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-2025/20

TEQS V1.0 (version 1.0)

Paris, le 16 Juin 2025

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

Vincent STRUBEL

[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

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

Référence du rapport de certification **ANSSI-CC-2025/20**
Nom du produit **TEQS V1.0**
Référence/version du produit **version 1.0**
Type de produit **Cartes à puce**
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
Référence du rapport d'évaluation *Evaluation Technical Report TEQS v1.0 – CORFOU* référence TEQS_V1.0_ETR version 1.1 15 avril 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 **THALES DIS FRANCE** La Vigie – Avenue de Jujubier, ZI Athelia IV 13705 La Ciotat Cedex, France
Commanditaire **THALES DIS FRANCE** 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

SOG-IS

Ce certificat est reconnu au niveau EAL2.

2 Le produit

2.1 Présentation du produit

Le produit évalué est « TEQS V1.0, version 1.0 » développé par THALES DIS FRANCE.

Le produit est destiné à héberger et exécuter une ou plusieurs applications, 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.

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 au profil de protection [PP-GP].

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 4.3 « *TEQS v1.0 platform description* ».

2.2.3 *Architecture*

L'architecture du produit est décrite dans la cible de sécurité [ST], au chapitre 4.1 « *Architecture of TEQS v1.0* ». Elle est constituée :

- du microcontrôleur « S3SSE2A », voir [CER_IC] ;
- de la plateforme TEQS V1.0 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[1] est une plateforme ouverte décrite au chapitre *4.2 « TOE Boundaries* » de [ST]. Elle comprend le microcontrôleur avec le logiciel embarqué TEQS V1.0 composé :

- du *Java Card System* (JCS) implémenté selon le standard *Java Card (Oracle's Java Card 3.1)*, qui gère et exécute les applets. Il fournit également des *API JavaCard* pour leur développement ;
- 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 ;

[1] *Target Of Evaluation.*

- de l'application *GemActivate*, qui est une solution propriétaire de THALES DIS permettant d'activer des services et/ou charger des logiciels correctifs après émission.

Bien qu'aucune application ne soit pas incluse dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN].

2.2.4 *Identification du produit*

La version certifiée du produit est identifiable par les éléments détaillés dans la cible de sécurité [ST] au chapitre 3.2 « *TOE Identification* ».

2.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 4.5 « *TOE Life Cycle* » de la cible de sécurité [ST] ; 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].

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 le propriétaire du smartphone comme indiqué chapitre 4.5 « *TOE Life Cycle* » de la cible de sécurité [ST] .

2.2.6 *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 4.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

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, 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.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « S3SSE2A », 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** ».

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-2025/20 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], 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 [AGD_APP-Dev].

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'accord[2], 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 signataires[3] , 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 SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

[3] 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 : - *TEQS V1.0 Platform Security Target*, référence D1620313, version 1.0, 12 février 2025. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *TEQS V1.0 Platform Security Target – Public version*, référence D1620313, version 1.0p, 12 février 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report TEQS v1.1 - CORFOU*, référence TEQS_V1.0_ETR, version 1.1, 25 avril 2025. 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 TEQS v1.0 - CORFOU*, référence TEQS_V1.0_ETRLite, version 1.1, 26 mai 2025.
[ANA_CRY]	*Analysis of Cryptographic Mechanisms TEQS v1.0 - CORFOU*, référence TEQS_V1.0_CRY, version 1.0, 17 mars 2025.
[CONF]	Liste de configuration du produit : *Card Project Configuration Check For TEQS v1.0 Platform*, référence D1628214_CCF_001, version 1.0, 7 février 2025.
[GUIDES]	Guide d'installation du produit [AGD_PRE] : - *Preparative guidance On CC platforms – TEQS V1.0*, référence D1622628, version 1.1, novembre 2024. Guide d'administration et d'utilisation du produit [AGD_OPE] : - *Operational guidance on CC platforms – TEQS V1.0, With or Without Controlling Authority And Optional Verification Authority*, référence D1622715, version 1.2, novembre 2024 ; - *Guidance for profile set up vs. JavaCard System Protection Profile*, référence D1578508, version 1.6, 4 juillet 2024 ; - *Patch Loading Management for Certified Secure Elements – External Procedure*, référence D1344508, version A04, Mars 2022 ; - *Operational guidance on CC platforms for Verification Authority – TEQS V1.0*, référence D1622983, version 1.0, juillet 2024 ; - *TEQS V1.0 Platform - Identification & Configurability*, référence D1627926, version 1.5, February 12th 2025 ; - *TEQS v1.0 APDU Guide*, référence D1621521, version 1.1, 5 juillet 2024. Guides de développement d'applications [AGD_APP-Dev] :

	- *GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications*, référence GPC_GUI_050, version 2.0, novembre 2014 ; - *Guidance for Secure application development Thales Embedded Secure Elements (eSE)*, référence D1623097, version 1.0, février 2025. Guides pour l'autorité de vérification [AGD_OPE_VA] : - *Application Verification for Certified Secure Elements – External Procedure*, référence D1258682, version C03, février 2021.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - *Thales DIS Development Environment ALC Class Evaluation Report (Generic Documentary activities)*, DISGEN24_ALC_GEN_v1.1, 11 octobre 2024 ; - *Site Technical Audit Report Thales DIS Gémenos*, DISGEN24_GEM_ STAR_v1.0, 18 octobre 2024 ; - *Site Technical Audit Report Thales DIS La Ciotat*, DISGEN24_LVG_STAR_v1.0, 23 octobre 2024 ; - *Site Technical Audit Report Thales DIS Pont-Audemer*, DISGEN22_PAU_STAR_v1.0, 5 décembre 2022 ; - *Site Technical Audit Report Thales DIS PTE LTD*, DISGEN24_SGP_STAR_v1.0, 8 octobre 2024 ; - *Site Technical Audit Report Sopra Steria Noida & Sopra Steria Chennai*, DISGEN23_SSN_ SSC_STAR_v1.0, 19 mars 2024 ; - *Site Technical Audit Report THALES DIS Polska Sp. Zo.o*, DISGEN23-TCZ_STAR_v1.0, 25 avril 2023 ; - *Site Technical Audit Report Telehouse*, DISGEN23_TLH_ STAR_v1.0, 19 mars 2024 ; - *Site Technical Audit Report Verizon Thales DIS Calamba*, DISGEN23_VFO-CAL_STAR_v1.0, 10 août 2023.
[CER_IC]	Produit S3SSE2A Certifié par l'ANSSI sous la référence ANSSI-CC-2024/26.
[PP-GP]	*GlobalPlatform Technology - Secure Element Protection Profile*, version 1.0, référence GPC_SPE_174. Certifié par OC-CCN *(Organismo de Certificación, Centro Criptológico Nacional)* le 18 mars 2021 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, 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,* 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 3.2.1, février 2024.
[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 2.0, mai 2024.
[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.

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