



*Liberté • Égalité • Fraternité*  
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale  
Agence nationale de la sécurité des systèmes d'information

## **Rapport de certification ANSSI-CC-2018/34**

### **AT90SO128 revision H including optional cryptographic library Toolbox 00.03.1x.xx family**

*Paris, le 9 août 2018*

*Le directeur général adjoint de l'agence  
nationale de la sécurité des systèmes  
d'information*

Emmanuel GERMAIN  
[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.

<i>Référence du rapport de certification</i>	<b>ANSSI-CC-2018/34</b>
<i>Nom du produit</i>	<b>AT90SO128</b>
<i>Référence/version du produit</i>	<b>Révision H, référence interne 58U58, Toolbox version 00.03.12.01, 00.03.11.08, 00.03.10.02 ou 00.03.14.03</b>
<i>Conformité à un profil de protection</i>	<b>Security IC Platform Protection Profile certifié BSI-CC-PP-0035-2007 en juin 2007</b>
<i>Critères d'évaluation et version</i>	<b>Critères Communs version 3.1 révision 4</b>
<i>Niveau d'évaluation</i>	<b>EAL 5 augmenté ALC_DVS.2, AVA_VAN.5</b>
<i>Développeur</i>	<b>Wisekey Semiconductors Rue de la carrière de Bachasson, Arterparc Bachasson, Bat. A 13590 Meyreuil - France</b>
<i>Commanditaire</i>	<b>Wisekey Semiconductors Rue de la carrière de Bachasson, Arterparc Bachasson, Bat. A 13590 Meyreuil - France</b>
<i>Centre d'évaluation</i>	<b>Serma Safety &amp; Security 14 rue Galilée, CS 10055, 33615 Pessac Cedex, France</b>
<i>Accords de reconnaissance applicables</i>	<div style="display: flex; justify-content: space-around; align-items: center;"><div style="text-align: center;"><b>CCRA</b> </div><div style="text-align: center;"><b>SOG-IS</b> </div></div> <p><b>Ce certificat est reconnu au niveau EAL2</b></p>

# Préface

## La certification

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 Premier ministre 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](http://www.ssi.gouv.fr).

# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Introduction</i> .....	6
1.2.2. <i>Services de sécurité</i> .....	6
1.2.3. <i>Architecture</i> .....	6
1.2.4. <i>Identification du produit</i> .....	8
1.2.5. <i>Cycle de vie</i> .....	8
1.2.6. <i>Configuration évaluée</i> .....	9
<b>2. L’EVALUATION .....</b>	<b>10</b>
2.1. REFERENTIELS D’EVALUATION .....	10
2.2. TRAVAUX D’EVALUATION .....	10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	10
2.4. ANALYSE DU GENERATEUR D’ALEAS .....	10
<b>3. LA CERTIFICATION .....</b>	<b>11</b>
3.1. CONCLUSION .....	11
3.2. RESTRICTIONS D’USAGE .....	11
3.3. RECONNAISSANCE DU CERTIFICAT .....	12
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	12
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	12
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT .....</b>	<b>13</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>14</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>15</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est le microcontrôleur « AT90SO128, révision H, embarquant la bibliothèque cryptographique optionnelle *Toolbox* version 00.03.12.01, 00.03.11.08, 00.03.10.02 ou 00.03.14.03 » développé par *WISEKEY SEMICONDUCTORS*.

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 conforme au profil de protection [PP0035].

### 1.2.2. Services de sécurité

Les principaux services de sécurité fournis par la TOE<sup>1</sup> sont :

- la gestion sécurisée de la mémoire ainsi qu'une protection des accès à cette mémoire ;
- la protection en intégrité et en confidentialité des données utilisateur et des logiciels embarqués exécutés ou stockés dans les différentes mémoires de la TOE ;
- la protection physique ;
- la non-observabilité des informations sensibles ;
- le support au chiffrement cryptographique à clés symétriques ou asymétriques ;
- le support à la génération de nombres non prédictibles ;
- le service optionnel de bibliothèque cryptographique *Toolbox* offrant des fonctionnalités RSA, ECC, AES, DES, ainsi que la génération sécurisée de nombres premiers et de clés RSA.

