Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2013/69

Dispositif de placement sous surveillance électronique PSE/PSEM/DEPAR

Paris, le 24 janvier 2014

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

[Original signé]
Patrick Pailloux

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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2013/69

Nom du produit

Dispositif de placement sous surveillance électronique PSE/PSEM/DEPAR

Référence/version du produit

Version 10

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 2 augmenté

ALC_DVS.1, ALC_FLR.3, AVA_VAN.3

Développeur

G4S Monitoring Technologies

3 Centurion Court
Meridian Business Park
Leicester LE19 1TP
Royaume Uni

Commanditaire

G4S Monitoring Technologies

3 Centurion Court
Meridian Business Park
Leicester LE19 1TP
Royaume Uni

Centre d'évaluation

Serma Technologies

14 rue Galilée, CS 10055
33615 Pessac Cedex
France

Accords de reconnaissance applicables

CCRA **SOG-IS**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. LE PRODUIT 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Identification du produit 6
1.2.3. Services de sécurité 7
1.2.4. Architecture 7
1.2.5. Cycle de vie 7
1.2.6. Configuration évaluée 8

2. L'EVALUATION 9

2.1. REFERENTIELS D'EVALUATION 9
2.2. TRAVAUX D'EVALUATION 9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 9
2.4. ANALYSE DU GENERATEUR D'ALEAS 9

3. LA CERTIFICATION 10

3.1. CONCLUSION 10
3.2. RESTRICTIONS D'USAGE 10
3.3. RECONNAISSANCE DU CERTIFICAT 10
3.3.1. Reconnaissance européenne (SOG-IS) 10
3.3.2. Reconnaissance internationale critères communs (CCRA) 10

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT [CCV3.1R3] 12

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 13

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 15

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « Dispositif de placement sous surveillance électronique PSE/PSEM/DEPAR**,** Version 10 » développé par G4S Monitoring Technologies.

Le produit évalué est un système de surveillance électronique destiné à vérifier qu'un bracelet électronique reste dans un périmètre assigné. Si le bracelet sort de ce périmètre, le produit signale cet événement à un centre de télésurveillance.

Le périmètre est défini, soit par la distance maximale autour d'une borne fixe dans un mode nommé « placement sous surveillance électronique » (PSE), soit par une zone définie par ses coordonnées géographiques dans un mode nommé « placement sous surveillance électronique mobile » (PSEM).

Le produit comporte également un mode appelé DEPAR (Dispositif Electronique de Protection Anti Rapprochement) dans lequel les dispositifs fixes et mobiles, identiques à ceux utilisés dans les modes PSE et PSEM, sont utilisés pour détecter la présence dans un périmètre défini d'un bracelet électronique donné afin d'en faire le signalement au centre de télésurveillance.

1.2. Description du produit

1.2.1. Introduction

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

La cible ne réclame pas de conformité à un profil de protection.

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit est identifiable par les éléments suivants :

Elément de la TOE	**Version**	
	Hardware	*Firmware*
Bracelet électronique	10-0149-4	3.5.1
Unité de surveillance fixe (GSM)	10-0141-4	10.04.03
Unité de surveillance fixe (ligne terrestre)	10-0154-4	10.04.04
Unité de surveillance mobile (mode PSEM)	10-0138-4	9.4.12
Unité de surveillance mobile (mode DEPAR)	10-0136-4	9.4.12
Station d'accueil	10-0139-4	1.6.7
Porte-clés	10-0143-4	3.5.2
Outil de montage et d'installation	10-0142-4	3.4.1
Outil de diagnostic	38-0098-1	2.1.0.2

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- administration distante depuis le centre de télésurveillance ;
- administration locale par l'intermédiaire de l'outil de diagnostic ;
- audit local à l'aide de l'outil de diagnostic ;
- initialisation à l'aide de l'outil de montage et d'installation ;
- protection des communications en confidentialité et intégrité à l'aide de chiffrement AES128 en mode CBC et CMAC ;
- utilisation d'une source de temps fiable ;
- génération de journaux d'événements ;
- détection de perte d'intégrité sur le bracelet, l'unité de surveillance fixe, l'unité de surveillance mobile et la station d'accueil ;
- détection de perte de signal et de brouillage par l'unité de surveillance (fixe et mobile).

1.2.4. Architecture

Les éléments constitutifs du produit, identifiés dans la liste de configuration [CONF] sont :

1. un bracelet électronique ;
2. une station d'accueil (modes PSEM et DEPAR);
3. une unité de surveillance fixe (mode PSE et PSEM) ;
4. une unité de surveillance mobile (modes PSEM et DEPAR) associée à la station d'accueil ;
5. un porte-clés ;
6. un outil de montage et d'installation ;
7. un outil de diagnostic ;
8. un centre de télésurveillance ;
9. une application de télésurveillance.

En phase d'initialisation, c'est-à-dire lorsqu'on associe le bracelet à une personne, le porte-clés, l'outil de montage et d'installation et l'outil de diagnostic doivent être à proximité du bracelet et de l'unité de surveillance.

En phase d'utilisation, le bracelet électronique communique avec l'unité de surveillance fixe ou mobile. Cette unité relaye les informations au centre de télésurveillance.

