



*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-2013/06**

**Microcontrôleurs sécurisés SA23YL18 et  
SB23YL18 incluant la bibliothèque  
cryptographique NesLib v2.0, v3.0 ou v3.1,  
révision externe B, révision interne G**

*Paris, le 11 février 2013*

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

[Original signé]

Patrick Pailloux



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

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

Référence du rapport de certification

**ANSSI-CC-2013/06**

Nom du produit

**Microcontrôleurs sécurisés SA23YL18 et SB23YL18  
incluant la bibliothèque cryptographique NesLib v2.0, v3.0  
ou v3.1, révision externe B, révision interne G**

Référence/version du produit

**Référence maskset K2L0A, révision externe B, révision  
interne G**

Conformité à un profil de protection

**[BSI-PP-0035-2007], version v1.0  
Security IC Platform Protection Profile**

Critères d'évaluation et version

**CC version 3.1 révision 3**

Niveau d'évaluation

**EAL5 Augmenté  
ALC\_DVS.2 et AVA\_VAN.5**

Développeur

**STMicroelectronics  
190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 ROUSSET, France**

Commanditaire

**STMicroelectronics  
190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 ROUSSET, France**

Centre d'évaluation

**SERMA Technologies  
30 avenue Gustave Eiffel, 33608 PESSAC Cedex, France**

Accords de reconnaissance applicables

**CCRA**



**SOG-IS**



**Le produit est reconnu au niveau EAL4.**

## 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. PRÉSENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Identification du produit</i> .....	6
1.2.2. <i>Services de sécurité</i> .....	7
1.2.3. <i>Architecture</i> .....	7
1.2.4. <i>Cycle de vie</i> .....	9
1.2.5. <i>Configuration évaluée</i> .....	11
<b>2. L'ÉVALUATION .....</b>	<b>12</b>
2.1. RÉFÉRENTIELS D'ÉVALUATION .....	12
2.2. TRAVAUX D'ÉVALUATION .....	12
2.3. COTATION DES MÉCANISMES CRYPTOGRAPHIQUES SELON LES RÉFÉRENTIELS TECHNIQUES DE L'ANSSI .....	12
2.4. ANALYSE DU GÉNÉRATEUR D'ALÉAS.....	13
<b>3. LA CERTIFICATION .....</b>	<b>14</b>
3.1. CONCLUSION.....	14
3.2. RESTRICTIONS D'USAGE.....	14
3.3. RECONNAISSANCE DU CERTIFICAT .....	15
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	15
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	15
<b>ANNEXE 1. NIVEAU D'ÉVALUATION DU PRODUIT.....</b>	<b>16</b>
<b>ANNEXE 2. RÉFÉRENCES DOCUMENTAIRES DU PRODUIT ÉVALUÉ .....</b>	<b>17</b>
<b>ANNEXE 3. RÉFÉRENCES LIÉES À LA CERTIFICATION .....</b>	<b>19</b>

# 1. Le produit

## 1.1. Présentation du produit

Les produits évalués sont les microcontrôleurs sécurisés SA23YL18 et SB23YL18 incluant la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1, révision externe B, révision interne G, développés par STMicroelectronics.

Les préfixes SA ou SB des références du produit concernent la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1. La configuration SA (NesLib v2.0, v3.0 et v3.1) ne fournit que des implémentations des algorithmes RSA et SHA. La configuration SB (NesLib v2.0, v3.0 et v3.1) apporte, en plus, des implémentations de l'algorithme AES et de protocoles basés sur la cryptographie des courbes elliptiques (NesLib v2.0, v3.0 et v3.1) ainsi qu'un service de génération de nombres premiers et de clés RSA protégé contre les attaques par canaux auxiliaires (NesLib v3.0 et v3.1).

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,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

## 1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité est strictement conforme au profil de protection [BSI-PP-0035-2007].

### 1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par des éléments d'identification :

- gravés sur le microcontrôleur :
  - identification de la puce (*maskset*) : K2L0 ;
  - référence du logiciel dédié : AKB (séquence de démarrage & initialisation, autotest) ;
  - référence du logiciel embarqué : UBV<sup>1</sup> représentant le *Card Manager*, système d'exploitation de démonstration, embarqué en ROM User dans les échantillons soumis aux tests pour les besoins de l'évaluation seulement. Le *Card Manager* n'entre pas dans le périmètre d'évaluation, voir §1.2.5 ;

<sup>1</sup> Ce trigramme caractérise le logiciel embarqué et est propre à chaque utilisateur *user* car le logiciel embarqué est fourni par le client au commanditaire pour être mis en ROM. Le trigramme présent sur les puces fournies à un client sera donc forcément différent de celui apparaissant sur les microcontrôleurs évalués.

