



**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-R02**

**PEGASUS\_CB\_05  
(Référence : PEGASUS\_TOE\_v3)**

Paris, le 22 Juillet 2024

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 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](mailto:certification@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	<b>ANSSI-CC-2020/34-R02</b>
Nom du produit	<b>PEGASUS_CB_05</b>
Référence/version du produit	<b>Référence : PEGASUS_TOE_v3</b>
Conformité à un profil de protection	<b>Security IC Platform Protection Profile with Augmentation Packages, version 1.0</b> certifié BSI-CC-PP-0084-2014 le 19 février 2014 avec conformité aux packages : <i>"Authentication of the security IC"</i> <i>"Loader dedicated for usage in Secured Environment only"</i> <i>"Loader dedicated for usage by authorized users only"</i>
Critère d'évaluation et version	<b>Critères Communs version 3.1 révision 5</b>
Niveau d'évaluation	<b>EAL6 augmenté</b> <b>ASE_TSS.2</b>
Développeur	<b>THALES DIS France SAS</b> Route de la Cote d'Azur, Arterparc 13590 Meyreuil, France
Commanditaire	<b>THALES DIS France SAS</b> Route de la Cote d'Azur, Arterparc 13590 Meyreuil, France
Centre d'évaluation	<b>CEA - LETI</b> 17 avenue des martyrs, 38054 Grenoble Cedex 9, France
Accords de reconnaissance applicables	  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.cyber.gouv.fr](http://www.cyber.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 .....	7
1.2.4	Identification du produit.....	7
1.2.5	Cycle de vie .....	7
1.2.6	Configuration évaluée .....	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation .....	8
2.2	Travaux d'évaluation .....	8
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 .....	10
3.1	Conclusion.....	10
3.2	Restrictions d'usage .....	10
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 .....	12
ANNEXE B.	Références liées à la certification .....	14

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « PEGASUS\_CB\_05, Référence : PEGASUS\_TOE\_v3 » développé par THALES DIS France 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* » (Package 1);
- le package « *loader dedicated for usage by authorized users only* » (Package 2).

### 1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- Une protection physique du produit et des données qu'il contient grâce notamment à un système d'*active shield*, ainsi que plusieurs détecteurs de sécurité ;
- Des mécanismes de chiffrement des mémoires et des bus de communication ;
- Un générateur physique de nombres aléatoires (PTRNG) ;
- Un accélérateur cryptographique matériel fournissant des instructions pour l'implémentation des algorithmes cryptographiques TDES et AES ;
- Un *PKI Engine* appelé MEXPA en charge de fournir des instructions d'accélération pour l'implémentation des algorithmes cryptographiques RSA, ECDSA et ECDH.

### 1.2.3 Architecture

Le produit est constitué d'une partie matérielle et d'une partie logicielle toutes deux décrites dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Overview* ».

### 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* ».

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]).

### 1.2.5 Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité [ST] au chapitre 1.2.4 « *TOE Life Cycle* ». Il est conforme au cycle de vie de sept phases décrites dans [PP0084] au chapitre 1.2.3 « *TOE Definition* ».

### 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 du présent rapport. Toute autre application, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne font 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 [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 jour de sa finalisation par le CESTI 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 [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].

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. Afin que les mécanismes analysés soient conformes aux exigences de ce référentiel, les recommandations identifiées [GUIDES] doivent être suivies.

Dans le cas où le générateur d'aléa serait utilisé à des fins cryptographiques, il est obligatoire de le combiner à un mécanisme algorithmique de génération de pseudo-aléa, de nature cryptographique, afin de fournir des données aléatoires cryptographiquement satisfaisantes, comme énoncé dans le document [ANSSI Crypto].

Ce générateur d'aléa a aussi été analysé conformément à la méthode d'évaluation [AIS20/31] et suivant les dispositions décrites dans la note d'application [CC-NOTE-24] et il répond aux exigences de la classe PTG.2.

### **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.

Ce certificat donne une appréciation de la résistance du produit 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 microcontrôleur 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].

### 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<sup>1</sup>, 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 :

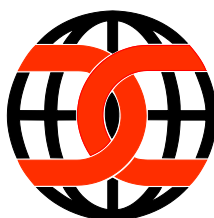


#### 3.3.2 Reconnaissance internationale critères communs (CCRA)

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<sup>2</sup>, 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 :



---

<sup>1</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.eu](http://www.sogis.eu).

