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-2020/34

## PEGASUS
## Microcontroller PEGASUS_CB_05

Fait le 18 septembre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

# 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-2020/34**

Nom du produit

**PEGASUS**

Référence/version du produit

**Microcontroller PEGASUS_CB_05**

Conformité à un profil de protection

***Security IC Platform Protection Profile with Augmentation Packages*, version 1.0**

certifié BSI-CC-PP-0084-2014 le 19 février 2014

avec conformité aux packages :

*"Authentication of the security IC"*
*"Loader dedicated for usage in Secured Environment only"*
*"Loader dedicated for usage by authorized users only"*

Critère d'évaluation et version

**Critères Communs version 3.1 révision 5**

Niveau d'évaluation

**EAL 6 augmenté**

ASE_TSS.2

éveloppeur <cas un développeur>

**THALES DIS DESIGN SERVICES SAS**

Arteparc – Bât D, Route de la côte d'Azur
13590 Meyreuil, France

Commanditaire

**THALES DIS DESIGN SERVICES SAS**

Arteparc – Bât D, Route de la côte d'Azur
13590 Meyreuil, 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 national 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 « PEGASUS, Microcontroller PEGASUS_CB_05 » développé par THALES DIS DESIGN SERVICES SAS.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

## 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 strictement conforme au profil de protection [PP0084], avec :
- le *package* « *authentication of the security IC* » ;
- le *package* « *loader dedicated for usage in secured environment only* » ;
- le *package* « *loader dedicated for usage by authorized users only* ».

### 1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :
- la protection physique du produit et des données qu'il contient grâce notamment à son *active shield* et différents détecteurs de sécurité ;
- des mécanismes de chiffrement des mémoires et bus ;
- des mécanismes d'intégrité des données ;
- un générateur physique d'aléa (PTRNG) ;
- un accélérateur cryptographique matériel fournissant des instructions de support pour l'implémentation des algorithmes Triple DES et AES ;
- un crypto-processeur appelé MEXPA fournissant des instructions de support pour l'implémentation d'algorithmes asymétriques (par exemple RSA, ECDSA et ECDH).

### 1.2.3 *Architecture*

L'architecture matérielle de la TOE est illustrée dans la suivante :