- identification du site de fabrication : ST 4 (Rousset) ;
- présents dans la zone OTP *One Time Programmable* de la mémoire EEPROM (cf. [GUIDES]) :
  - aux adresses C007h et C008h, l'utilisateur peut lire le numéro d'identification du produit, égal à « AC04h » pour les SA/SB23YL18 ;
  - à l'adresse C011h, l'utilisateur peut lire la version interne du produit, égal à « 47h » pour la version G ;
- via l'utilisation de la commande « NesLib\_GetVersion » présente dans une API de NesLib et qui fournit une valeur sur 2 octets (voir [GUIDES]) :
  - « 1310h » pour la version 3.1 de la NesLib ;
  - « 1300h » pour la version 3.0 de la NesLib ;
  - « 1200h » pour la version 2.0 de la NesLib .

### 1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'initialisation de la plate-forme matérielle et des attributs ;
- la gestion sécurisée du cycle de vie ;
- l'intégrité logique du produit ;
- le test du produit ;
- la gestion mémoire (firewall) ;
- la protection physique ;
- la gestion des violations sécuritaires ;
- la non-observabilité des données secrètes pendant les calculs cryptographiques ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support au chiffrement cryptographique à clés asymétriques ;
- le support à la génération de nombres non prédictibles ;
- la bibliothèque cryptographique offrant, suivant la version et la configuration choisies, des implémentations RSA, SHA, AES, ECC et un service de génération de nombres premiers et de clés RSA protégé contre les attaques par canaux auxiliaires.

### 1.2.3. Architecture

Les microcontrôleurs SA23YL18 et SB23YL18 sont constitués des éléments suivants :

- une partie matérielle composée :
  - d'un processeur 8/16-bits ;
  - de mémoires :
    - 18 Ko (dont 128 octets d'OTP) de mémoire EEPROM (avec contrôle d'intégrité) pour le stockage des programmes et des données ;
    - 196 Ko de mémoire ROM pour le stockage des programmes utilisateurs ;
    - 4 Ko de mémoire RAM ;
    - 20 Ko de mémoire ROM pour le stockage des logiciels dédiés (logiciel de test) ;
  - de modules de sécurité : protection des mémoires (MPU), génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, contrôle d'intégrité des mémoires, détection de fautes ;