### 1.2.3. Architecture

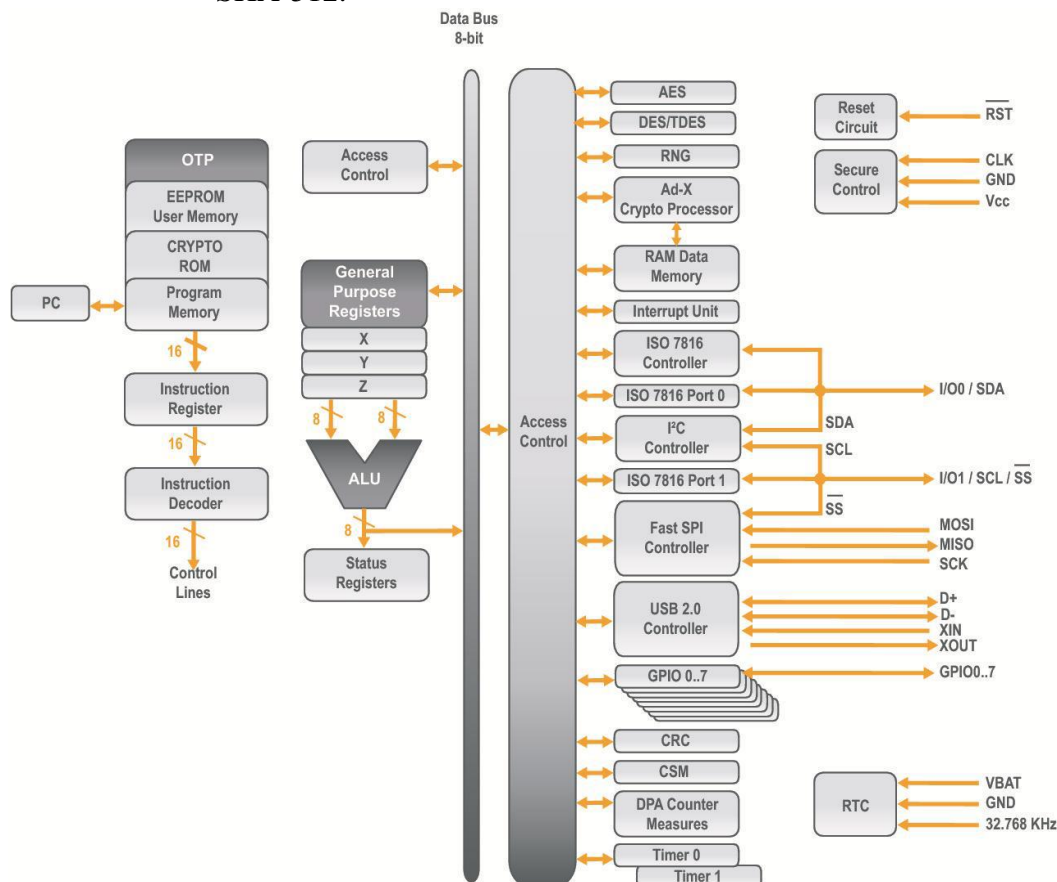
Le produit est constitué des éléments suivants (voir Figure 1) :

- une partie matérielle comprenant :
  - o un processeur 8-/16-bit *Enhanced RISC Architecture CPU* ;
  - o des mémoires ROM (288Ko à disposition de l'utilisateur), *EEPROM* (128Ko) et RAM (12Ko pour le CPU dont 2Ko partagés avec l'accélérateur matériel Ad-X) ;

---

<sup>1</sup> *Target Of Evaluation* - périmètre d'évaluation.