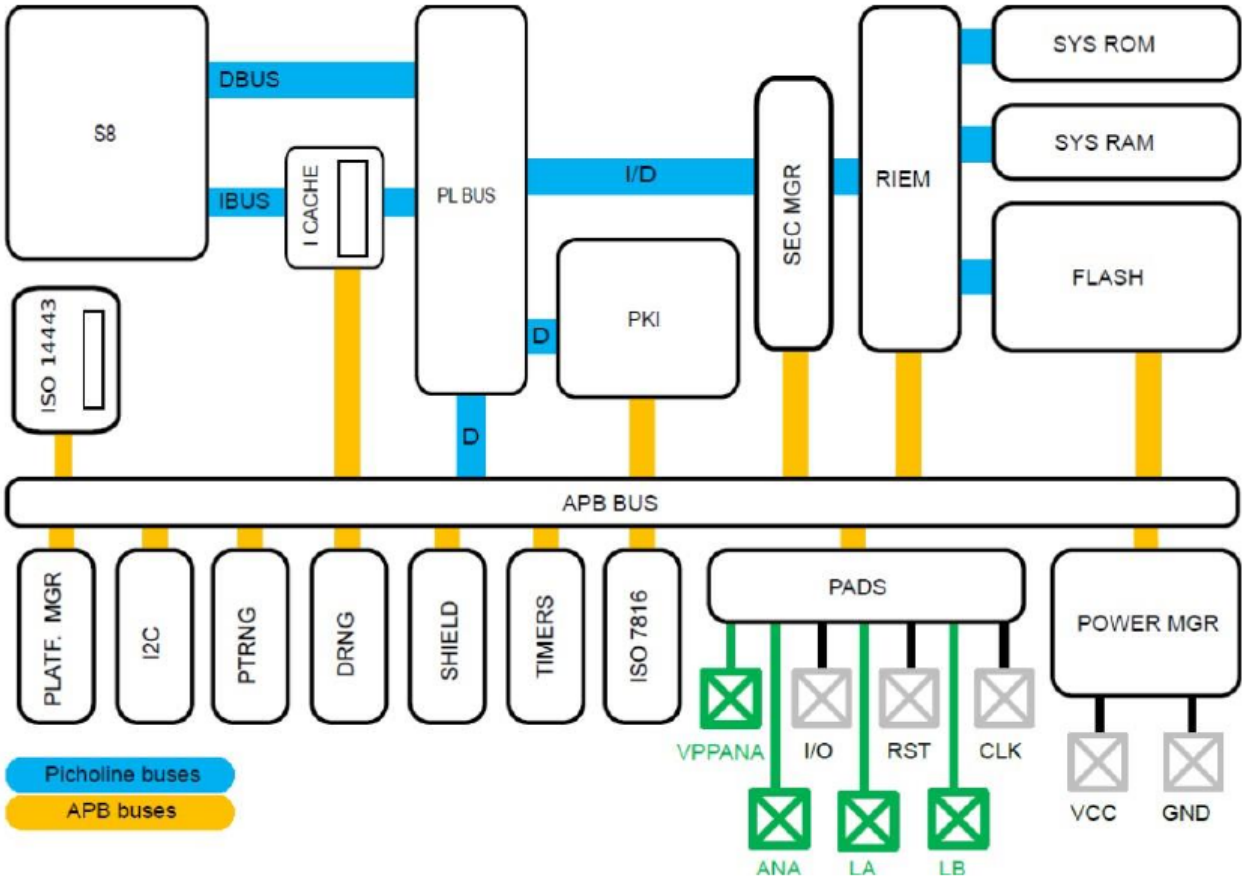


Figure 1 – Architecture matérielle

Elle est composée :

- d'un processeur S8 Secure 32-bit RISC ;
- de mémoires (ROM, RAM, *Flash*) ;
- de modules de sécurité : mécanisme de chiffrement de la mémoire et des bus, mécanisme d'intégrité des données, génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;
- de modules fonctionnels : gestion des entrées et sorties avec et sans contact (ISO7816 et ISO14443), générateurs de nombres aléatoires (PTRNG et DTRNG), coprocesseurs cryptographiques implémentant des instructions dédiées pour les algorithmes symétriques et de hashage, crypto-processeurs PKI fournissant des instructions pour l'implémentation d'algorithmes cryptographiques asymétriques.

La TOE comporte également d'une partie logicielle composée :

- d'un *loader* permettant le chargement de logiciels ;
- d'un *boot loader* permettant l'initialisation, la configuration et le démarrage du produit.

Le *Product Engineering Operating System* (PEOS) dédié au test et inclus dans le *boot loader* est hors du périmètre de l'évaluation. Il ne sera pas disponible pour l'utilisateur final.

### 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 1.2.1 « TOE Identification ».

| Eléments de configuration | | Données d'identification lues |
|---|---|---|
| Identification du microcontrôleur | Nom de la TOE (PEGASUS) | 0x08 |
| | Révision matérielle (C) | 0x43 |
| Identification des logiciels embarqués | Révision logicielle de la plateforme ROM (B) | 0x42 |
| | Révision logicielle *Flash* (05) | 0x05 |
| | Version du *loader* (1.8) | 0x3138 |

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans les guides « PEGASUS User Manual » et « PEGASUS Loader User Manual » (voir [GUIDES]).

La principale différence entre le produit et la TOE (la plateforme) correspond au PEOS mentionné à la section précédente qui est hors TOE.

### 1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit dans la cible de sécurité [ST], il est conforme au cycle de vie de sept phases décrit dans [PP0084].

Seules les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous la forme de *wafers* ou de *wafers* sciés (*dices*). En option, la TOE peut également être livrée après la phase 4, dans sa forme finale, par exemple sous forme de carte à puce.

La phase 2 correspond à la phase de développement du microcontrôleur. Elle comprend notamment la conception du circuit et le développement du logiciel dédié.

La phase 3 quant à elle couvre la fabrication du microcontrôleur. Elle comprend l'intégration et la fabrication du masque, la fabrication et le test du circuit, la préparation et la pré-personnalisation si nécessaire.

Enfin, la phase 4, pouvant être gérée optionnellement par le développeur, comprend le conditionnement, le test et la pré-personnalisation si nécessaire.

