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-2010/08

Microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB

Paris, le 8 mars 2010

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-2010/08

Nom du produit

Microcontrôleurs sécurisés SA23ZL48/34/18A et SB23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB

Référence/version du produit

SA23ZL48/34/18A et SB23ZL48/34/18A en révision A (logiciel dédié ASD, maskset K320ACA), incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB

Conformité à un profil de protection

BSI-PP-0035-2007 version 1.0

Security IC Platform Protection Profile v1.0, 15 June 2007

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 5 augmenté

AVA_DVS.2, AVA_VAN.5

Développeur

STMicroelectronics

Smartcard IC division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France

Commanditaire

STMicroelectronics

Smartcard IC division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

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, publié au Journal officiel de la République française. 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 SA23ZL48, SA23ZL34, SA23ZL18, SB23ZL48, SB23ZL34 et SB23ZL18 en révision A (logiciel dédié ASD, *maskset* K320ACA), développés par STMicroelectronics. Ils incluent la bibliothèque cryptographique NesLib dans l'une des versions v2.0 ou v3.0, en configuration SA pour les produits SA23ZL48/34/18A et en configuration SB pour les produits SB23ZL48/34/18A.

La seule différence entre les produits SA/SB23YR48A, SA/SB23ZL34A et SA/SB23ZL18A réside dans la taille (logique) de la mémoire EEPROM attribuée (48 Ko ou 34 Ko ou 18 Ko) attribuée, sachant que la mémoire est toujours physiquement d'une taille de 48 Ko mais que seulement 34 Ko ou 18 Ko sont accessibles dans les produits SA/SB23ZL34A ou SA/SB23ZL18A.

La seule différence entre les produits SA23ZL48/34/18A et SB23ZL48/34/18A ne concerne que la configuration SA ou SB de la bibliothèque cryptographique Neslib v2.0 ou v3.0. La configuration SA fournit des implémentations des algorithmes RSA et SHA, alors que la configuration SB apporte en plus des implémentations des algorithmes AES et ECC. Seule la version v3.0 de la bibliothèque Neslib, en configuration SB, offre en plus un service (SKG) de génération sûre de nombres premiers et clés RSA, pour les produits SB23ZL48/34/18A.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger un ou plusieurs logiciels applicatifs. 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 évalué

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

Cette cible de sécurité est strictement conforme au profil de protection [PP0035].

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*) : K320ACA ;
  - référence du logiciel dédié : ASD (séquence de *boot & reset*, autotest) ;

  - référence du logiciel embarqué : UBX[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, cf. §1.2.5 ;
  - 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 0001h pour les SA/SB23ZL48[2].
- via l'utilisation de la commande « NesLib_GetVersion » présente dans une API de NesLib et qui fournit une valeur sur 2 octets : 0x1300 pour v3.0 ou 0x120a[3] pour la v2.0. (cf. [Guides]).

A ce niveau, il n'existe pas d'éléments d'identification différentiant la Neslib configuration SA de la NesLib configuration SB car ces configurations ne seront réellement intégrées et différenciées qu'avec le logiciel du client qui sera mis en ROM.

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 ;
- 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 (SKG) de génération sûre de nombres premiers et clés RSA.

1.2.3. Architecture

Les microcontrôleurs SA/SB23ZL48/34/18A sont constitués des éléments suivants :

- une partie matérielle composée :
  - d'un processeur 8/16-bits ;
  - de mémoires :
    - 48 Ko (dont 128 octets d'OTP) de mémoire EEPROM (avec contrôle d'intégrité) pour le stockage des programmes et des données ;
    - 300 Ko de mémoire ROM pour le stockage des programmes utilisateurs ;
    - 6 Ko de mémoire RAM ;

[1] 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.
[2] Ce serait 000Ch pour SA/SB23ZL34 et 000Bh pour SA/SB23ZL18.
[3] « a » pouvant prendre des valeurs différentes suivant la documentation associée.