<sup>2</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://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"><li>- <i>Security Target for PEGASUS (Microcontroller PEGASUS_CB_05)</i>, référence PEGASUS_ST, version 1.35, 15 février 2024.</li></ul> <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"><li>- <i>Security Target Lite for PEGASUS (Microcontroller PEGASUS_CB_05)</i>, référence PEGASUS_CB_05_ST_Security_Target_Lite, version 009, 15 février 2024.</li></ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"><li>- <i>Evaluation Technical Report (full ETR) – TREZENE_2024</i>, référence LETI.CESTI.TRE.FULL.001 – V6.0, révision 6.0, 19 février 2024.</li></ul> <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none"><li>- <i>Evaluation Technical Report (ETR for composition) – TREZENE_2024</i>, référence LETI.CESTI.TRE.COMPO.001 – V6.0, révision 6.0, 19 février 2024.</li></ul>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"><li>- <i>PEGASUS List of Documentation</i>, référence PEGASUS – Documentation List_v6, révision 6, 15 février 2024 ;</li><li>- <i>PEGASUS_CB_05 Identification</i>, référence PEGASUS_CB_05_Identification_v1.1, révision 1.1, 02 juillet 2020 ;</li><li>- <i>PEGASUS Hardware Configuration List</i>, référence PEGASUS_ALC_Hardware Configuration List-v1.0, révision 1.0, 08 octobre 2019 ;</li><li>- <i>PEGASUS Software Configuration List – Firmware B05</i>, référence Pegasus_Firmware_B05_Tracking_File_INVIA_v1.0, révision 1.0, 22 juin 2020 ;</li><li>- <i>PEGASUS Software Configuration List – Loader v1.8</i>, référence Pegasus_Loader1_8Tracking_File_INVIA_v1.1, révision 1.1, 02 juillet 2020.</li></ul>
[GUIDES]	<ul style="list-style-type: none"><li>- <i>PEGASUS User Manual</i>, référence PegasusUM_0.9.6, révision 0.9.6, 11 décembre 2019 ;</li><li>- <i>PEGASUS Loader User Manual</i>, référence <i>UserManual_CC_Loader_v1.1</i>, révision 1.1, 20 décembre 2019 ;</li><li>- <i>PEGASUS Security Guidance</i>, référence <i>INVIA_PEGASUS_Security_Guidance_v0.8</i>, révision 0.8, 15 février 2024 ;</li><li>- <i>S8 Instruction Set Architecture</i>, référence s8-isa-v1.2a, version 1.2a, 28 janvier 2019 ;</li><li>- <i>Secure 32 bits CPU Embedded Application Binary Interface (EABI)</i>, référence s8-abi, version 0.6, mars 2013 ;</li></ul>

	<ul style="list-style-type: none"><li>- <i>PEGASUS Assembly Instructions</i>, référence Pegasus Assembly, révision 0.4, 18 avril 2018 ;</li><li>- <i>Guidance – Secure Delivery</i>, référence AGD-Secure delivery-v1.0, révision 1.0, 12 décembre 2016 ;</li><li>- <i>Pegasus API Guide</i>, référence Pegasus_API_Guide, révision 0.6, 06 mars 2023.</li></ul>
[PP0084]	<p><i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages</i>, version 1.0, 13 janvier 2014. Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-PP-0084-2014.</p>

## 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]	<i>Common Criteria for Information Technology Security Evaluation:</i> <ul style="list-style-type: none"><li>- <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;</li><li>- <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;</li><li>- <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.</li></ul>
[CEM]	<i>Common Methodology for Information Technology Security Evaluation: Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[IIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[IIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.2, novembre 2022.
[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.
[AIS20/31]	<i>A proposal for: Functionality classes for random number generators, AIS20/AIS31</i> , version 2.0, 18 septembre 2011, BSI ( <i>Bundesamt für Sicherheit in der Informationstechnik</i> ).

[CC-NOTE-24]	Note d'application – Evaluation de générateurs d'aléa selon AIS20/31 dans le schéma français, référence ANSSI-CC-NOTE-24, version 1.0.
--------------	--

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