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

| | |
|---|---|
| **Thales DIS Design Services SAS (INVIA)**<br>Arteparc – Bât D,<br>Route de la côte d'Azur<br>13590 Meyreuil<br>France | **Trusted Labs (Thales Digital Identity and Security)**<br>6 rue de la Verrerie<br>92190 Meudon<br>France |
| **MU-Electronics**<br>49 rue de Jabal Tazekka, 1er étage, Agdal<br>10000 Rabat<br>Maroc | **Thales Digital Identity and Security**<br>6 rue de la Verrerie<br>92190 Meudon<br>France |
| **Thales Digital Identity and Security Singapore**<br>12 Ayer Rajah Crescent<br>139941 Singapour | **PDMC Masks Manufacturing (1A)**<br>1st Floor, N°2, Li-Hsin Rd, Science Park<br>Hsinchu 30078<br>Taïwan |
| **UMC Fab 12i**<br>No.3, Pasir Ris Drive 12,<br>Singapore 519528<br>Singapour | **Masks Manufacturing (1B)**<br>N°13, Tongshan Rd, Daya District<br>Taishung 42879<br>Taïwan |
| **UTAC USG1**<br>5 Serangoon North Avenue 5,<br>Singapore 554916<br>Singapour | **Masks Manufacturing (1D)**<br>N°6, Li-Hsin 7th Rd, Science Park<br>Hsinchu 30078<br>Taïwan |
| **UTAC Thai Limited 1 (UTL1)**<br>237 Lasalle road, Bangna,<br>Bangkok 10260<br>Thaïlande | **UTAC Thai Limited 3 (UTL3)**<br>73 Moo5, Bangsamak,<br>Chachoengsao, 24180<br>Thaïlande |

### 1.2.6 *Configuration évaluée*

Le certificat porte sur le microcontrôleur tel que décrit au chapitre 1.2.3 et identifié au chapitre 1.2.4. Toute autre application, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre de l'évaluation.

# 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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 27 juillet 2020, 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 a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation et il répond aux exigences de la classe PTG.2.

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [REF] il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

# 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 « PEGASUS, Microcontroller PEGASUS_CB_05 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 6 augmenté du composant ASE_TSS.2.

## 3.2 Restrictions d'usage

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

Ce certificat donne une appréciation de la résistance du produit « PEGASUS, Microcontroller PEGASUS_CB_05 » à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

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]. En particulier, l'implémentation des algorithmes cryptographiques devra être entièrement évaluée lors de l'évaluation en composition.

## 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[1], 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 :

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

### 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[2] , 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. 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 6+ | Intitulé du composant |
| ADV Développement | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 | **1** | *Security architecture description* |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 | **5** | *Complete semi-formal functional specification with additional error information* |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 | **2** | *Complete mapping of the implementation representation of the TSF* |
| | ADV_INT | | | | | 2 | 3 | 3 | **3** | *Minimally complex structured internals* |
| | ADV_SPM | | | | | | 1 | 1 | **1** | *Formal TOE security policy model* |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 | **5** | *Complete semiformal modular design* |
| AGD Guides d'utilisation | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | *Operational user guidance* |
| | AGD_PRE | 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 | **5** | *Advanced support* |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 | **5** | *Development tools CM coverage* |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 | **1** | *Delivery procedures* |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 | **2** | *Sufficiency of security measures* |
| | ALC_FLR | | | | | | | | | |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 | **1** | *Developer defined life-cycle model* |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 | **3** | *Compliance with implementation standards – all parts* |
| ASE Evaluation de la cible de sécurité | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | *Conformance claims* |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | *Extended components definition* |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **1** | *ST introduction* |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | **2** | *Security objectives* |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | **2** | *Derived security requirements* |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 | **1** | *Security problem definition* |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | **2** | *TOE summary specification with architectural design summary* |
| ATE Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 | **3** | *Rigorous analysis of coverage* |
| | ATE_DPT | | | 1 | 2 | 3 | 3 | 4 | **3** | *Testing: modular design* |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 | **2** | *Ordred functional testing* |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 | **2** | *Independent testing: sample* |
| AVA Estimation des vulnérabilités | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 | **5** | *Advanced methodical vulnerability analysis* |

