coupures est autorisée.