



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CC-2022/38

**Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h
(version 2.2.1.M)**

Paris, le 16 août 2022

Le Directeur général adjoint de l'Agence
nationale de sécurité des systèmes d'information

Emmanuel NAEGELEN

[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-2022/38	
Nom du produit	Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h	
Référence/version du produit	version 2.2.1.M	
Conformité à un profil de protection	Digital Tachograph – Smart Card (Tachograph Card P) référence BSI-CC-PP-0070, version 1.02, 15 novembre 2011 certifié sous la référence BSI-CC-PP-0070-2011 Digital Tachograph – Tachograph Card (TC PP), version 1.0, 9 May 2017 certifié sous la référence BSI-CC-PP-0091-2017	
Critère d'évaluation et version	Critères Communs version 3.1 révision 5	
Niveau d'évaluation	EAL 4 augmenté ALC_DVS.2, ATE_DPT.2, AVA_VAN.5	
Développeurs	THALES DIS 6 rue de la Verrerie 92190 Meudon, France	INFINEON TECHNOLOGIES AG AIM CC SM PS – Am Campeon 1-12, 85579 Neubiberg, Allemagne
Commanditaire	THALES DIS 6 rue de la Verrerie 92190 Meudon, France	
Centre d'évaluation	CEA - LETI 17 avenue des martyrs, 38054 Grenoble Cedex 9, France	
Accords de reconnaissance applicables	 CCRA	 SOG-IS
Ce certificat est reconnu au niveau EAL2.		

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit.....	6
1.2.1	Introduction	6
1.2.2	Services de sécurité.....	6
1.2.3	Architecture	6
1.2.4	Identification du produit.....	7
1.2.5	Cycle de vie	8
1.2.6	Configuration évaluée	8
2	L'évaluation.....	9
2.1	Référentiels d'évaluation	9
2.2	Travaux d'évaluation	9
2.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	9
2.4	Analyse du générateur d'aléa.....	9
3	La certification	11
3.1	Conclusion.....	11
3.2	Restrictions d'usage	11
3.3	Reconnaissance du certificat.....	11
3.3.1	Reconnaissance européenne (SOG-IS).....	11
3.3.2	Reconnaissance internationale critères communs (CCRA).....	11
ANNEXE A.	Références documentaires du produit évalué	13
ANNEXE B.	Références liées à la certification	15

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h, version 2.2.1.M » développé par THALES DIS.

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 aux profils de protection [PP70] et [PP91].

1.2.2 Services de sécurité

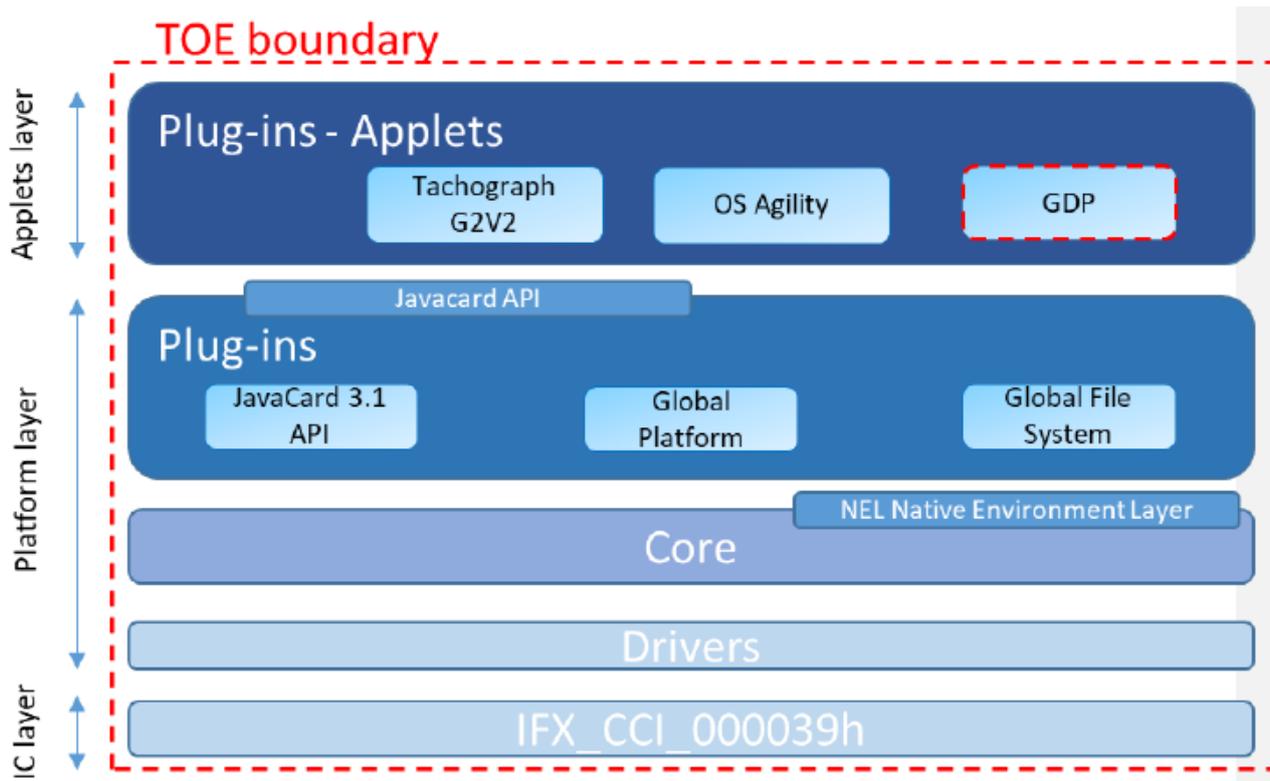
Les principaux services de sécurité fournis par le produit sont :

- 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 principalement constitué :

- du composant IFX_CCI_000039 (SLC37) précédemment certifié (voir [CER_IC]) ;
- d'un système d'exploitation MultiApp V5.0 sous forme d'une plateforme Java Card en configuration fermée ;
- de l'application OS-Agility dédiée au chargement de patch ;
- de l'application Tachograph G2V2.



