



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-2018/11

Smart Tachograph G2 on MultiApp V4.0.1 (version 2.0.1.G)

Paris, le 03/04/2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]



Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

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

certification@ssi.gouv.fr

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



Référence du rapport de certification

ANSSI-CC-2018/11

Nom du produit

Smart Tachograph G2 on MultiApp V4.0.1

Référence/version du produit

version 2.0.1.G

Conformité à un profil de protection

[PP-0091] Digital Tachograph – Tachograph Card (TC PP), Version 1.0

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté
ALC_DVS.2, ATE_DPT.2 et AVA_VAN.5

Développeurs

Gemalto
6, rue de la Verrerie,
92197 Meudon cedex, France

Infineon Technologies AG
AIM CC SM PS – Am Campeon 1-12,
85579 Neubiberg, Allemagne

Commanditaire

Gemalto
6, rue de la Verrerie,
92197 Meudon cedex, France

Centre d'évaluation

Serma Safety & Security
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables



SOG-IS



Ce certificat est reconnu au niveau EAL2.

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. <i>Introduction</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	6
1.2.4. <i>Identification du produit</i>	6
1.2.5. <i>Cycle de vie</i>	7
1.2.6. <i>Configuration évaluée</i>	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	11
3.1. CONCLUSION	11
3.2. RESTRICTIONS D’USAGE	11
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	11
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	13
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	14
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	15

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Smart Tachograph G2 on MultiApp V4.0.1, version 2.0.1.G » développé par GEMALTO et *INFINEON TECHNOLOGIES AG*.

Ce produit est destiné à être utilisé par les tachygraphes électroniques (équipements d'enregistrement des activités d'un véhicule de transport routier) ou par des ordinateurs personnels (pour réaliser les opérations de contrôle de l'activité du véhicule).

Les principales fonctions de cette carte sont :

- le stockage des identifiants de la carte et de son porteur en vue de l'identification du porteur de la carte afin de fournir les droits d'accès appropriés aux fonctions et aux données, et d'assurer l'imputation des activités ;
- le stockage des informations relatives à l'activité du porteur de la carte.

1.2. Description du produit

1.2.1. Introduction

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

Cette cible de sécurité est conforme au profil de protection [PP-0091].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'authentification mutuelle Gen1 ou Gen2 ;
- le stockage de l'identification de la carte et des données du porteur ;
- le stockage des données d'activité ;
- la vérification des certificats Gen1 et Gen2 ;
- la génération de signature des données internes à exporter ;
- la vérification en intégrité et en authenticité du *Dedicated Short Range Communication* (DSRC) message ;
- le téléchargement des données utilisateurs ;
- la personnalisation du produit.

1.2.3. Architecture

Le produit est constitué :

- du composant M7892 G12 précédemment certifié (voir [CER-IC]) ;
- d'un système d'exploitation sous forme d'une plateforme en configuration fermée Java Card MultiApp V4.0.1. Cette plateforme est certifiée sous la référence [ANSSI-CC-2017/76] ;
- de l'application Smart Tachograph G2.

1.2.4. Identification du produit

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

La version certifiée du produit est identifiable par les éléments présents dans la réponse que donne le produit suite à la commande *READ BINARY* (voir [GUIDES]).

La réponse attendue correspond aux éléments du tableau ci-après :

Eléments de configuration		Origine
Nom de la TOE	Smart Tachograph G2 on MultiApp V4.0.1	<i>GEMALTO</i>
Référence TOE	Tachograph Gen V2 on MultiApp V4.0.1 Version 2.0.1.G	
Applet Label	TACHOGRAPH G2	
Applet version	2.0.1.G	
Operating System Identifier	12 91	
Operating System release date	70 90	
Operating System release level	04 00	
IC Fabricator	40 90	<i>INFINEON</i>
IC Type	78 97	

L'identification de la plateforme est décrite dans le paragraphe 1.2.4 de [ANSSI-CC-2017/76].

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

	Phase	Acteur	Couvert par
Etape 1	Développement	<i>GEMALTO</i>	ALC
Etape 2	Développement	<i>INFINEON</i>	ALC
Etape 3	Fabrication	<i>INFINEON</i>	ALC
Etape 4	<i>Packaging</i>	<i>GEMALTO</i>	ALC
Etape 5	Pré-Personnalisation	<i>GEMALTO</i>	ALC
Point de livraison TOE			
Etape 6	Personnalisation	Personnalisateur	AGD_PRE
Etape 7	Utilisation opérationnelle	Utilisateur final	AGD_OPE

Le produit a été développé sur les sites suivants :

