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-2012/68

Microcontrôleurs sécurisés SA23YR80/48 et SB23YR80/48, incluant la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1, en configuration SA ou SB

Référence : maskset K2M0A, révision externe B, révision interne H ou I

Paris, le 04 janvier 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 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-2012/68

Nom du produit

Microcontrôleurs sécurisés SA23YR80/48 et SB23YR80/48, incluant la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1, en configuration SA ou SB

Référence/version du produit

Référence maskset K2M0A,
révision externe B, révision interne H ou I

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 SA23YR80/48 et SB23YR80/48 révision externe B, révision interne H ou I développés par STMicroelectronics. Ils incluent la bibliothèque cryptographique NesLib dans l'une des versions v2.0, v3.0 ou v3.1, en configuration SA pour les produits SA23YR80/48 et en configuration SB pour les produits SB23YR80/48.

Le préfixe SA ou SB des références du produit concerne la bibliothèque cryptographique Neslib v2.0, v3.0 ou v3.1. La configuration SA (Neslib v2.0) fournit des implémentations des algorithmes RSA et SHA, alors que la configuration SB (Neslib v3.0 et 3.1) apporte, en plus, des implémentations de l'algorithme AES et de protocoles basés sur des courbes elliptiques ainsi qu'un service de génération de nombres premiers et de clés RSA protégé contre les attaques par canaux auxiliaires.

Le suffixe « 80/48 » exprime la taille (logique) de la mémoire EEPROM attribuée (80 Ko ou 48 Ko), sachant que la mémoire est toujours physiquement d'une taille de 80 Ko mais que seulement 48 Ko sont accessibles dans les produits SA/SB23YR48.

La version interne H correspond à la version du produit fonctionnant en mode "Dual" RF et contact, ou RF uniquement. La version I correspond à la version du produit fonctionnant en mode contact seulement.

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*) : « K2M0AHB » ou « K2M0AIB » ;

  - référence du logiciel dédié : « ANC » (séquence de démarrage & initialisation, autotest) ;
  - référence du logiciel embarqué : « UBT[1] » 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 ;
- 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 « B214h » pour les SA23YR80/48 et SB23YR80/48 ;
  - à l'adresse « C011h » l'utilisateur peut lire la révision interne du produit, égale à :
    - « 48h » pour la version H ;
    - « 49h » pour la version I ;
- 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 SA23YR80/48 et SB23YR80/48 sont constitués des éléments suivants :

- une partie matérielle composée :
  - d'un processeur 8/16-bits ;
  - de mémoires :

[1] Ce trigramme caractérise le logiciel embarqué et 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.

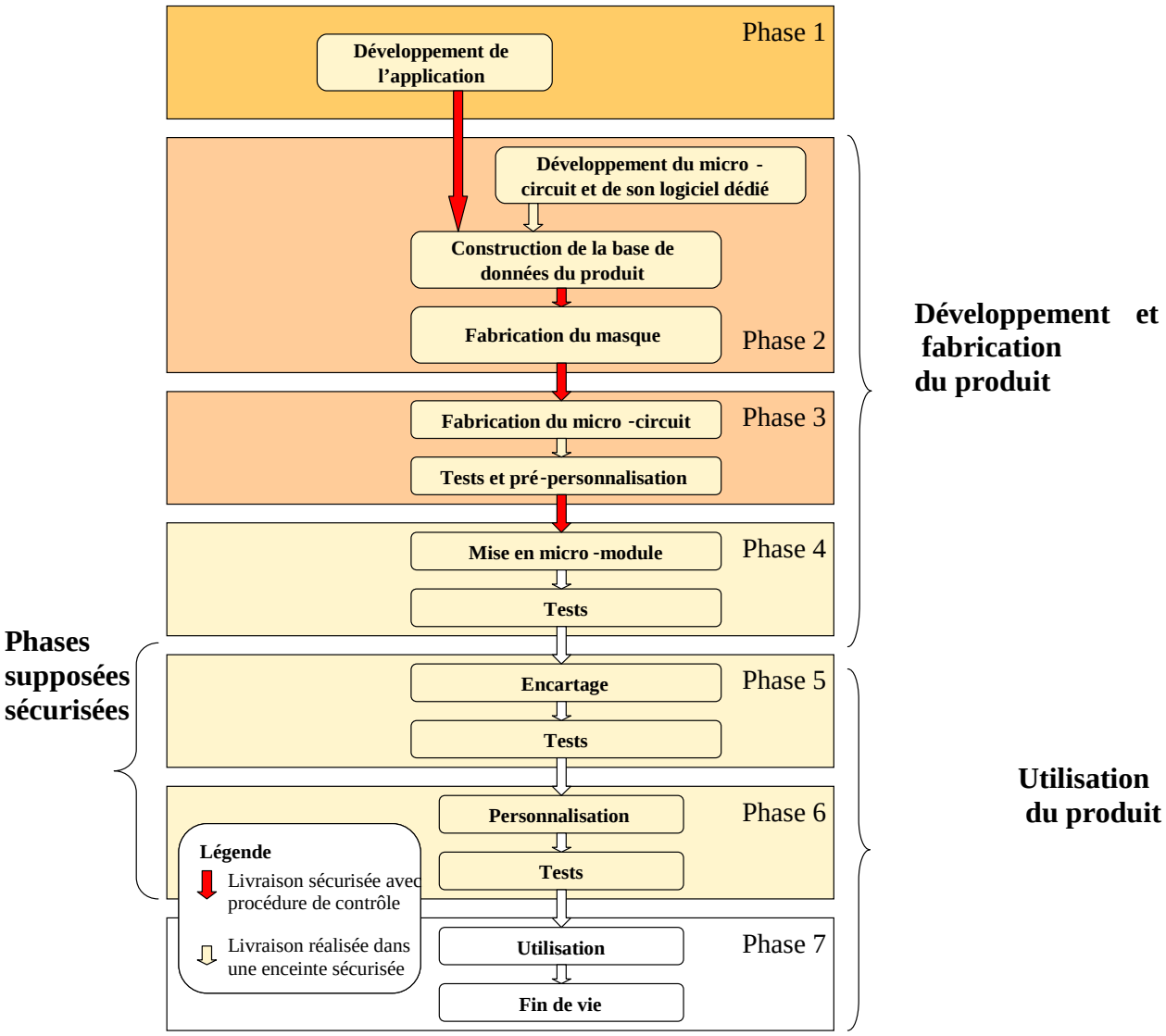
        - 80 Ko[1] (dont 128 octets d'OTP) de mémoire EEPROM avec contrôle d'intégrité pour le stockage des programmes et des données ;
        - 390 Ko de mémoire ROM pour le stockage des programmes utilisateurs ;
        - 6 Ko de mémoire RAM ;
        - 20 Ko de mémoire ROM pour le stockage des logiciels 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, gestion des entrées/sorties en mode contact (IART ISO 7816-3) ou sans contact (ISO14443-B), 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] Selon la version commerciale du produit, 80 Ko ou 48 Ko sont accessibles.

