



**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-2022/36v2-R01

**TachoDrive v4 on ID-One Cosmo X
(Code SAAAAR : 41 63 06)**

Paris, le 14/8/2025 | 18:31 CEST

Vincent Strubel



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.

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 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.cyber.gouv.fr.

TABLE DES MATIERES

1	Résumé	5
2	Le produit.....	7
2.1	Présentation du produit.....	7
2.2	Description du produit.....	7
2.2.1	Introduction	7
2.2.2	Services de sécurité.....	7
2.2.3	Architecture	8
2.2.4	Identification du produit.....	8
2.2.5	Cycle de vie	8
2.2.6	Configuration évaluée	8
3	L'évaluation.....	9
3.1	Référentiels d'évaluation	9
3.2	Travaux d'évaluation	9
3.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	9
4	La certification	10
4.1	Conclusion.....	10
4.2	Restrictions d'usage	10
4.3	Reconnaissance du certificat.....	11
4.3.1	Reconnaissance européenne (SOG-IS).....	11
4.3.2	Reconnaissance internationale critères communs (CCRA).....	11
ANNEXE A.	Références documentaires du produit évalué	12
ANNEXE B.	Références liées à la certification	14

1 Résumé

Référence du rapport de certification	ANSSI-CC-2022/36v2-R01
Nom du produit	TachoDrive v4 on ID-One Cosmo X
Référence/version du produit	Code SAAAAR : 41 63 06
Type de produit	Cartes à puce et dispositifs similaires
Conformité à un profil de protection	<i>Digital Tachograph – Smart Card (Tachograph Card) Protection Profile, version 1.02</i> certifié BSI-CC-PP-0070 le 15 novembre 2011 <i>Digital Tachograph – Tachograph Card (TC PP) Protection Profile, version 1.0</i> certifié BSI-CC-PP-0091 le 9 mai 2017
Critère d'évaluation et version	Critères Communs version 3.1 révision 5
Niveau d'évaluation	EAL4 augmenté ALC_DVS.2, ATE_DPT.2, AVA_VAN.5
Référence du rapport d'évaluation	<i>Evaluation Technical Report (full ETR) – KASHYAPA</i> référence LETI.CESTI.KAS.FULL.001 version 3.2 28 juillet 2025.
Fonctionnalité de sécurité du produit	voir 2.2.2 Services de sécurité
Exigences de configuration du produit	voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation	voir 4.2 Restrictions d'usage
Développeur	IN SMART IDENTITY FRANCE 2 place Samuel de Champlain 92400 Courbevoie, France

Commanditaire	IN SMART IDENTITY FRANCE 2 place Samuel de Champlain 92400 Courbevoie, 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.

2 Le produit

2.1 Présentation du produit

Le produit évalué est « TachoDrive v4 on ID-One Cosmo X, Code SAAAAR : 41 63 06 » développé par IDEMIA devenue aujourd'hui IN SMART IDENTITY FRANCE.

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 la réalisation d'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.

2.2 Description du produit

2.2.1 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 [PP0070] et [PP0091].

2.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont décrits dans la cible de sécurité [ST] au chapitre 3 « *Target of Evaluation Overview* ». Ils comprennent notamment :

- 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.

2.2.3 Architecture

Le produit est constitué de :

- la plateforme ouverte JavaCard « ID-One Cosmo X » embarquée sur un microcontrôleur SLC37 ;
- l'application TachoDrive v4.

Il n'y a aucune autre *known applet* au sens de la note d'application [OPEN].

2.2.4 Identification du produit

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

La procédure d'identification est décrite au chapitre 7 du guide AGD_PRE (voir [GUIDES]). La version certifiée du produit correspond aux valeurs attendues décrites dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Reference* ».

2.2.5 Cycle de vie

Le cycle de vie du produit est décrit au chapitre 4 de la cible de sécurité [ST]. Il présente différentes options selon le moment et le lieu de chargement des composants logiciels du produit.