<i>GEMALTO</i> Meudon 6 Rue de la Verrerie 92190 Meudon, France	<i>GEMALTO</i> Singapore 12 Ayer Rajah Crescent Singapor 139941, Singapour
<i>GEMALTO</i> Gémenos Avenue du Pic de Bretagne 13881 Gémenos, France	<i>GEMALTO</i> La Ciotat Avenue du Jjubier, ZI Athelia IV 13705 La Ciotat, France
<i>ATOS</i> Paris (Aubervilliers / Croissy) 4 rue des Vieilles Vignes 77 183 Croissy-Beaubourg, France	<i>ATOS</i> Bydgoszcz – (ATOS Poland) Biznes Park, ul. Kraszewskiego 1 85-240 Bydgoszcz, Poland
<i>GEMALTO</i> Barcelona Poligono Industrial Llevant CL Llevant 12,	<i>GEMALTO</i> Montgomeryville 101 & 106 Park Drive Montgomeryville, PA 18 936 United States

08150 Parets del Valles, Barcelona, Spain	
<i>GEMALTO</i> Curitiba Rodovia Dep. Leopoldo Jacomel, 13102 83323-410 Pinhais, PR Brazil	<i>GEMALTO</i> Vantaa Myllynkivenkuja 4, Vantaa, Finland, FI-01620
<i>GEMALTO</i> Tczew Ul. Skarszewska 2 33-110 Tczew, Poland	<i>GEMALTO</i> Pont Audemer Z.1. Saint Ulfrant rue de Saint Ulkfrant 27500 Pont Audemer, France

Les sites de développement du composant et de la bibliothèque sont respectivement couverts par le certificat [CER-IC].

1.2.6. Configuration évaluée

Le certificat porte sur le produit identifié au 1.2.4 et configuré comme suit :

- l'application Smart Tachograph G2, version 2.0.1.G » est instanciée et la plateforme est fermée sans possibilité de charger et d'instancier d'autres applications ;
- les recommandations des guides [GUIDES] sont strictement appliquées durant la phase « Personnalisation » du cycle de vie, ainsi que dans la phase de pré-personnalisation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « Infineon Security Controller M7892 Design Steps D11 and G12 with optional RSA2048/4096 v2.03.008, ECv2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware) » au niveau EAL6 augmenté des composants ALC_FLR.1 conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 20 décembre 2016 sous la référence BSI-DSZ-CC-0891-V2-2016, voir [CER_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 9 mars 2018, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « réussite ».

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

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).

Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique. Ce retraitement

a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation. Le générateur atteint le niveau « DRG.4 ».

Les 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.5 visé.

3. La certification

3.1. Conclusion

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

Ce certificat atteste que le produit « Smart Tachograph G2 on MultiApp V4.0.1, version 2.0.1.G » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2, ATE_DPT.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, 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'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. 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 La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires¹, des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR.

Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit		
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant	
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	2	2	Testing: security enforcing modules
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - Tachograph Generation V2 Security Target, référence : D1432172, version 1.2, 15/11/2017, GEMALTO. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Security Target Lite – Tachograph Generation V2, référence : D1432172, version 1.3p, GEMALTO.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Poseidon Project: Evaluation Technical Report, référence : POSEIDON_ETR_v1.2, version 1.2, SERMA SAFETY & SECURITY.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - Build Project [/IDApplets/TachoV20/TachoGen2_on_MAV401/project.pj (1.14)], 12/10/2017, GEMALTO ; - D1436010-LIS-DOC-TACHOV2, référence : D1436010, version 1.5, 12/09/2013, GEMALTO.
[GUIDES]	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none"> - AGD_PRE: PREPARATIVE PROCEDURE TACHOGRAPH GENERATION V2, référence : D1436041, version 1.3, 04/10/2017, GEMALTO. <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - AGD_OPE: OPERATIONAL USER GUIDANCE PROCEDURE TACHOGRAPH GENERATION V2, référence : D1436050, version 1.0, GEMALTO.
[PP-0091]	<p>Digital Tachograph – Tachograph Card (TC PP), version 1.0, 18 May 2017. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0091-2017.</i></p>
[CER-IC]	<p>Infineon Security Controller M7892 Design Steps D11 and G12 with optional RSA2048/4096 v2.03.008, ECv2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware). <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 20 décembre 2016, sous la référence BSI-DSZ-CC-0891-V2-2016.</i></p>
[ANSSI-CC-2017/76]	<p>Plateforme JavaCard MultiApp V4.0.1 - PACE en configuration ouverte masquée sur le composant M7892 G12. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-2017/76 le 18 décembre 2017.</i></p>

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	<p>Common Criteria for Information Technology Security Evaluation :</p> <ul style="list-style-type: none"> - Part 1: Introduction and general model, août 2005, version 2.3, référence CCMB-2005-08-001; - Part 2: Security functional requirements, août 2005, version 2.3, référence CCMB-2005-08-002; - Part 3: Security assurance requirements, août 2005, version 2.3, référence CCMB-2005-08-003. <p>Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.</p>
[CC]	<p>Common Criteria for Information Technology Security Evaluation :</p> <ul style="list-style-type: none"> - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.4, août 2015.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, mai 2000.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.

[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr .
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>).

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.