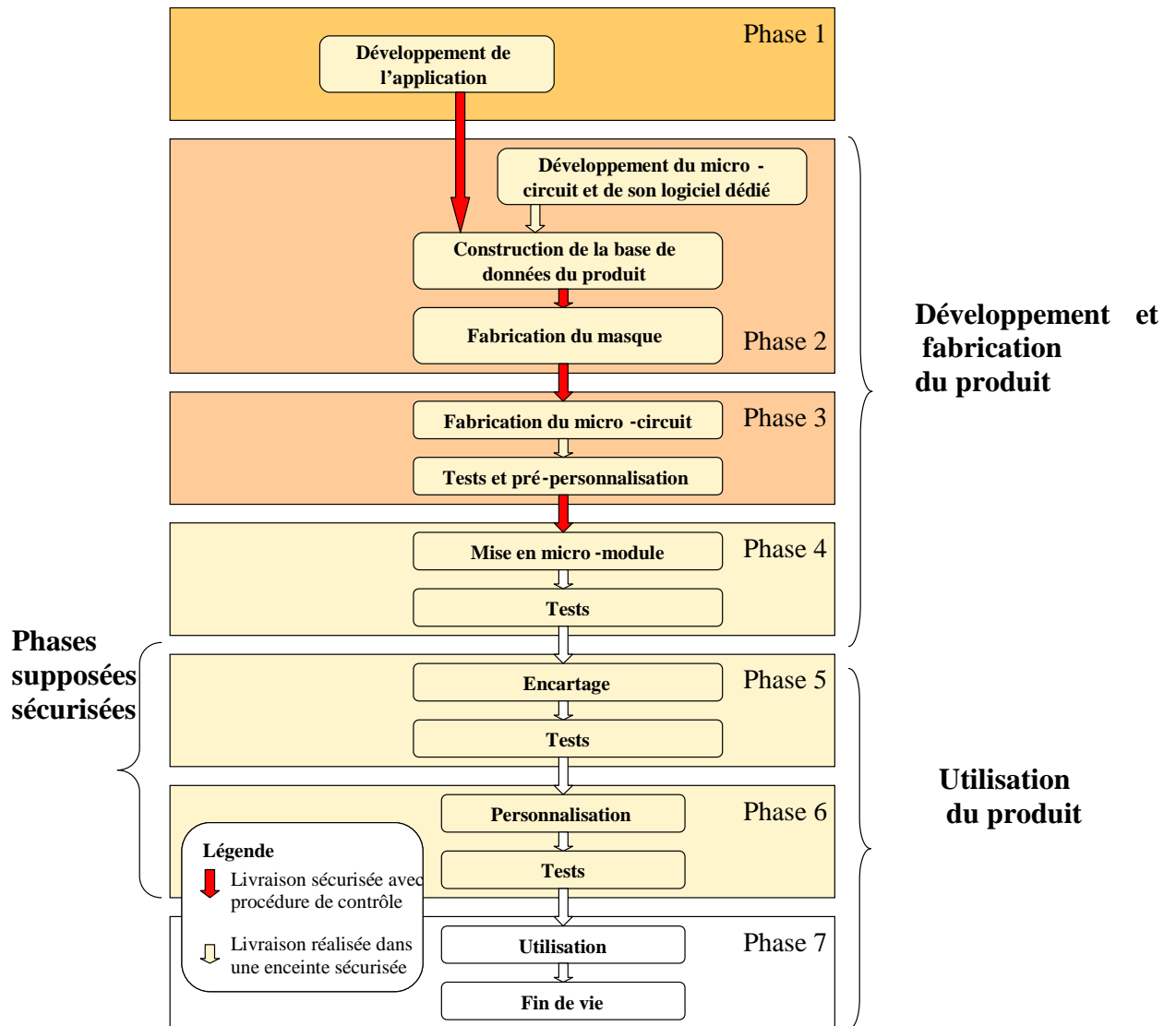
- de modules fonctionnels : 3 compteurs 8-bits, gestion des entrées/sorties en mode contact (IART ISO 7816-3), générateur de nombres aléatoires (TRNG), co-processeur EDES pour le support des algorithmes DES et co-processeur NESCRYPT muni d'une RAM dédiée de 2 Ko pour le support des algorithmes cryptographiques à clé publique ;
- une partie « logiciels dédiés » en ROM intégrant :
  - des logiciels de test du microcontrôleur ;
  - des utilitaires pour la gestion du système et de l'interface matériel/logiciel ;
- une bibliothèque cryptographique (NesLib v2.0, v3.0 ou 3.1) fournissant :
  - des services cryptographiques RSA et SHA, en configuration SA ;
  - des services cryptographiques RSA, SHA, AES, ECC et un service de génération de nombres premiers et de clés RSA protégé contre les attaques par canaux auxiliaires (ce service est contenu uniquement dans les versions 3.0 et 3.1 de la NesLib) en configuration SB.

La bibliothèque est incluse dans la cible de sécurité du produit. Cette bibliothèque est intégrée dans le code client, et est donc embarquée dans la mémoire ROM utilisateur du produit.



### 1.2.4. Cycle de vie

Le cycle de vie du produit dans le cycle global d'une carte à puce est le suivant :



Le développement du produit est réalisé sur les sites suivants (phases 2, 3 et 4) :