        - 20 Ko de mémoire ROM pour le stockage des logiciels dédiés (logiciel de test).
    - de modules de sécurité : unité de protection des mémoires (MPU), générateur 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 hardware/software.
- une bibliothèque cryptographique (NesLib v2.0 ou v3.0) fournissant :
    - des services cryptographiques RSA et SHA, en configuration SA ;
    - des services cryptographiques RSA, SHA, AES, ECC et un service SKG (contenu uniquement dans la Neslib v3.0) de génération sûre de nombres premiers et clés RSA, 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 développement est résumé dans le schéma suivant :

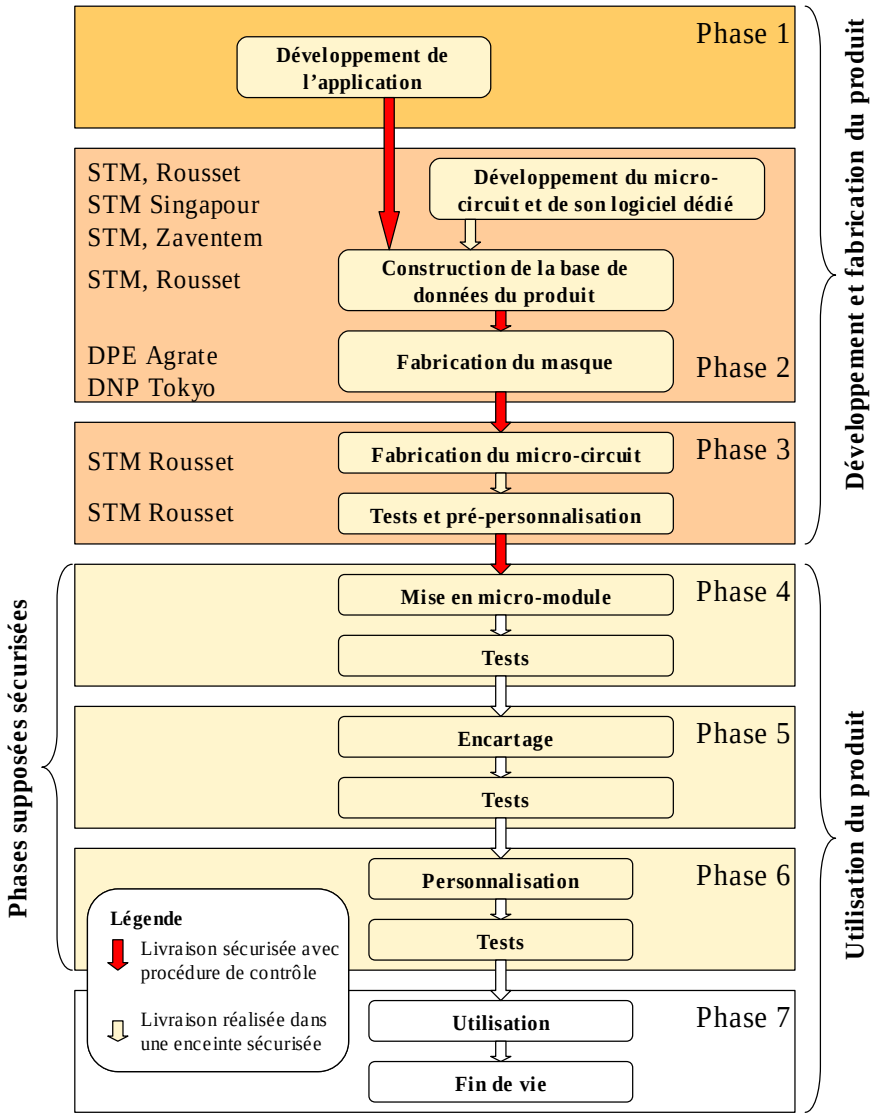

Figure 1 - Cycle de vie standard d'une carte à puce

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

STMicroelectronics SAS

Smartcard IC division
190 Avenue Célestin Coq, ZI de Rousset, BP2
13106 Rousset Cedex
France

Une partie du développement du produit est réalisée par :

STMicroelectronics Pte ltd

5A Serangoon North Avenue 5,
554574 Singapore.
Singapour

et par :

STMicroelectronics

Excelsiorlaan 44-46,
B-1930 Zaventem,
Belgique

Les réticules du produit sont fabriqués par :

DAI NIPPON PRINTING CO., LTD

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

et par :

DAI NIPPON PRINTING EUROPE

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

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 (phase 3).
Pour les besoins de l'évaluation, seuls les microcontrôleurs SB23ZL48A, SB23ZL34A et SB23ZL18A (en révision interne C), munis de la bibliothèque cryptographique Neslib v3.0,

ont été fournis au centre d'évaluation, avec un système d'exploitation logiciel dédié, dans un mode dit « ouvert[1] ».
L'évaluateur précise clairement au chapitre 5.3 du *ETR lite* [RTE] que les résultats de l'évaluation peuvent être généralisés aux composants ST23ZL48/34/18A[2].