1.2.4 Identification du produit

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]).

Éléments de configuration		
Applet Label	TACHOGRAPH G2	54 41 43 48 4F 47 52 41 50 48 20 47 32
Applet version	2.2.1.M	32 2E 32 2E 31 2E 4D
IC Fabricator		40 90
IC Type		00 39
Operating System Identifier		19 81
Operating System release date	24/02/21	10 55
Operating System release level	5.0	05 00
THALES Family Name		B0
THALES OS name		85
Mask number		5F
Product name		5E
Flow ID Version,		01
Filter set		00

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

1.2.5 Cycle de vie

Le produit a été développé sur les sites suivants (voir [SITES]) :

Thales Meudon [MDN] 6 Rue de la Verrerie 92190 Meudon France	Thales Singapore [SGP] 12 Ayer Rajah Crescent Singapor 139941 Singapou
Thales Gémenos [GEM] Avenue du Pic de Bretagne 13881 Gémenos France	Thales Tczew [TCZ] Ul. Skarszewska 2 33-110 Tczew Pologne
Thales Vantaa [VAN] Myllynkivenkuja 4 Vantaa Finlande, FI-01620	Thales Curitiba [CUR]] Rodovia Dep. Leopoldo JacomeI 13102 83323-410 Pinhais PR Brésil
La Ciotat [VIG] Thales DIS La Ciotat ZI Athelia IV, Avenue du Jujubier 13705 La Ciotat, France	

1.2.6 Configuration évaluée

Le certificat porte sur les configurations suivantes (sélectionnées au moment de la personnalisation de la carte) :

- Application Tachograph G1 v1.6;
- Application Tachograph G2V1;
- Application Tachograph G2V2

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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 [COMP] 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 « IFX_CCI_000039 (SLC37) », voir [CER_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 potentiel d'attaque visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

2.4 Analyse du générateur d'aléa

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 [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le potentiel d'attaque 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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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 [CCRA].

¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires², 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 :



² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - <i>TACHOGRAPH G1, G2V1, G2V2 ON IFX_CCI_000039H SECURITY TARGET</i>, référence D1551037, révision. 1.4, 12 mai 2022. <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"> - <i>TACHOGRAPH G1, G2V1, G2V2 ON IFX_CCI_000039H SECURITY TARGET – PUBLIC VERSION</i>, référence D1551037, révision Rev. 1.4p, 12 mai 2022.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - « <i>Evaluation Technical Report – POSEIDON</i> », référence LETI.CESTI.POS.FULL.001 version 1.1 du 16 juin 2022.
[ANA_CRY]	<p>« <i>Cotation des mécanismes cryptographiques- POSEIDON</i> », référence LETI.CESTI.POS.RT.007- V1.2 du 2 août 2022.</p>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - <i>ROR29917_ALC_LIS</i>, référence ROR29917_ALC_LIS, version 1.6, 20/05/22 ; - <i>Source code filelisting</i>, référence filelisting_SGP-RND-GP-17, version R007.
[GUIDES]	<ul style="list-style-type: none"> - <i>Tachograph Generation 1 (version 1.6) - Personalization Manual</i>, référence D1564669, version 1.F, 12/05/22 ; - <i>Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h Traceability information</i>, référence D1559331, version G, 12/05/22 ; - <i>Tachograph Generation 2 Version 2 & Tachograph - Generation 2 Version 1 Personalization Manual</i>, référence D1549733, version 1.I, 12/05/22 ; - <i>AGD_OPE document TACHOGRAPH G2V2</i>, référence D1551042, version 1.2, 07/04/22 ; - <i>AGD_PRE document TACHOGRAPH G2V2</i>, référence D1551041, version 1.3, 07/04/22.
[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> - DISGEN20_ALC_GEN_v1.1 ; - DISGEN21_ALC_GEN_v1.0 ; - [MDN] DISGEN21_MDN_STAR_v1.1 ; - [SGP] DISGEN20_SGP_STAR_v1.0 ; - [GEM] DISGEN20_GEM_STAR_v1.0 ; - [VAN] DISGEN21_VAN_STAR_v1.0 ; - [TCZ] DISGEN20_TCZ_STAR_v1.0 ; - [VIG] DISGEN20_VIG_STAR_v1.1 ; - [CUR] DISGEN21_CTB_STAR_v1.1.
[CER_IC]	<p>Produit Infineon IFX_CCI_000039 (SLC37) Certifié par le BSI sous la référence BSI-DSZ-CC-1107-V2-2021 le 7 juillet 2021.</p>
[PP70]	<p><i>Digital Tachograph – Smart Card (Tachograph Card P)</i>, référence BSI-CC-PP-0070, version 1.02, 15 novembre 2011. Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0070-2011.</p>

[PP91]	<i>Digital Tachograph – Tachograph Card (TC PP), version 1.0, 9 May 2017. Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0091-2017.</i>
--------	--

ANNEXE B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 4.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	<i>Common Criteria for Information Technology Security Evaluation:</i> <ul style="list-style-type: none">- <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;- <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;- <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.1, juin 2020.
[COMP] *	<i>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices</i> , version 1.5.1, mai 2018.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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