<p><b>STMicroelectronics SAS</b></p> <p>Smartcard IC division          190 Avenue Célestin Coq, ZI de Rousset,          BP2          13106 Rousset Cedex          France</p>	<p><b>STMicroelectronics Pte ltd</b></p> <p>5A Serangoon North Avenue 5,          554574 Singapour          Singapour</p>
<p><b>STMicroelectronics</b></p> <p>Excelsiorlaan 44-46,          B-1930 Zaventem,          Belgique</p>	<p><b>STMicroelectronics</b></p> <p>629 Lorong 4/6 Toa Payoh          319521 Singapour          Singapour</p>
<p><b>STS Microelectronics</b></p> <p>16 Tao hua Rd.,          Futian free trade zone,          518048 Shenzhen,          P.R. Chine</p>	<p><b>STMicroelectronics</b></p> <p>7 Loyang drive          508938 Singapour          Singapour</p>
<p><b>STMicroelectronics</b></p> <p>101 Boulevard des Muriers          BP97, 20 180 Casablanca          Maroc</p>	<p><b>DAI NIPPON PRINTING CO., LTD</b></p> <p>2-2-1, Fukuoka, Kamifukuoka-shi,          Saitama-Ken, 356-8507          Japon</p>
<p><b>DAI NIPPON PRINTING EUROPE</b></p> <p>Via C. Olivetti, 2/A,          I-20041 Agrate Brianza,          Italie</p>	<p><b>Smartflex Technologies</b></p> <p>No 27, UBI rd 4,          MSL building #04-04          408618 Singapour          Singapour</p>
<p><b>DISCO Hi-Tec Europe GmbH</b></p> <p>Liebigstrasse 8          D-85551 Kirchheim bei Munchen          Allemagne</p>	<p><b>NEDCARD</b></p> <p>Bijsterhuizen 25-29          6604 LM Wijchen          Pay-Bas</p>
<p><b>GlobalFoundries (Singapore)</b></p> <p>60 Woodlands industrial park,          D street 2, Singapore 738406</p>	

Le produit comporte lui-même une gestion de son cycle de vie, prenant la forme de deux configurations d'utilisation :

- configuration « Test » : à la fin de sa fabrication, le microcontrôleur est testé à l'aide du logiciel de test présent en ROM. Les données de pré-personnalisation peuvent être chargées en EEPROM. Cette configuration est ensuite bloquée de manière irréversible lors du passage en configuration « User » ;
- configuration « User » : mode comprenant trois sous-modes :
  - o mode « *reduced test* », permettant à STMicroelectronics d'effectuer quelques tests restreints ;
  - o mode « *diagnosis* » : sous-ensemble du mode « *reduced test* », réservé à STMicroelectronics ;
  - o mode « *end user* » : mode final d'utilisation du microcontrôleur qui fonctionne alors sous le contrôle du logiciel embarqué de la carte à puce. Le logiciel de test n'est plus accessible. Les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans cette configuration.

### ***1.2.5. Configuration évaluée***

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur, aux logiciels dédiés et à la bibliothèque cryptographique, identifiés au §1.2.1. Toute autre application éventuellement embarquée, notamment les routines embarquées 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 de fabrication, tests et pré-personnalisation (fin de phase 3) ou le produit qui sort de la phase d'assemblage et de test final (fin de phase 4).

Les résultats de cette évaluation s'appliquent au composant ST23LY18 qui ne contient pas la bibliothèque cryptographique NesLib.

## 2. L'évaluation

### 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [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.

Pour répondre aux spécificités des cartes à puce, les guides [CC 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 des « Microcontrôleurs sécurisés SA23YL18B et SB23YL18B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB » certifiés le 29 avril 2010 sous la référence [ANSSI-CC-2009/63].

Le niveau de résistance de ces microcontrôleurs a été confirmé le 27 septembre 2012 dans le cadre du processus de surveillance [SUR-CI].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 janvier 2013, 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

Le produit évalué offre les services de support cryptographique suivants :

- support au chiffrement cryptographique à clés symétriques (EDES) ;
- support au chiffrement cryptographique à clés asymétriques (NESCRIPT) ;
- support à la génération de nombres non prédictibles (TRNG).

Il contient également une bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1 offrant, suivant la configuration choisie, des implémentations RSA, SHA, AES, ECC.

Ces services n'ont pas été analysés vis-à-vis des référentiels techniques de l'ANSSI [REF]. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception ni de construction pour le niveau AVA\_VAN visé.

## 2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation : le générateur est de classe « P2 – *SOF-high* » selon l' [AIS 31].

## 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 les « Microcontrôleurs sécurisés SA23YL18 et SB23YL18 incluant la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1, révision externe B, révision interne G », soumis à l'évaluation répondent aux caractéristiques de sécurité spécifiées dans la cible de sécurité [ST] pour le niveau d'évaluation EAL5 augmenté des composants ALC\_DVS.2 et AVA\_VAN.5.