[1] Mode permettant de charger et d'exécuter du code natif en EEPROM et de déconnecter les mécanismes sécuritaires paramétrables.
[2] Composants qui ne prennent pas en compte la bibliothèque cryptographique Neslib v3.0

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, 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.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 4 mars 2010, 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).

Ces services ne peuvent cependant pas être analysés vis-à-vis des référentiels techniques de l'ANSSI [REF-CRY], [REF-CLE] et [REF-AUT], car ils ne concourent pas à la sécurité propre du produit ; leur résistance dépendra de leur emploi par l'application embarquée sur le microcircuit.

Les produits SA/B23ZL48/34/18A contiennent également une bibliothèque cryptographique Neslib v2.0 ou v3.0. La cotation des mécanismes cryptographiques offerts par cette bibliothèque, selon les référentiels techniques [REF-CRY], [REF-CLE] et [REF-AUT], n'a pas été réalisée par l'ANSSI. 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 [AIS31] par le centre d'évaluation : le générateur est de classe « P2 – *SOF-high* » selon l' [AIS31].

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 SA/B23ZL48/34/18A, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB, soumis à l'évaluation, répondent aux caractéristiques de sécurité spécifiées dans la cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté.

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 SA/B23ZL48/34/18A 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 microcircuit 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] au chapitre 5.2 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 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. 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'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

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[1], 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 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]	Cible de sécurité de référence pour l'évaluation : - Sx23ZLxxA Security Target, Référence : SMD_Sx23ZLxx_ST_09_001, v01.00, STMicroelectronics Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Sx23ZLxxA Security Target - Public Version, Référence : SMD_Sx23ZLxx_ST_09_002, v01.00, STMicroelectronics
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - LAFITE Project, Référence : LAFITE_SB23ZL48A_ETR_v1.2 / 1.2, 4 Mars 2010, 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 – LAFITE Project, Référence: LAFITE_SB23ZL48A_ETRLiteComp_v1.2/ 1.2, 4 Mars 2010, Serma Technologies
[CONF]	Liste de configuration des produits : - Configuration list SA/SB23ZL48/34/18 (internal version C), Référence : SMD_STSB23ZL48_CFGL_09_001 rev 2.0, STMicroelectronics Liste de la documentation : - documentation report, Référence : SMD_STSB23ZL48_DR_09_001_v1.0, STMicroelectronics. Liste de configuration de la bibliothèque NesLib v3.0 : - Neslib 3.0 configuration list Référence : NesLib_3.0_CFGL_09_004_V01.00 STMicroelectronics.
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : - ST23ZL48 Datasheet, Référence : DS_23ZL48 Rev 0.4, STMicroelectronics - ST23ZL34 Datasheet, Référence : DS_23ZL34 Rev 0.2, STMicroelectronics - ST23ZL18 Datasheet, Référence : DS_23ZL18 Rev 0.2, STMicroelectronics

	- ST23Z Platform - Security Guidance, Référence : AN_SECU_23Z Rev 2, STMicroelectronics - ST23 Reference Implementation User Manual, Référence : UM_23_RefImp Rev 18, STMicroelectronics - ST21/23 programming manual Référence : PM_21_23/0709 Rev 1, STMicroelectronics - User Manual of Neslib 2.0 library, Référence : UM_NesLib_2.0 Rev 2, STMicroelectronics - User Manual of Neslib 3.0 library, Référence : UM_NesLib_3.0 Rev 1, STMicroelectronics - NesLib 3.0: using the dispatcher, Reference : PTD_NesLib_TN_09_018_v01.01, STMicroelectronics - Porting code from ST23Y to ST23Z devices, Référence : AN_23_Porting Rev 3, STMicroelectronics
[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-CC-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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2,ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, ref CCMB-2007-09-004, revision 2.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5, revision 1, April 2008.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.11 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-CLE]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-AUT]	Authentification - Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, v0.13 du 12 avril 2007, réf: 729/SGDN/DCSSI/SDS.
[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)