- des modules de sécurité : protection de la mémoire (MMU, *Memory Management Unit*), génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;
- des modules fonctionnels : gestion des entrées / sorties en mode contact (ISO7816), interfaces I2C, SPI et USB, générateur de nombres aléatoires (RNG, *Random Number Generator*) ;
- des coprocesseurs cryptographiques optionnels pour accélérer les calculs AES pour le support des algorithmes AES, EDES pour le support des algorithmes DES et d'un accélérateur cryptographique 32-bit Ad-X pour les opérations à cryptographie asymétrique,
- une partie logicielle composée :
  - de logiciels de test du microcontrôleur embarqués en mémoire ROM et en EEPROM ; ces logiciels ne font pas partie de la TOE ;
  - une bibliothèque cryptographique *Toolbox* optionnelle appartenant à la famille 00.03.1x.xx, à savoir optionnellement une des versions suivantes :
    - la version 00.03.14.03 incluant les fonctionnalités : SelfTest, AIS31OnlineTest, PrimeGen (Miller Rabin), RSA without CRT et RSA with CRT ;
    - la version 00.03.10.02 incluant les fonctionnalités précédentes ainsi que SHA-1, SHA-224 et SHA-256 ;
    - la version 00.03.11.08 incluant les fonctionnalités précédentes ainsi que ECDSA over Zp et EC-DH over Zp ;
    - la version 00.03.12.01 incluant toutes les fonctionnalités précédentes ainsi que ECDSA over GF(2n), EC-DH over GF(2n), SHA-384 et SHA-512.



**Figure 1. Architecture de la TOE**

### 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 1.4 « *TOE Overview* ».

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur AT90S0128	58U58	0x3D
	<i>Révision H</i>	0x87 ou 0xA7
Identification des logiciels embarqués	<i>Firmware version</i>	NA
	<i>Dedicated Software</i>	NA
Identification des bibliothèques	<i>Cryptograohic Toolbox SW : version 00.03.12.01</i>	0x00031201
	<i>version 00.03.11.08</i>	0x00031108
	<i>version 00.03.10.02</i>	0x00031002
	<i>version 00.03.14.03</i>	0x00031403

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 le guide « AT90SO128 Technical Datasheet », voir [GUIDES]. L'identification du microcontrôleur est également possible en lisant directement sur la surface du microcontrôleur les données 58U58 et H.

