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-2012/77

Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib v3.1

Maskset K2V0A, révision interne B

Paris, le 8 novembre 2012

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

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2012/77

Nom du produit

Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib v3.1

Référence/version du produit

Maskset K2V0A, révision interne B

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

EAL6 Augmenté

ALC_FLR.1

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.

Table des matières

1. Le produit

1.1. Présentation du produit

Les produits évalués sont les microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A en révision interne B, développés par STMicroelectronics. Ils incluent optionnellement la bibliothèque cryptographique NesLib en version 3.1.

Le tableau ci-dessous détaille les caractéristiques de taille mémoire EEPROM et d'interfaces pour les différentes variantes des produits :

Produits	ST23R160	ST23R80A	ST23R48A	ST23L160	ST23L80A	ST23L48A
Taille mémoire EEPROM	160K	80K	48K	160K	80K	48K
Interfaces	Mode « *Dual* » (contact et sans-contact)			Mode contact uniquement		

Remarque : la mémoire est toujours physiquement d'une taille de 160 Ko mais sa capacité est bridée selon les variantes.

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

1.2.1. Introduction

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].

1.2.2. 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 d'identification suivants gravés sur le microcontrôleur :

- K2V0A : nom interne STMicroelectronics du produit, appelé aussi « *Maskset* », le suffixe A identifiant la révision majeure du silicium ;
- AZB : référence identifiant le logiciel dédié appelé aussi OST (« *Operating system for Test* » - système d'exploitation dédié pour le démarrage, les tests et la maintenance du produit) ;
- UZC[1]: référence identifiant le logiciel utilisateur embarqué en ROM « *User* ». Dans le cas présent de l'évaluation, il identifie le système d'exploitation de démonstration STMicroelectronics appelé « *Card Manager* ». Le « *Card Manager* » n'entre pas dans le périmètre d'évaluation, voir §1.2.5 ;
- ST 4 : identification du site de fabrication de Rousset.

Des éléments supplémentaires d'identification sont présents dans la zone OTP (« *One Time Programmable »)* de la mémoire EEPROM (cf. [GUIDES]) aux adresses suivantes :

Adresses	Item	ST23R160	ST23R80A	ST23R48A	ST23L160	ST23L80A	ST23L48A
C007h C008h	Circuit	0019h	001Bh	001Ch	001Dh	001Eh	001Fh
C00Eh	Version OST	4Fh					
C011h	Révision interne	42h[2]					

La librairie cryptographique NesLib peut être identifiée via l'utilisation de la commande « NesLib_GetVersion » présente dans une API de NesLib qui fournit une valeur sur 2 octets (voir [GUIDES]) : « 1310h » pour la version 3.1 de la NesLib.

1.2.3. 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 ;

[1] Ce trigramme identifie le logiciel embarqué et est propre à chaque utilisateur 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.

[2] Code ASCII en hexadécimal du caractère B (révision interne du « *Maskset* »).

- 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 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.

1.2.4. Architecture

Les microcontrôleurs ST23R160/80A/48A et ST23L160/80A/48A sont constitués des éléments suivants (voir figure 1 ci-après):

- une partie matérielle composée :
  - d'un processeur 8/16-bits ;
  - de mémoires :
    - 160/80/48 Ko (selon la version dont 128 octets d'OTP) de mémoire EEPROM (avec contrôle d'intégrité) pour le stockage des programmes et des données ;
    - 390 Ko de mémoire ROM pour le stockage des programmes utilisateur ;
    - 6 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, module de 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, co-processeur AES pour le support des algorithmes AES et co-processeur NESCRYPT muni d'une RAM dédiée de 2 Ko pour le support des algorithmes cryptographiques à clé publique ;
  - pour les microcontrôleurs ST23R160/80A/48A uniquement, d'un module de communication radio-fréquence ISO 14443 type B et B' ;
- 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 v3.1) fournissant 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.

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.