Il est conforme à celui décrit dans [PP0084]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit : le personnaliseur, le gestionnaire de la carte chargé de l'administration de la carte, et comme utilisateur du produit : l'utilisateur du produit final sur le terrain.

2.2.6 Configuration évaluée

Le certificat porte sur les configurations listées au chapitre 3.1 de la cible de sécurité [ST].

3 L'évaluation

3.1 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 et dispositifs similaires, 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).

3.2 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 dans le cadre d'un schéma national reconnu au titre de l'accord du SOG-IS.

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** ».

3.3 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 niveau d'attaquant 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.

4 La certification

4.1 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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2022/36v2-R01 a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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].

4.3 Reconnaissance du certificat

4.3.1 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 :



4.3.2 Reconnaissance internationale critères communs (CCRA)

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

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 :



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

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]	Cible de sécurité de référence pour l'évaluation : - <i>Security Target TachoDrive v4 on ID-One Cosmo X</i>, référence FQR 550 0299, version 7, 11 février 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - <i>Security Target Lite TachoDrive v4 on ID-One Cosmo X</i>, référence FQR 550 0336, version 6, 26 mai 2025.
[RTE]	Rapport technique d'évaluation : - <i>Evaluation Technical Report (full ETR) – KASHYAPA</i>, référence LETI.CESTI.KAS.FULL.001, version 3.2, 28 juillet 2025.
[ANA_CRY]	Cotation des mécanismes cryptographiques GARUDA, référence LETI.CESTI.GAR.RT.001 – V1.1, version 1.1, 28 juillet 2022.
[GUIDES]	Guides d'installation, d'administration et d'utilisation du produit : - [AGD_PRE] <i>TachoDrive v4 on ID-One Cosmo X AGD_PRE</i>, référence FQR 401 9054, version 7, 29 mars 2023. - [AGD_OPE] <i>TachoDrive v4 on ID-One Cosmo X AGD_OPE</i>, référence FQR 401 9055, version 2, 28 mars 2022. Guide cryptographique : - <i>TachoDrive v4 on ID-One Cosmo X cryptographic mechanisms</i>, référence FQR 401 9119, version 1, 28 janvier 2022.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA-2022_GEN_v1.0 ; - IDEMIA_2023_ALC_GEN_v1.0 ; - IDEMIA_2024_ALC_GEN_v1.0 ; - IDEMIA2024_CRB_STAR_v1.0 ; - IDEMIA-2024_Haarlem_STAR_v1.0 ; - IDEMIA_2023_NOI-P_STAR_v1.0 ; - IDEMIA2022_Pessac_STAR_v1.0 ; - IDEMIA_2023_VTR_STAR_v1.1 ; - IDEMIA_2024_SZN_STAR_v1.0 ; - IDEMIA_2023_OST_STAR_v1.0 ; - IDEMIA_2024_MNL_STAR_v1.1.
[CER-IC]	<i>Certification Report BSI-DSZ-CC-1107-V5-2024 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh,</i>

	<i>IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0 & 80.306.16.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 and v2.11.003, optional ACLv3.33.003 and v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and guidance.</i> Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) le 4 septembre 2024.
[CER-PLF]	Rapport de certification ANSSI-CC-2021/29v2-R01, ID-One Cosmo X (Code SAAAAR : 093363). Certifiée par l'ANSSI le 18 décembre 2024 sous la référence ANSSI-CC-2021/29v2-R01.
[PP0070]	<i>Protection Profile Digital Tachograph - Smart Card (Tachograph Card), Version 1.02, 15 novembre 2011.</i> Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-CC-PP-0070-2011.
[PP0091]	<i>Protection Profile Digital Tachograph - Tachograph Card (TC PP), version 1.0, 18 mai 2017.</i> Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-CC-PP-0091-2017.
[PP0084]	<i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014.</i> Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-PP-0084-2014.

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, ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.4.
[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> - <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> , version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[JIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.2.1, février 2024.
[COMP] *	<i>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices</i> , version 1.5.1, mai 2018.
[OPEN]	<i>Certification of « Open » smart card products</i> , version 1.1 (for trial use), 4 février 2013.
[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.