PREMIÈRE 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-2022/51

5G PK 5.2.2 Advanced SIM (D00233151F016B)

Paris, le 1er Mars 2023

Le Directeur général adjoint de l'Agence nationale de la 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 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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-2022/51**
Nom du produit **5G PK 5.2.2 Advanced SIM**
Référence/version du produit **D00233151F016B**
Conformité à un profil de protection ***GlobalPlatform Technology - Secure Element Protection Profile, référence GPC_SPE_174, version 1.0.*** Certifié par le OC-CCN sous la référence 2020-37-INF-3429- v1.
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL 4 augmenté** ALC_DVS.2, AVA_VAN.5
Développeur **THALES DIS** La Vigie – Avenue de Jujubier, ZI Athelia IV 13705 La Ciotat Cedex, France
Commanditaire **THALES DIS** La Vigie – Avenue de Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France
Centre d'évaluation **THALES / CNES** 290 allée du Lac, 31670 Labège, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2. **SOG-IS**

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

1.1 Présentation du produit

Le produit évalué est une carte à puce « 5G PK 5.2.2 Advanced SIM, version D00233151F016B » développée par THALES DIS.

Ce produit est destiné à être utilisé dans un smartphone ou un modem. En tant que tel, il assure l'authentification de l'abonné au réseau MNO, donnant accès aux services et applications MNO[1]

Le produit est également destiné à héberger et exécuter une ou plusieurs applications (telles que l'application e-ID), dites applets dans la terminologie Java Card. Ces applications peuvent revêtir un caractère sécuritaire différent (selon qu'elles soient « sensibles » ou « basiques ») et peuvent être chargées et instanciées avant ou après émission du produit.

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-GP].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits dans la cible de sécurité [ST], au chapitre *« 4.3 5G PK 5.2.2 Platform Description » .*

1.2.3 *Architecture*

L'architecture du produit est décrite dans la cible de sécurité [ST] aux chapitres *« 4.1 Architecture of the 5G PK 5.2.2 Advanced SIM »*. Elle est constituée :

- du microcontrôleur « ORION_CB_03 », voir [CER_IC] et [SUR_IC] ;
- de la plateforme 5G PK 5.2.2 qui est l'*operating system* du produit ;
- d'une couche applicative, comprenant des applications basiques ou sensibles, ainsi que les *security domains* (ISD, GASD, VASD, CASD and APSDs).

La TOE[2] est une plateforme ouverte décrite au chapitre « *4.2 TOE Boundaries* ». Elle comprend le microcontrôleur avec le logiciel embarqué 5G PK 5.2.2 composé :

- du *Java Card System* (JCS) implémenté selon le standard *Java Card (Oracle's Java Card 3.0.5)*, qui gère et exécute les applets. Il fournit également des *API JavaCard* pour leur développement ;

[1] *Mobile Network Operator.*

[2] *Target Of Evaluation.*

- des fonctionnalités *GlobalPlatform* (GP) implémentées selon le [PP-GP], qui fournissent une interface largement utilisée pour communiquer avec une carte à puce et gérer les applications de manière sécurisée ;
- de l'environnement télécom mis en œuvre selon les normes ETSI et 3GPP (hors périmètre de l'évaluation), y compris *Network Authentication Applications* (non évaluées) et les protocoles de communication télécom ;
- de l'application *GemActivate*, qui est une solution propriétaire de THALES DIS permettant d'activer des services et/ou charger des logiciels correctifs post-émission, sous administration MNO et THALES DIS.

Les applications déjà chargées dans le produit sont toutes identifiées la section suivante.

Bien que ces applications ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, ces applications ont été vérifiées conformément aux contraintes de développements d'applications décrites dans -[AGD_APP-Dev].

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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre « 3.2 TOE Identification » et dans le document [Identification].

Eléments de configuration		Origine
Product Name	5G PK 5.2.2 Advanced SIM	THALES DIS FRANCE SAS
TOE Name	Platform part of the 5G PK 5.2.2 smartcard software	
TOE Identification Data	D00233151F016B	
Référence du microcontrôleur :	ORION_CB_03 security controller, voir [CER_IC]	

La principale différence entre le produit et la TOE (la plateforme) correspond aux applications chargées pré-émission sur ce produit. Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après, associées à leur nom et leur AID[3].

AID	Nom de l'application
A000000151000000	ISD
A00000015153504341534400	CASD
A000000018434DFF33FFFF89C00000	RFM SoR SD
A00000001810010801000000BAFE02	GemActivate
A00000001842675072696D6547656E01	OBKG RSA Background Primes Generator

[3] *Application Identifier.*

1.2.5 *Cycle de vie*

Le cycle de vie du produit est le celui du profil de protection [PP0084] et est décrit au chapitre « 4.5 *TOE Life Cycle* » de la cible de sécurité [ST]. En particulier, la table 2 « *Product and TOE Life* cycle phase » de ce même chapitre décrit les sites de développement du produit. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site sont mentionnés dans [SITES].

Le guide [AGD_OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs, les guides [AGD_APP-Dev] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD_OPE_VA] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le « pré personnalisateur », le « personnalisateur » et le gestionnaire de la carte chargé de l'administration de la carte et comme utilisateur du produit les développeurs des applications à charger sur la plateforme.

1.2.6 *Configuration évaluée*

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

Toutes les applications identifiées à la section 1.2.4 ont été vérifiées conformément aux contraintes décrites dans [AGD_OPE_VA].

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 [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 « ORION_CB_03 », voir [CER_IC]. Le niveau de résistance du microcontrôleur a été confirmé le 7 juin 2022 dans le cadre du processus de surveillance, voir [SUR_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 [RTE].

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 recommandations sécuritaires de la TOE, voir [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 produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01]. 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 niveau d'attaquant visé.

