PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2009/27

Microcontrôleur sécurisé SB23YR48A incluant la bibliothèque cryptographique NesLib v2.0 en configuration SB

Paris, le 1er décembre 2009

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 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-2009/27

Nom du produit

Microcontrôleur sécurisé SB23YR48A incluant la bibliothèque cryptographique NesLib 2.0 en configuration SB

Référence/version du produit

SB23YR48 révision A (logiciel dédié ANC, maskset K2M0ADB) incluant la bibliothèque cryptographique NesLib v2.0 en configuration SB

Conformité à un profil de protection

BSI-PP-0035-2007 version 1.0

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 5 augmenté

ALC_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 :

- La direction centrale 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

Le produit évalué est le microcontrôleur sécurisé SB23YR48 en révision A (logiciel dédié ANC, *maskset* K2M0ADB) incluant la bibliothèque cryptographique NesLib révision 2.0 en configuration SB (RSA, SHA, AES, ECC), développés par STMicroelectronics.

La partie matérielle et les logiciels dédiés sont identiques à ceux du ST23YR48A certifié sous la référence ANSSI-CC-2009/26. Le produit SB23YR48A comporte en plus la bibliothèque cryptographique NesLib révision 2.0 en configuration SB. La seule différence entre ce produit SB23YR48A et le produit SB23YR80A, certifié par ailleurs sous la référence ANSSI-CC-2009/28, ne concerne que la taille de la mémoire EEPROM.

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 les éléments suivants :

- identification de la puce (*maskset*) : K2M0ADB ;
- référence de la bibliothèque cryptographique : NesLib révision 2.0 (configuration SB);
- référence du logiciel dédié : ANC (séquence de *boot & reset*, autotest) ;
- référence du logiciel embarqué : UBR (le *Card Manager* est un système d'exploitation de démonstration, embarqué en ROM *User* dans les échantillons soumis aux tests pour les besoins de l'évaluation seulement, car le *Card Manager* ne rentre pas dans le périmètre d'évaluation) ;
- identification du site de fabrication : ST 4 (Rousset).

Ces éléments d'identification sont gravés sur la puce et visibles au microscope. De plus deux octets dans la zone OTP (*One Time Programmable*) de la mémoire EEPROM permettent d'identifier logiquement le produit, comme indiqué dans le document « *Datasheet* » (cf. [GUIDES]). La bibliothèque NesLib dispose d'une API permettant d'interroger sa version, comme indiqué dans son guide « *User Manual* » (cf. [GUIDES]).

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 des implémentations RSA, SHA, AES, ECC.

1.2.3. Architecture

Le microcontrôleur SB23YR48A est constitué 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 ;
    - 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.
  - 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, la gestion des entrées/sorties en mode contact (IART ISO 7816-3) et sans-contact (RF UART ISO14443B), un générateur de nombres aléatoires (TRNG), le co-processeur EDES pour le support des algorithmes DES et le 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 tests du microcontrôleur ;
  - des utilitaires pour la gestion du système et de l'interface hardware/software ;
- une bibliothèque cryptographique (NesLib) fournissant des implémentations des fonctions cryptographiques RSA, SHA, AES et ECC (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 :

