Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2013/24

Microcontrôleur sécurisé ST31-K330A révision E pour version contact seulement, incluant optionnellement la librairie cryptographique Neslib révision 3.2

Paris, le 30 mai 2013

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

[Original signé]

Patrick Pailloux

SÉCURITÉ CERTIFICATION

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-2013/24

Nom du produit

Microcontrôleur sécurisé ST31-K330A révision E pour version contact seulement, incluant optionnellement la librairie cryptographique Neslib révision 3.2

Référence/version du produit

Référence maskset K330A, révision interne E

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 4

Niveau d'évaluation

EAL5 Augmenté

ALC_DVS.2 et AVA_VAN.5

Développeur

STMicroelectronics

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

Commanditaire

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, 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

Le produit évalué est le « microcontrôleur sécurisé ST31-K330A révision E en version contact seulement, incluant optionnellement la librairie cryptographique Neslib révision 3.2 », développé par STMicroelectronics.

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 conforme au profil de protection [BSI_PP_0035-2007]. La conformité est démontrable.

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 (voir [ST] au paragraphe 3.1 « TOE identification » et [GUIDES]) :

- informations écrites sur le microcontrôleur :
  - K330A : nom interne STMicroelectronics du produit de la famille ST31, la lettre A identifiant la lettre de la révision majeure du silicium ;
  - YGC : trigramme identifiant le logiciel dédié appelé aussi OST[1] (« *Operating system for Test* ») ;
  - UZQ[2] : trigramme 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* ». Celui-ci n'entre pas dans le périmètre d'évaluation ;
  - ST4 : identification du site de fabrication (4 correspond au site de STMicroelectronics/Rousset) ;
  - identification, par une lettre, de la révision de chaque niveau du process de fabrication correspondant à la séquence de masques (« *Maskset* ») révision interne E ;

[1]Système d'exploitation dédié pour les tests et la maintenance de la TOE.
[2]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.

- informations présentes dans la zone OTP (« *One Time Programmable* ») de la mémoire EEPROM :
  - *0033h* : numéro d'identification « Master » du produit ST31-K330A écrit sur 2 octets aux adresses *0x0010000A-0Bh*, ce numéro d'identification « Master » est unique pour toutes les versions commerciales du produit ;
  - *0050h* : numéro d'identification « Child » du produit ST31-K330A écrit sur 2 octets aux adresses *0x0010000E-0Fh (0050h correspond à la version commerciale SB31ZD16E, pour la valeur exacte du numéro d'identification « Child » pour chaque version commerciale, se reporter à la Datasheet du Produit) ;*
  - *12h* : version du code OST, valeur en hexadécimal écrite sur 1 octet à l'adresse *0x00100010h* ;
  - *45h* : lettre de révision E interne du produit, caractère ASCII codé en format hexadécimal écrite sur 1 octet à l'adresse *0x00100013h*.

1.2.1. 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 ;
- les tests du produit ;
- le contrôle d'accès aux mémoires ;
- la protection physique ;
- la gestion des violations sécuritaires ;
- la non-observabilité des informations sensibles ;
- la gestion sécurisée de la mémoire EEPROM ;
- 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 NesLib v3.2 optionnelle offrant, suivant la configuration choisie, des implémentations RSA, SHA, AES, ECC et un service de génération sécurisée de nombres premiers et clés RSA.

1.2.2. Architecture

L'architecture matérielle de la TOE est illustrée par la figure 1.
Le microcontrôleur ST31-K330A est constitué des éléments suivants :

- une partie matérielle composée :
  - d'un processeur ARM® SecurCore® SC000™ 32-bit RISC core ;
  - de mémoires :
    - 52[1]/38/22/16 Ko de mémoire EEPROM (avec contrôle d'intégrité) pour le stockage de données ;
    - 320 Ko de mémoire ROM pour le stockage des programmes utilisateur ;
    - 8 Ko de mémoire RAM ;

[1] Une version commerciale 40Ko de mémoire EEPROM existe sur la base d'un produit 52Ko.

- 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 : deux compteurs 16-bits, un bloc de gestion des entrées/sorties en mode contact (IART ISO 7816-3), un générateur de nombres aléatoires (TRNG) ;
- de coprocesseurs :
  - EDES pour le support des algorithmes DES ;
  - AES pour le support des algorithmes AES ;
  - NESCRYPT muni d'une RAM dédiée pour le support des algorithmes cryptographiques à clé publique ;