### 1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

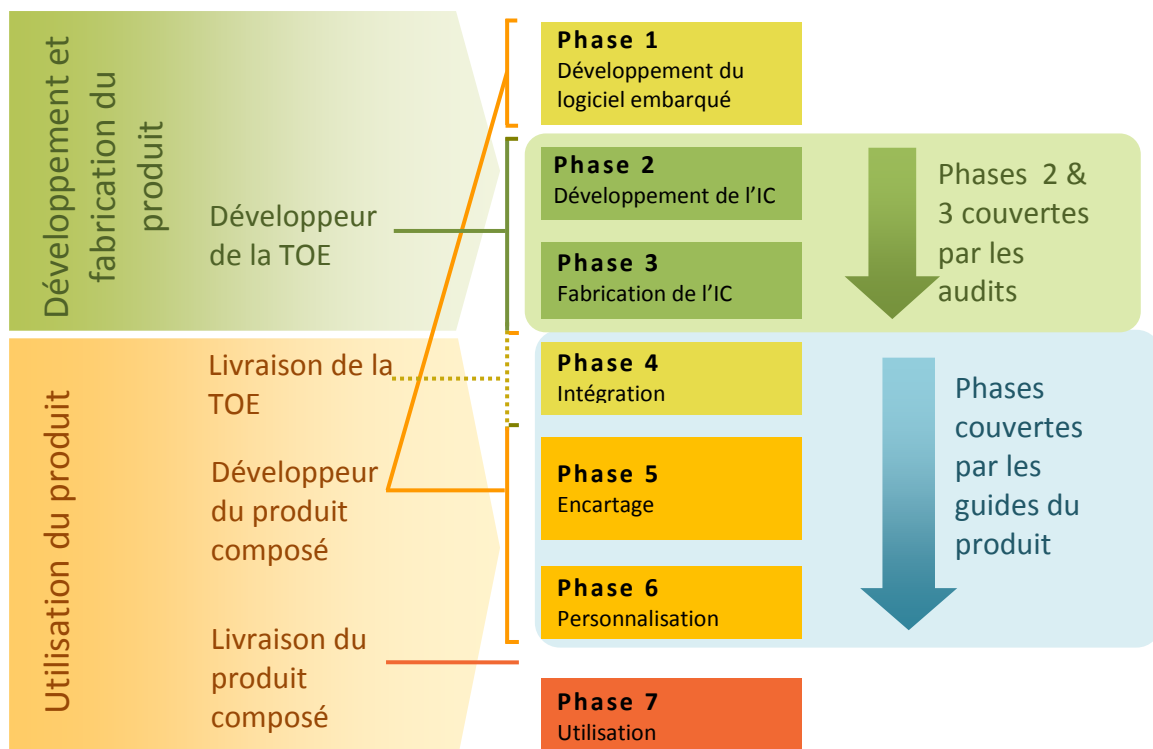


Figure 2. Cycle de vie de la TOE



Le produit a été développé sur les sites suivants :

WISEKEY Meyreuil ( <i>Design Centre</i> ) Rue de la carriere de Bachasson 13590 Meyreuil – France	PRESTO Meyreuil ( <i>Manufacturing operation suport and Warehouse</i> ) Rue de la carriere de Bachasson 13590 Meyreuil – France
UMC : UNITED MICROELECTRONIC Corp ( <i>Wafer Manufacturing Fab 8C, 8D</i> ) HsinChu – Taiwan	TOPPAN PHOTOMASKS ( <i>Masks Manufacturing</i> ) 1127-3 Hopin Road Padeh City Taoyuan – Taiwan
ASE : ADVANCED SEMICONDUCTOR ENGINEERING ( <i>Test Centre</i> ) 26 Chin 3rd Rd Nantze Export Processing Zone Kaohsiung – Taiwan	UTAC - UTL3 ( <i>Test Centre</i> ) 73 Moo 5, Bangsamak, Bangpakong Chachoengsao 24180, Thaïlande

Le produit comporte lui-même une gestion de son cycle de vie, prenant la forme de trois modes :

- mode *Test* qui permet à l'administrateur authentifié de tester la TOE en fin de phase de fabrication, il est désactivé par le sciage du *wafer* à la fin de la phase 3 ;
- mode *User* qui est le mode final d'utilisation du microcontrôleur par le porteur du produit final ; le produit a été évalué dans ce mode ;
- mode *Secure Test Return* qui est utilisé pour diagnostiquer le produit s'il se trouve défaillant ; dans ce mode, les droits d'accès à la TOE sont restreints.

### 1.2.6. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur et à la bibliothèque cryptographique. Toute autre application éventuellement embarquée, notamment les logiciels de test du microcontrôleur embarqués pour les besoins de l'évaluation, ne fait donc pas partie du périmètre d'évaluation.

Au regard du cycle de vie, le produit évalué est le produit qui sort de la phase 3 (au titre d'ALC) du cycle de vie. Le produit fourni au centre d'évaluation est le microcontrôleur AT90SO128 en révision H incluant la bibliothèque cryptographique *Toolbox* en version complète 00.03.12.01. Enfin, pour les besoins de l'évaluation, une application de test *WISEKEY* présente en ROM, mais ne faisant pas partie de la TOE, a été livrée.