Ce générateur d'aléa a aussi été analysé conformément à la méthode d'évaluation [AIS20/31]. Il est conforme au niveau DRG.4.

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], notamment :

- toutes les futures applications chargées sur ce produit (chargement post--émission) doivent respecter les contraintes de développement de la plateforme (guides [AGD-APP_Dev]) selon la sensibilité de l'application considérées ;
- les autorités de vérification doivent appliquer le guide [AGD_OPE_VA] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications de [GUIDES] ;
- le chargement des applications pré-émission doit être protégé conformément au guide [ORG_LOAD].

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[4], 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].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[5] , 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 :

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

[5] 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 : - *5G PK 5.2.2 Platform Security Target*, référence D1537958, version 1.2, 4 juillet 2022. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *5G PK 5.2.2 Platform Security Target – Public version*, référence D1537958, version 1.2p, 4 juillet 2022.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report RIGEL2*, référence RIGEL2_ETR, version 1.2, 5 décembre 2022. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation Technical Report for composite evaluation* RIGEL2, référence RIGEL2_ETRLite, version 1.0, 15 décembre 2022.
[CONF]	Liste de configuration du produit : - *Documentation list*, référence R1R29702_CCD_ALC_DocLIS, version 1.3, juillet 2022 ; - *[Identification] Platform Identification and Configurability* - rSIM 5G PK 522, référence D1542800, Release 1.4, July 4th 2022 ; - *Configuration list (TOE, parts and source code, excl. Crypto),* référence LIS__5GPK522_1-107 / 1.107, mai 2022 ; - *Configuration list (crypto lib and source code),* référence LIS__CryptoLib_v7-8-0-0 / 7.8.0.0, mars 2022.
[GUIDES]	[ORG_LOAD] Guide spécifique détaillant les utilisations pour les rôles/domaines de sécurité et les opérations : - *Operational guidance of Thales Advanced 5G PK removable SIM, With or Without Controlling Authority And Optional Verification Authority*, reference D1542809, Release 1.0, février 2021. [AGD_OPE_VA] Guides pour l'autorité de vérification : - *Operational guidance of Thales Advanced 5G PK removable SIM for Verification Authority,* référence D1542814, Release 1.0, février 2021 ; - *Application Verification for Certified Secure Elements – External Procedure*, référence D1258682, Release C03, février 2021. [AGD_OPE] Guides de l'utilisateur : - *5G PK 522 - User s Guide*, référence D1542792A, février 2021 ; - *UpTeq - OTA Messaging Guide*, référence D1363477C, février 2021 ; - *Patch Loading Management for Certified Secure Elements – External Procedure*, référence D1344508, Release A03, février 2021;

	- *UpTeq Card - APDU Guide*, référence D1542791A, février 2021. *Preparative guidance* : - *Preparative guidance of Thales Advanced 5G PK removable SIM*, référence D1542808, Release 1.0, février 2021. [AGD_APP-Dev] Guide pour le développement des applications - *Guidance for Secure application development on Thales Advanced 5G PK removable SIM*, référence D1542841, Release 1.2, de juillet 2022 ; - *UpTeq Card - Applet Development Guide*, référence D1542793A, février 2021 ; - *GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications*, référence GPC_GUI_050, Version 2.0, Novembre 2014, document de GlobalPlatform.
[SITES]	Rapports d'audit de site pour la réutilisation : - *Site Technical Audit Report Thales DIS Gémenos*, référence DISGEN20_GEM_STAR_v1.0 / 1.0 ; - *Site Technical Audit Report ATOS Les Clayes Sous-Bois*, référence DISGEN20_LCY_STAR_v1.0 / 1.0 - *Site Technical Audit Report Thales DIS Pont Audemer*, référence DISGEN20_PAU_STAR_v1.0 / 1.0 ; - *Site Technical Audit Report Thales DIS PTE LTD Singapore*, référence DISGEN22_SGP_STAR_v1.0_ / 1.0 ; - *Site Technical Audit Report Thales La Ciotat*, référence DISGEN20_VIG_STAR_v1.1_ / 1.1 ; - *Site Technical Audit Report Gemalto TCZEW*, référence DISGEN20_TCZ_STAR_v1.0 / 1.0 ; - *Site Technical Audit Report PUNE,* référence DISGEN21_PUN_STAR_v1.0 ; - *Site Technical Audit Report Atos Marcoussis,* référence DISGEN21_MAR_STAR_v1.1 ; - *Site Technical Audit Report Thales DIS Calamba,* référence DISGEN21_VFO-CAL_STAR_v1.0.
[CER_IC]	Rapport de certification ANSSI-CC-2017/41 Microcontrôleur ORION_CB_03 révision matériel C. Certifié par l'ANSSI le 26 juillet 2017.
[SUR_IC]	Rapport de surveillance ANSSI-CC-2017/41-S05 Microcontrôleurs ORION_CB_03 révision matériel C et ORION_DB_03 révision matériel D. Certifié par l'ANSSI le 7 juin 2022.
[PP-GP]	*GlobalPlatform Technology - Secure Element Protection Profile*, référence GPC_SPE_174, version 1.0. Certifié par le OC-CCN *(Organismo de Certificacion Centro Criptologico Nacional)* sous la référence 2020-37-INF-3429- v1.

[PP0084]	*Protection Profile, Security IC Platform Protection Profile with Augmentation Packages*, version 1.0, 13 janvier 2014. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) 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, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[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]	*Common Criteria for Information Technology Security Evaluation:* - *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 and similar devices*, version 3.1, juin 2020.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[OPEN]	*Certification of « Open » smart card products*, version 1.1 (*for trial use*), 4 février 2013.
[CCRA]	*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.
[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.
[AIS20/31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

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