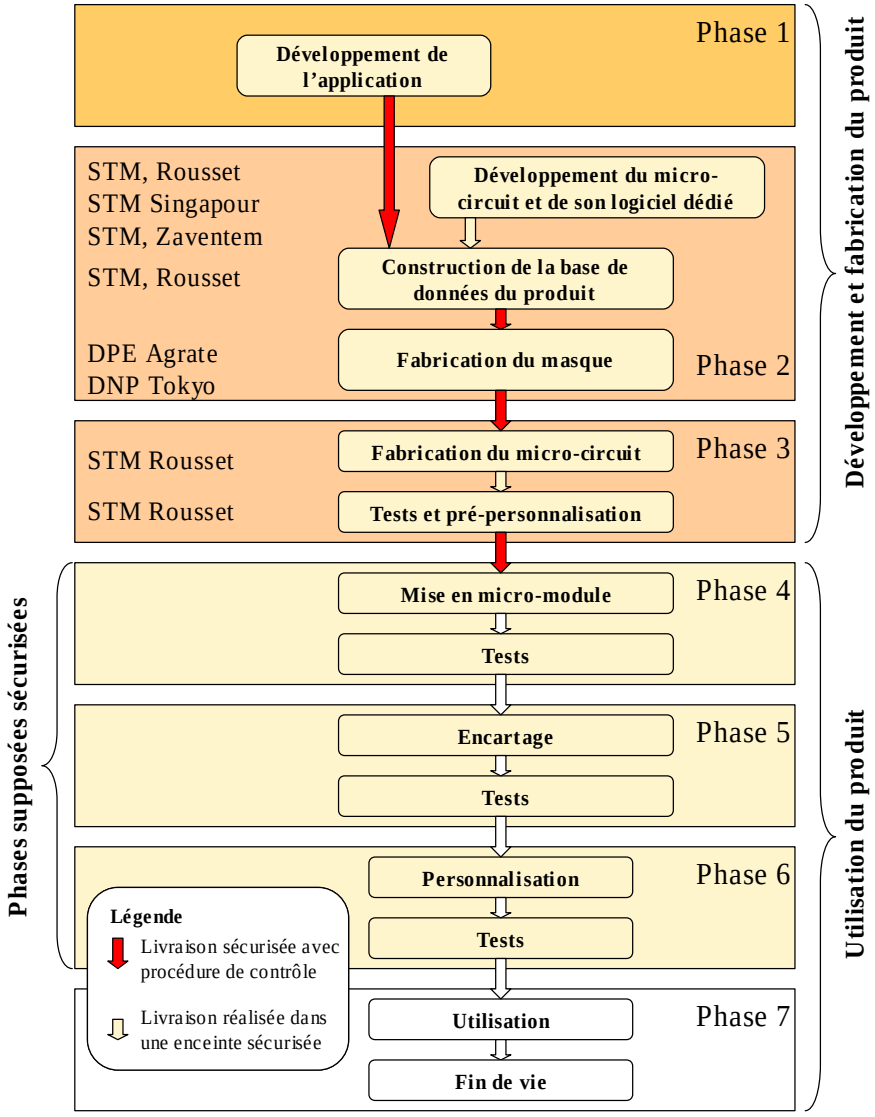

Figure 1 - Cycle de vie standard d'une carte à puce

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 » : comprenant trois 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.
En 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, le microcontrôleur SB23YR48A a été fourni au centre d'évaluation avec un système d'exploitation logiciel dédié, dans un mode dit « ouvert[1] ».

[1] Mode permettant de charger et d'exécuter du code natif en EEPROM et de déconnecter les mécanismes sécuritaires paramétrables.

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

L'évaluation s'appuie également sur les résultats d'évaluation des produits ST23YR80A et SA23YR80A (Neslib 1.0 en configuration SA) certifiés le 26 mars 2009 sous leur référence respective DCSSI-2009/05 et DCSSI-2009/06, cf. [2009/05] et [2009/06].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 23 juin 2009, 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.

Le produit SB23YR48A contient également une bibliothèque cryptographique Neslib v2.0 en configuration SB. 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 le microcontrôleur sécurisé SB23YR48A, incluant la bibliothèque cryptographique NesLib v2.0 en configuration SB, soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa 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 du microcontrôleur sécurisé SB23YR48A 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] 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

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	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 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	**4**	Production support, acceptance procedures and automation
	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									
	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 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	**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**	Independant 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 : - SB23YR48 Security Target, Référence : SMD_SB23YR48_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 : - SB23YR48 Security Target - Public Version, Référence : SMD_SB23YR48_ST_09_002, v01.00, STMicroelectronics
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - LAFITE Project, Référence : LAFITE_SB23YR80A_ETR_v1.0 / 1.0, 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 – SB23YR80A, Référence : LAFITE_SB23YR80A_ETRLiteComp_v1.0, Serma Technologies
[CONF]	Liste de configuration des produits : - Configuration list, Référence : SMD_SB23YR80_CFGL_09_001 rev 1.2, STMicroelectronics Liste de la documentation : - documentation report, Référence : SMD_SB23YR80_DR_09_001_v1.3, STMicroelectronics. Liste de configuration de la bibliothèque NesLib v2.0 : - Neslib 2.0 configuration list Référence : NesLib_2.0_CFGL_09_002_V01.01 STMicroelectronics.
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : - Datasheet, Référence : DS_23YR80 Rev 0.3, STMicroelectronics - ST23 Platform - Security Guidance, Référence : AN_SECU_23 Rev 6, STMicroelectronics - ST23 Reference Implementation User Manual, Référence : UM_23_RefImp Rev 14, STMicroelectronics

	- ST21/23 programming manual Référence : PM_21_23/0709 Rev1, STMicroelectronics - User Manual of Neslib 2.0 library, Référence : UM_NesLib_2.0 Rev 2, STMicroelectronics - NesLib 2.0: using the dispatcher on ST23YR80 UBO, Reference : PTD_NesLib_TN_09_006_v01.03, STMicroelectronics - ST23YR80/48: Recommendations for contactless operation, Référence : AN_23YR80_RCMD Rev 1, STMicroelectronics - Memory protection unit limitations on ST23Y devices, Référence : TN_23_MPU 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-PP-0035-2007.*
[2009/05]	Rapport de certification du produit ST23YR80A : Référence : DCSSI-2009/05, 26 mars 2009. ANSSI (www.ssi.gouv.fr)
[2009/06]	Rapport de certification du produit SA23YR80A : Référence : DCSSI-2009/06, 26 mars 2009. ANSSI (www.ssi.gouv.fr)

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)