## 2. L'évaluation

### 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4 [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 s'appuie sur les résultats d'évaluation du microcontrôleur « AT90SO128 révision F » certifié le 30 mai 2014 sous la référence ANSSI-CC-2014/24, voir [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 20 juin 2018, 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

Ce générateur a fait l'objet d'une analyse.

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. 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.

Le générateur d'aléas a en outre fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation : il atteint le niveau « P2 – *High level* ».

## 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 « AT90SO128, révision H, embarquant la bibliothèque cryptographique optionnelle *Toolbox* version 00.03.12.01, 00.03.11.08, 00.03.10.02 ou 00.03.14.03 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants AVA\_VAN.5 et ALC\_DVS.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 « AT90SO128, révision H, embarquant la bibliothèque cryptographique optionnelle *Toolbox* version 00.03.12.01, 00.03.11.08, 00.03.10.02 ou 00.03.14.03 » 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].

### 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 [CC RA].

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.org](http://www.sogis.org).

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

## Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- Security Target AT90SO128 (SPYDER), référence Spyder_ST_V1.7, référence 1.7, 09/04/2018.</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>- Security Target Lite AT90SO128 (SPYDER), référence TPG0028G, référence G, 09/04/2018.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report - SPYDER-H project, référence SPYDER-H_ETR_v1.1, version 1.1, 20/06/2018.</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>- Evaluation Technical Report Lite - SPYDER-H project, référence SPYDER-H_ETR-Lite_v1.1, version 1.1, 20/06/2018.</li> </ul>
[CONF]	<p>Evaluation Documents List, référence Spyder_EDL_v1.8, version 1.8.</p>
[GUIDES]	<ul style="list-style-type: none"> <li>- AT90SO128 Technical Datasheet, référence TPR0402DX, version D, 24/01/2017 ;</li> <li>- SmartACT's User Manual, référence TPR0134EX, version E ;</li> <li>- Toolbox 00.03.1x.xx on AT90SCXXXXC, référence TPR0454EX, version E, 28/03/2017 ;</li> <li>- Technical Datasheet AT90SC product Ad-X, référence TPR0116GX, version G, 13/04/2017 ;</li> <li>- Security Recommendations for 0.13µm Products - 2, référence TPR0456HX, version H, 2/12/2016 ;</li> <li>- Secure Hardware DES/TDES on AT90SC ASL5 Products (0.13µm), référence TPR0400LX, version L, 12/04/2017 ;</li> <li>- Generating Random numbers to known standards for 0.13µm Products, référence TPR0468GX, version G, 29/03/2017 ;</li> <li>- Secure use of TBX 00.3.1x.xx on AT90SC, référence TPR04551X, version L, 17/05/2017 ;</li> <li>- Secure Hardware AES on AT90SC products (0.13µm), référence TPR0573DX, version D, 12/04/2017 ;</li> <li>- Efficient use of Ad-X for implementing cryptographic operations, référence TPR0142FX, version F, 12/04/2017 ;</li> <li>- The Code Signature Module for 0.13µm Products, référence TPR0409DX, version D, 31/03/2017 ;</li> <li>- Wafer Saw Recommendations, référence TPG0079, version C, 31/03/2017.</li> </ul>
[PP0035]	<p>Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i></p>
[CER]	<p>Rapport de certification ANSSI-CC-2014/24, Microcontrôleur AT90SO128 révision F embarquant la bibliothèque cryptographique optionnelle Toolbox version 00.03.12.01. <i>Certifié par l'ANSSI sous la référence ANSSI-CC-2014/24 le 30 mai 2014.</i></p>

### Annexe 3. 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.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[CC]	Common Criteria for Information Technology Security Evaluation : <ul style="list-style-type: none"> <li>- Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001;</li> <li>- Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002;</li> <li>- Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.</li> </ul>
[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 2.9, janvier 2013.
[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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
[AIS 31]	Functionality classes and evaluation methodology for physical random number generator, AIS31, version 1, 25 septembre 2001, 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.