### 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 des « Microcontrôleurs sécurisés SA23YL18 et SB23YL18 incluant la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1, révision externe B, révision interne G » 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

### 3.3. Reconnaissance du certificat

#### Ce certificat fait l'objet d'une reconnaissance internationale

##### 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 puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. 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 EAL4 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> Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

<sup>2</sup> Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

## Annexe 1. Niveau d'évaluation du produit

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Name of the component
ADV Development	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	Complete semiformal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	4	Semiformal modular design
AGD Guidance	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedure
ALC Life-cycle support	ALC_CMC		2	3	4	4	5	5	4	Production support, acceptance procedures and automation
	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	2	Compliance with implementation standards
ASE Security target evaluation	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claim
	ASE_ECD	1	1	1	1	1	1	1	1	Extended component 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	1	TOE summary specifications
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	2	3	3	4	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing, sample
AVA Vulnerability assessment	AVA_VAN	1	2	2	3	4	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>- Sx23YLxx Security Target référence SMD_Sx23YLxx_ST_09_01, version v1.0 du 10 Septembre 2009.</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>- SA23YL18B / SB23YL18B Security Target - Public Version référence SMD_Sx23YL18_ST_09_001 Rev 03.00, version v3.0 du 1er décembre 2011.</li></ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"><li>- Evaluation Technical Report LAFITE Project référence LAFITE_Sx23YL18G_ETR_v1.1 version v1.1 du 7 janvier 2013.</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>- ETR Lite for Composition Sx23YL18 Project référence LAFITE_Sx23YL18G_ETRLiteComp_v1.0 version v1.0 du 7 janvier 2013.</li></ul>
[CONF]	<p>Liste de configuration :</p> <ul style="list-style-type: none"><li>- Neslib 3.1 Configuration List référence Neslib_3.1_CFGL_11_002_V01.00, version v1.0 du 17 Décembre 2011;</li><li>- Neslib 3.0 Configuration List référence NesLib_3.0_CFGL_09_005_V01.00, version v1.00 du 13 Octobre 2009 ;</li><li>- Neslib 2.0 Configuration List référence Neslib_2.0_CFGL_09_003_V01.00, version v1.00 du 16 Juin 2009 ;</li><li>- SA-SB23YL18 revision interne G Configuration List référence SMD_SA-SB23YL18G_SIA_11_001, version v1.4 du 17 Décembre 2012.</li></ul>

[GUIDES]	Guide d'utilisation du produit : <ul style="list-style-type: none"> <li>- ST23YL18 Smartcard MCU with enhanced security, cryptoprocessor and 18 Kbytes EEPROM - Datasheet référence DS_23YL18 Rev1.0, version V1.0 du 10 Mai 2011 ;</li> <li>- User manual: ST23 MCUs, NesLib 3.1 cryptographic library référence UM_23_NesLib_3.1 Rev2, version V2 du 16 Septembre 2011 ;</li> <li>- User manual: ST23 MCUs, NesLib 3.0 cryptographic library référence UM_23_NesLib_3.0 Rev3, version v3 du 16 Septembre 2011 ;</li> <li>- User manual: ST23 MCUs, NesLib 2.0 cryptographic library référence UM_23_NesLib_2.0 Rev5, version V5 du 8 Février 2012 ;</li> <li>- Application Note: ST23 Platform Security Guidance référence: AN_SECU_23 Rev10, version 10 du 14 Décembre 2012 ;</li> <li>- Addendum Security Guidance: ST23 secure MCUs with AES NesLib security guidance référence AN_23_AES_NesLib Rev1, version v1 du 27 Juin 2012;</li> <li>- ST21/23 programming manual référence PM_21_23 Rev3, version v3 du 20 août 2010 ;</li> <li>- ST23 AIS31 compliant random numbers, User Manual référence UM_23_AIS31 Rev2 version 2 du 18 décembre 2009 ;</li> <li>- ST23 AIS31 Reference implementation Start-up, Online and Total Failure tests référence AN_23_AIS31 Rev2 version 2 du 22 septembre 2009.</li> </ul>
[ANSSI-CC-2009/63]	Microcontrôleurs sécurisés SA23YL18B et SB23YL18B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB certifié le 29 avril 2010 sous la référence ANSSI-CC-2009/63.
[SUR-CI]	Surveillance des produits SA23YL18B et SB23YL18B du 27 septembre 2012.
[BSI-PP-0035-2007]	Protection Profile - Security IC Platform Protection Profile, version v1.0 du 15 juin 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i>

### Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[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 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> . Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), 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 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).