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) :

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

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

1.2.5. 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) ainsi que le produit qui sort de la phase d'assemblage (fin de phase 4).

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 [JIWG 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 du produit « Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB » certifié le 10 février 2010 sous la référence [ANSSI-CC-2010/02].

Le niveau de résistance du microcontrôleur 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 20 décembre 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

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 (NESCRYPT) ;
- 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 le produit « Microcontrôleurs sécurisés SA23YR80/48 et SB23YR80/48, incluant la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1, en configuration SA ou SB », référence maskset K2M0A, révision externe B, révision interne H ou I, version soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL6 augmenté de 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 du produit « Microcontrôleurs sécurisés SA23YR80/48 et SB23YR80/48, incluant la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1, en configuration SA ou SB » 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[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 semiformal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**2**	Complete mapping of the implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**3**	Minimally complex internals
	ADV_SPM						**1**	1	**1**	Formal TOE security policy model
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**5**	Complete semiformal modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedure
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**5**	Advanced support
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ADO_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 – all parts
ASE Evaluation de la cible de sécurité	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	**3**	Rigorous analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**3**	Testing: modular design
	ATE_FUN		**1**	1	1	1	**2**	2	**2**	Ordered 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 : - ST23YR48, SB23YR48, ST23YR80, SB23YR80 Security Target référence SMD_Sx23Yrxx_ST_09_001, version 1 du 13 août 2008. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B Security Target – Public Version référence SMD_Sx23Yrxx_ST_09_002, version v3.0 du 22 mars 2011.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report LAFITE Project référence LAFITE_Sx23YR80H-I_ETR_v1.0, version v1.0 du 20 décembre 2012. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ETR Lite for Composition Sx23YR80/48 Project référence LAFITE_Sx23YR80H-I_ETRLiteComp_v1.0, version v1.0 du 20 décembre 2012.
[CONF]	Liste de configuration : - Neslib 2.0 on ST23YR80 configuration list référence Neslib_2.0_CFGL_09_002_V01.01, version v1.01 du 26 mars 2009 ; - Neslib 3.0 on ST23YR80 configuration list référence NesLib_3.0_CFGL_09_003_V01.01, version v1.01 du 22 septembre 2009 ; - Neslib 3.1 on ST23YR80 Configuration List référence Neslib_3.1_CFGL_11_004_V01.00, version v1.0 du 17 Janvier 2012 ; - SA-SB23YR80/48 rev interne H et I Configuration List référence SMD_ST-SA-SB23YR80H-I_SIA_12_001, version v1.0 du 3 Décembre 2012.

[GUIDES]	Guide d'installation du produit : - Data sheet ST23YR48 référence DS23YR48 rev1, version 1 du 26 mars 2010 ; - Data sheet ST23YR80 référence DS23YR80 rev2, version 2 du 8 juin 2010 ; - User manual: ST23 MCUs, NesLib 2.0 cryptographic library référence UM_23_NesLib_2.0 Rev5, version V5 du 8 février 2012 ; - User manual: ST23 MCUs, NesLib 3.0 cryptographic library référence UM_23_NesLib_3.0 Rev3, version v3 du 16 septembre 2011 ; - User manual: ST23 MCUs, NesLib 3.1 cryptographic library référence UM_23_NesLib_3.1 Rev2, version V2 du 16 septembre 2011 ; - ST23Y platform security guidance AN_SECU_23 Rev10, version 10 du 14 décembre 2012 ; - Addendum to Security Guidance Application note: ST23 Secure MCUs with AES Neslib référence: AN_23_AES_Neslib rev 1 du 27 Juin 2012 ; - Application Note – ST23YR80/48 recommandations for contactless operation référence AN_23YR80_RCMD rev 4, version 4 du 19 janvier 2010 ; - ST21/23 programming manual référence PM_21_23 Rev3, version v3 du 20 août 2010 ; - ST23 AIS31 compliant random numbers, User Manual référence UM_23_AIS31 Rev2 version 2 du 18 décembre 2009 ; - ST23 AIS31 Reference implementation Start-up, Online and Total Failure tests référence AN_23_AIS31 Rev2 version 2 du 22 septembre 2009.
[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 certifié le 10 février 2010 sous la référence ANSSI-CC-2010/02.
[SUR-CI]	Surveillance du produit ST23YR80/48 du 27 septembre 2012.
[BSI-PP-0035-2007]	Protection Profile - Security IC Platform Protection Profile, version v1.0 du 15 juin 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 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 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 (RGS_B_2), 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).