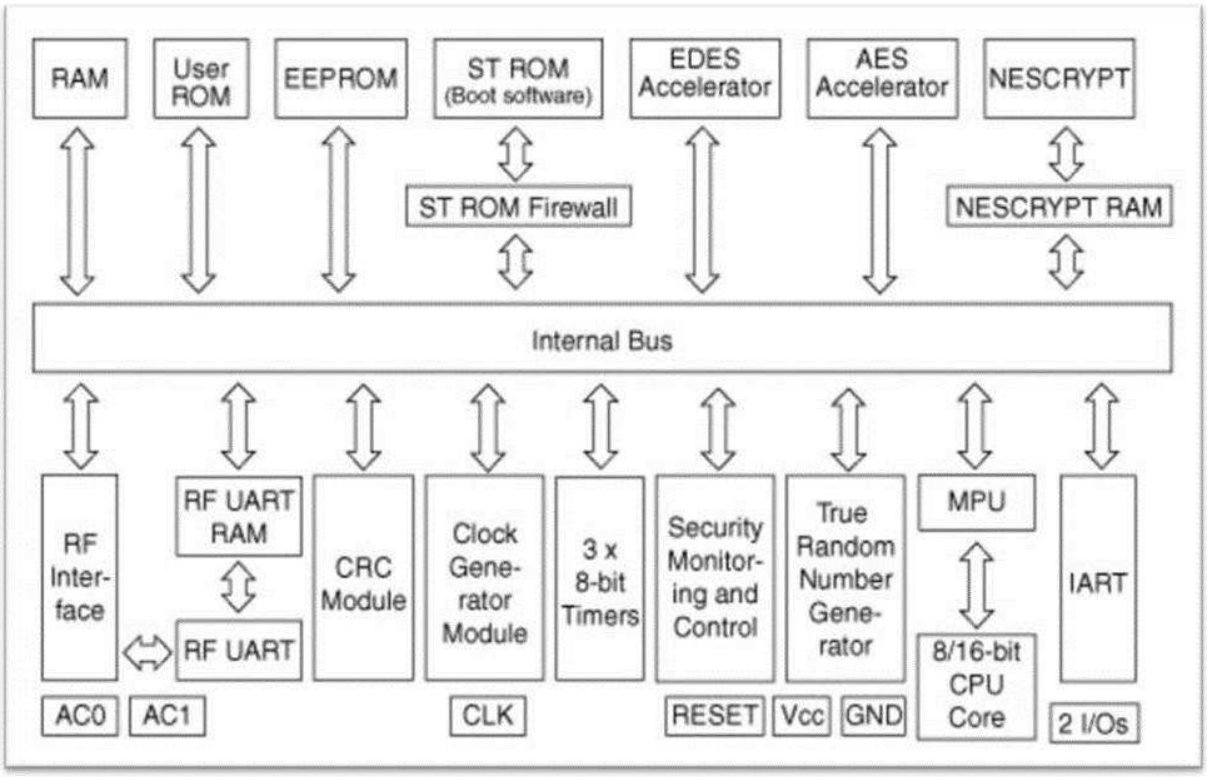

Figure 1. Architecture

1.2.5. Cycle de vie

Le cycle de vie du produit est conforme à celui décrit dans [BSI-PP-0035-2007]. Il est détaillé aux chapitres « 2.3 TOE life cycle » et « 2.4 TOE environment » de la [ST]. Les différentes étapes sont récapitulées dans le tableau suivant :

Phase	***Nom***	***Description***
1	Développement de l'application embarquée	Développement de l'application utilisateur
2	Développement du composant	- Conception du composant - Développement du logiciel dédié OST
3	Fabrication du composant	- Fabrication et intégration du *photomask* - Production du composant - Test du composant - Préparation - Pré-personnalisation
4	*Packaging* du composant	- *Packaging* du composant (et test)
5	Intégration du produit composite	- Process de finalisation du produit composite - Préparation du produit composite - Expédition du produit composite
6	Personnalisation	- Personnalisation du produit composite - Test du produit composite
7	Utilisation	Utilisation du produit composite par ses émetteurs et utilisateurs finaux

La présente évaluation a couvert les phases 2, 3 et 4 du cycle de vie.

L'évaluation a également couvert les procédures de livraison et de vérification de l'application développée en phase 1, ainsi que les procédures de livraison de la TOE à l'entité chargée du packaging du composant intervenant en phase 4. Les procédures correspondant aux autres phases sont en dehors du périmètre de cette évaluation.