# ANNEXE B. Références documentaires du produits évalué

| | |
|---|---|
| [ST] | Cible de sécurité de référence pour l'évaluation :<br>- Security Target for PEGASUS, référence PEGASUS_ST, version 1.1 et datée du 19 décembre 2019, THALES DIS DESIGN SERVICES SAS (INVIA).<br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>- Security Target Lite for PEGASUS, référence PEGASUS_C_ST, version 003 et datée du 20 juin 2020, THALES DIS DESIGN SERVICES SAS (INVIA). |
| [RTE] | Rapport technique d'évaluation :<br>- Evaluation Technical Report (full ETR) – TREZENE, référence LETI.CESTI.TRE.FULL.001 – V1.1, version 1.1 et daté du 27 juillet 2020, *CEA-Leti*.<br>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :<br>- Evaluation Technical Report (ETR for composition) – TREZENE, référence LETI.CESTI.TRE.COMPO.001 – V1.1, version 1.1 et daté du 27 juillet 2020, CEA-Leti. |
| [CONF] | Liste de configuration du produit :<br>- PEGASUS_CB_05 Identification, référence PEGASUS_CB_IDENTIFICATION, version 1.1, daté du 2 juillet 2020, THALES DIS DESIGN SERVICES SAS (INVIA) ;<br>- Hardware Configuration List – PEGASUS_CB, référence PEGASUS_HW_CONF_LIST, version 1.0, datée 8 octobre 2019, THALES DIS DESIGN SERVICES SAS (INVIA) ;<br>- PEGASUS Software Configuration List – Firmware B05, référence Pegasus_Firmware_B05_Tracking_File_INVIA_v1.0, version 1.0 et daté du 22 juin 2020, THALES DIS DESIGN SERVICES SAS (INVIA) ;<br>- PEGASUS Software Configuration List – Loader v1.8, référence Pegasus_Loader1_8_Tracking_File_INVIA_v1.1, version 1.1, THALES DIS DESIGN SERVICES SAS (INVIA). |
| [GUIDES] | - Pegasus User Manual, révision 0.9.6, daté du 11 décembre 2019, THALES DIS DESIGN SERVICES SAS (INVIA) ;<br>- Pegasus LOADER User Manual, référence LOADER_SPECIFICATION, révision 1.1, daté du 20 décembre 2019, THALES DIS DESIGN SERVICES SAS (INVIA) ;<br>- PEGASUS Security Guidance, référence Security Guidance, révision 0.6, daté du 19 décembre 2019, THALES DIS DESIGN SERVICES SAS (INVIA) ;<br>- S8 Instruction Set Architecture, version 1.2a, daté du 28 janvier 2019, THALES DIS DESIGN SERVICES SAS (INVIA) ;<br>- Secure 32 bits CPU Embedded Application Binary Interface (EABI), version 0.6, daté de mars 2013, THALES DIS DESIGN SERVICES SAS (INVIA) ;<br>- Pegasus Assembly Instructions, référence Pegasus_assy, révision 0.4, daté du 18 avril 2018, THALES DIS DESIGN SERVICES SAS (INVIA) ;<br>- Secure Delivery, référence AGD_Secure Delivery, révision V1.0, daté du 12 décembre 2016, THALES DIS DESIGN SERVICES SAS (INVIA). |

| | |
|---|---|
| [SITES] | Rapports d'analyse documentaire et d'audit de site pour la réutilisation :<br>- GEMALTO Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence GTOGEN19_GEN_v1.0, version 1.0, daté du 12 février 2019, SERMA Safety & Security ;<br>- GEMALTO Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence 17-0466_ALC-GEN_V1.0, version 1.0, daté du 23 mars 2018, SERMA Safety & Security ;<br>- INVIA Development Environment ALC Class Evaluation Report (Generic Documentary activitites), référence GTOGEN18-INVIA_GEN_v2.0, daté du 26 juin 2019, SERMA Safety & Security ;<br>- Site Technical Audit Report – MDN Site Audit, référence GTOGEN19_MDN_STAR_v1.0, version 1.0, daté du 2 aout 2019, SERMA Safety & Security ;<br>- Site Visit Lite Report – GEMALTO Singapore, référence 17-0466-SGP_SVR_M_v1.0, version 1.0, daté du 16 mai 2018, SERMA Safety & Security ;<br>- Site Technical Audit Report – INVIA Meyreuil, référence GTOGEN18-INVIA_STAR_v1.0, daté du 5 mars 2019, SERMA Safety & Security ;<br>- Site Technical Audit Report – Mu-E Rabat site audit, référence GTOGEN19-INVIA_MuE_STAR_v1.0, version 1.0, daté du 26 juillet 2019, SERMA Safety & Security ;<br>- Site Technical Audit Report – Site_PDMC2 site audit, référence Site_PDMC2_STAR_v1.0, version 1.0, daté du 21 novembre 2018, SERMA Safety & Security ;<br>- Site Technical Audit Report – UTAC Thai Limited 1, référence UTL1.2_STAR_v1.0, version 1.0, daté du 6 décembre 2018, SERMA Safety & Security ;<br>- Site Technical Audit Report – UTAC Thai Limited 3 (UTL3), référence UTL3.2_STAR_v1.1, version 1.1, daté du 22 janvier 2019, SERMA Safety & Security. |
| [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 C. 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] | *Common Criteria for Information Technology Security Evaluation:*<br>- *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;<br>- *Part 2: Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;<br>- *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 3.0, avril 2019. |
| [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 (*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.