Les éléments 1 à 7 sont inclus dans le périmètre de l'évaluation. Le centre de surveillance et l'application en sont exclus.

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

Phase	**Lieu**
Développement	G4S Monitoring Technologies
Fabrication	Assel
Livraison	Datacet
Initialisation	Chez l'utilisateur
Utilisation	Dans le périmètre assigné

Le produit a été développé sur les sites suivants :

G4S Monitoring Technologies
3 Centurion Court, Meridian Business Park
Leicester, LE19 1TP
Royaume-Uni

G4S Monitoring Technologies
1 Tiber Way, Meridian Business Park
Leicester LE19 1QP
Royaume-Uni

Assel
ul. Batalionow Chlopskich I
83-000 Pruzcz Gdanski
Pologne

Datacet
150 Grande Rue
54180 Heillecourt
France

1.2.6. Configuration évaluée

Le certificat porte sur les configurations matérielles et logicielles identifiées au paragraphe 1.2.2. L'application du centre de télésurveillance ne fait pas partie de la TOE.

La cible d'évaluation a été testée dans les configurations « initialisation » et « utilisation » pour les modes PSE, PSEM et DEPAR.

2. L'évaluation

2.1. Référentiels d'évaluation

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

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 23 septembre 2013, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément aux référentiels techniques de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Toutes les règles contenues dans [REF] sont satisfaites ; seule une des recommandations n'est pas suivie (par un unique mécanisme).

Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était en dehors du périmètre de l'évaluation et n'a pas été analysé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Dispositif de placement sous surveillance électronique PSE/PSEM/DEPAR, Version 10 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 2 augmenté des composants ALC_DVS.1, ALC_FLR.3 et AVA_VAN.3.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1 du présent rapport de certification.
L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit [CCv3.1R3]

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 2+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**2**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**1**	Architectural design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**2**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**2**	Implementation representation CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**		
	ALC_TAT				**1**	**2**	**3**	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**1**	Analysis of coverage
	ATE_DPT									
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible *de sécurité de référence pour l'évaluation :* - *Security target Common Criteria: Electronic tagging (PSE) and Mobile electronic tagging (PSEM) devices and Victim Protection (DEPAR)*, version 1.4, réf. : ST_PSE_PSEM_v1.4, G4S Monitoring Technologies ; Pour les besoins de publication, la cible de securite suivante a été fournie dans le cadre de cette évaluation : - *Security target Lite Common Criteria : Electronic tagging (PSE) and Mobile electronic tagging (PSEM) devices and Victim Protection DEPAR*, version 3.0, réf. : ST_LITE_PSE_PSEM_DEPAR_v3.0, G4S Monitoring Technologies.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report YELLOWFOOT Project*, version 1.0, réf. : YELLOWFOOT_ETR_v1.0, SERMA Technologies.
[EXP -CRY]	*Evaluation Technical Report YELLOWFOOT Project, ANNEX G*, version 1.0, réf. : YELLOWFOOT_ETR_v1.0, SERMA Technologies.
[ANA-CRY]	Cryptographic Mechanisms Evaluation Report YELLOWFOOT Project, version 1.1, réf. : YELLOWFOOT_Cryptography_v1.1, SERMA Technologies.
[CONF]	Liste de configuration du produit : - ALC: LIFECYCLE SUPPORT (CMS.2: CONFIGURATION LIST), version 0.23, réf. : ALC_CMS2_Configuration_V23, G4S Monitoring Technologies.

[GUIDES]	Guide d'installation du produit : - Installation Bracelet (Unité Fixe GSM) / Dépannage (Unité Fixe GSM), réf. : 94-0032-05, G4S Monitoring Technologies, - Installation Bracelet (Unité Fixe Filaire) / Dépannage (Unité Fixe Filaire), réf. : 94-0042-05, G4S Monitoring Technologies, - Installation d'une unité mobile GPS, réf. : 94-0237-02, G4S Monitoring Technologies. Guide d'administration du produit : - Guide en cas de violation de l'Unité Fixe / Guide en cas de violation du Bracelet, 94-0034-04, G4S Monitoring Technologies, - Guide en cas de violation du TRAK ou de l'unité relais / Guide en cas de violation du Bracelet, réf. : 94-0055-05, G4S Monitoring Technologies, - Guide d'utilisation EMMO, réf. : 94-0104-04, G4S Monitoring Technologies, - Guide rapide sur EMMO (MU/Bracelet), réf. : 94-0035-05, G4S Monitoring Technologies, - Guide rapide sur EMMO (Unité Relais/TRAK), réf. : 94-0266-01, G4S Monitoring Technologies. Guide d'utilisation du produit : - Placement sous surveillance électronique: guide de la personne placée, réf. : 94-0105-03, G4S Monitoring Technologies. - Placement sous surveillance électronique mobile: guide de la personne placée, réf. : 94-0243-02, G4S Monitoring Technologies, - DEPAR: guide de la personne protégée, réf. : 94-0214-4-A-fr-FR, G4S Monitoring Technologies.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), voir www.ssi.gouv.fr.