La TOE est toujours livrée en mode « *End User* » :
- soit sous forme de « *wafer* », éventuellement scié, en fin de phase 3 ;
- soit sous une forme packagée en fin de phase 4.

Le produit est conçu, développé, intégré (préparation de la base de données du produit), fabriqué et testé par :

STMicroelectronics SAS (Rousset/France),

SMD division, 190 Avenue Célestin Coq, ZI,
13106 Rousset Cedex,
France.

Une partie du développement du produit est réalisée par :

STMicroelectronics Pte ltd (Ang Mo Kio/Singapour),

5A Serangoon North Avenue 5,
554574, Singapore,
Singapour.

STMicroelectronics (Zaventem/Belgique),

Excelsiorlaan 44-46,
B-1930 Zaventem,
Belgique.

Le produit peut également être testé par :

STMicrolectronics (Toa Payoh/Singapour),

629 Lorong 4/6 Toa Payoh,
319521, Singapore,
Singapour.

Les réticules du produit sont fabriqués par :

DAI NIPPON PRINTING CO., LTD (DNP/Japon),

2-2-1, Fukuoka, kamifukuoka-shi,
Saitama-Ken, 356-8507,
Japon.

DAI NIPPON PRINTING EUROPE (DPE/Italie),

Via C. Olivetti, 2/A,
I-20041 Agrate Brianza,
Italie.

Le produit peut être mis en module ou en boitier par :

STMicroelectronics SA (Bouskoura/Maroc),

101, boulevard des Muriers BP 97,
20180, Bouskoura – Casablanca,
Maroc.

SMARTFLEX TECHNOLOGIES (Singapour),

20, tampines St 92,
528875 Singapore,
Singapour.

NEDCARD BV (Pays-bas),

Bijsterhuizen 25-29,
6604 LM Wijchen,
Pays-Bas.

Le produit peut être scié ou aminci par :

DISCO HI-Tec Europe GmbH (Allemagne),
Liebigstasse 8,
D-85551Kirchheim bei Munchen,
Allemagne.

STS Microelectronics (China),
16 Tao hua Rd., Futian free trade zone,
Shenzhen 518048,
P.R. China.

Le produit peut être stocké et expédié par les sites suivants :

STMicroelectronics SAS (Rousset/France),

SMD division, 190 Avenue Célestin Coq, ZI,
13106 Rousset Cedex,
France.

STMicroelectronics SA (Bouskoura/Maroc),

101, boulevard des Muriers BP 97,
20180, Bouskoura – Casablanca,
Maroc.

STMicroelectronics (Loyang, Singapore),

7 Loyang drive,
Singapore 508938,
Singapour.

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit le développeur de l'application utilisateur à embarquer dans le microcontrôleur (il n'y a pas de rôle « administrateur » défini dans le produit).

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 en phase 3, 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 » :* ce mode, activé en fin de phase 3, comprend trois sous-modes :

- mode « *reduced test* » permettant à STMicroelectronics d'effectuer quelques tests restreints ;
- mode « *diagnosis* » : sous-ensemble du mode « *reduced test* », il est réservé à STMicroelectronics ;
- 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.

1.2.6. Configuration évaluée

Le certificat porte sur la TOE définie plus haut au chapitre « 1.2.4.Architecture » et configurée en mode « *end user* ».

Pour les besoins de l'évaluation, les échantillons de la TOE livrés à l'évaluateur embarquaient dans la ROM un système d'exploitation dit « *Card Manager* », identifié par le trigramme UZC, et dont l'objet était de permettre :

- l'interaction avec la TOE au travers de commandes passées par l'I/O ;
- le chargement en EEPROM, ou en RAM, d'applications de tests.

Ce « *Card Manager* » ne fait 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 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 ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [CC 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 produits :

- « Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB » qui ont été certifiés par l'ANSSI (voir [ANSSI-CC-2010_02]) ;
- « Microcontrôleurs sécurisés SA23YR18A et SB23YR18A, incluant la bibliothèque cryptographique Neslib V3.1 en configuration SA ou SB » qui ont été certifiés par l'ANSSI (voir [ANSSI-CC-2011_06]) .

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 septembre 2012, 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 vulnérabilités de conception et de construction pour le niveau AVA_VAN 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.
Le générateur atteint le niveau « P2 – SOF High».

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 produits « Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib v3.1 » soumis à l'évaluation répondent aux caractéristiques de sécurité spécifiées dans la cible de sécurité [ST] pour le niveau d'évaluation EAL6 augmenté du composant ALC_FLR.1.

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 produits « Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib v3.1 » 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 un de ces micro-circuits 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[1], 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[2], 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 :

[1] 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.

[2] 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

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	Implementation representation of the TSF
	ADV_INT					2	3	3	3	Well-structured internals
	ADV_SPM						1	1	1	Formal TOE security policy model
	ADV_TDS		1	2	3	4	5	6	5	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	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								1	Basic flaw remediation
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	3	Compliance with implementation standards
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	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	3	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	2	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 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *ST23R160, ST23R80A, ST23R48A, ST23L160, ST23L80A, ST23L48A, all with optional cryptographic library NESLIB 3.1 Security Target*, Référence : SMD_ST23xxxx_ST_10_001_V02.01, *July 2011*, STMicroelectronics. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *ST23R160B, ST23R80AB, ST23R48AB, ST23L160B, ST23L80AB, ST23L48AB, all with optional cryptographic library NESLIB 3.1 Security Target - Public Version*, Référence : SMD_ST23RLxxx_ST_11_001 Rev 01.00, *July 2011*, STMicroelectronics.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report – STR160 Project*, Référence : LAFITE_ST23R160B_ETR_v2.1/2.1, 24 septembre 2012, Serma Technologies. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *ETR Lite for Composition – ST23R160 Project*, Référence : LAFITE_ST23R160B_ETRLiteComp_v2.1/2., 24 septembre 2012, Serma Technologies.
[CONF]	Liste de configuration des produits : - *ST23R160, ST23R80A, ST23R48A, ST23L160, ST23L80A, ST23L48A products - Configuration list*, Référence : SMD_ST23R160_CFGL_11_001 V02.00, STMicroelectronics. Liste de la documentation : - *ST23R160 (and derivatives) EAL6+ documentation report*, Référence *: SMD_ST23R160_DR_10_001 V1.1* STMicroelectronics.
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : - *ST23R160, ST23R80A, ST23R48A, ST23L160, ST23L80A, ST23L48A – Datasheet*, Référence : DS_23R160 Rev 1.0, STMicroelectronics. - *ST23 Platform - Security Guidance*, Référence : AN_SECU_23 Rev 9, STMicroelectronics. - *Application Note ST23Rxxx: recommendations for contactless operations*, Référence : AN_23R160_RCMD_CL_Rev1,

	STMicroelectronics. - *User Manual of NesLib 3.1*, Référence : UM_23_NesLib Rev 1, STMicroelectronics. - *ST23Rxxx/ST23Lxxx security guidance*, Référence : AN_23R160_SECU Rev2, STMicroelectronics. - *ST23secure MCUs with AES NesLib security guidance*, Référence : AN_23_AES_NesLib Rev1, STMicroelectronics. - *ST23R160 OST User Manual (full and reduced test configuration)*, Référence : PEN_ST23_UM_10_001, STMicroelectronics. - *ST23 AIS 31: Compliant Random Number – User Manual*, Référence UM_23_AIS31, v2.0, STMicroelectronics. - *ST23 AIS 31: Reference Implementation - StartUp, Online and Total Failure Tests*, Référence AN_23_AIS31, v2.0, STMicroelectronics.
[2010/02]	Rapport de certification ANSSI-CC-2010/02, Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, 10 février 2010, ANSSI.
[2011/06]	Rapport de certification ANSSI-CC-2011/06, Microcontrôleurs sécurisés SA23YR18A et SB23YR18A, incluant la bibliothèque cryptographique Neslib V3.1 en configuration SA ou SB, 8 septembre 2011, ANSSI.
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

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 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.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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, voir www.ssi.gouv.fr.
	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, voir www.ssi.gouv.fr.
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).