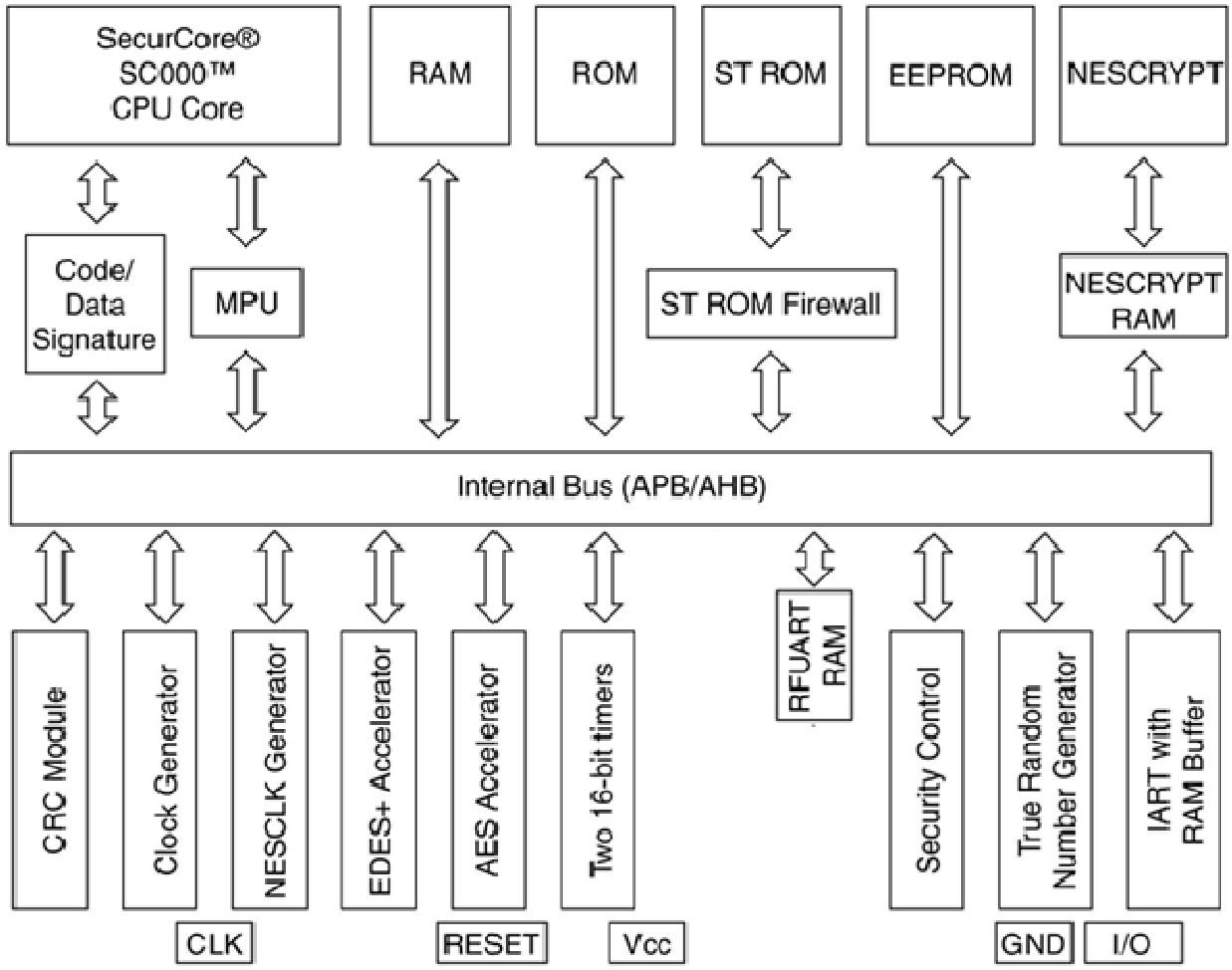

Figure 1: Architecture

Le client peut également choisir d'intégrer une bibliothèque cryptographique (NesLib v3.2) fournissant des implémentations des fonctions cryptographiques RSA, SHA, AES, ECC et un service de génération sécurisée de nombres premiers et de clés RSA. Cette bibliothèque est incluse dans la cible de sécurité du produit et de chacun de ses dérivés. La bibliothèque est embarquée partiellement ou en totalité selon son besoin, avec le code client, dans la mémoire ROM du produit.

En plus de ces composants matériels, la TOE embarque également, dans la ROM, un composant logiciel de test dédié (OST).
Celui-ci :

- assure le démarrage du produit (« *Boot* ») ;
- offre des commandes pour les tests et la maintenance de la TOE ;
- assure également un contrôle d'accès à ces fonctionnalités lorsque la TOE est en configuration « *Test* » ou en configuration « *User* ».

La partie test de ce logiciel n'est plus accessible par l'application qui sera embarquée par l'utilisateur de la TOE une fois celle-ci configurée pour la phase d'utilisation sur le terrain, correspondante à la configuration « *end user* ».

1.2.3. Cycle de vie

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

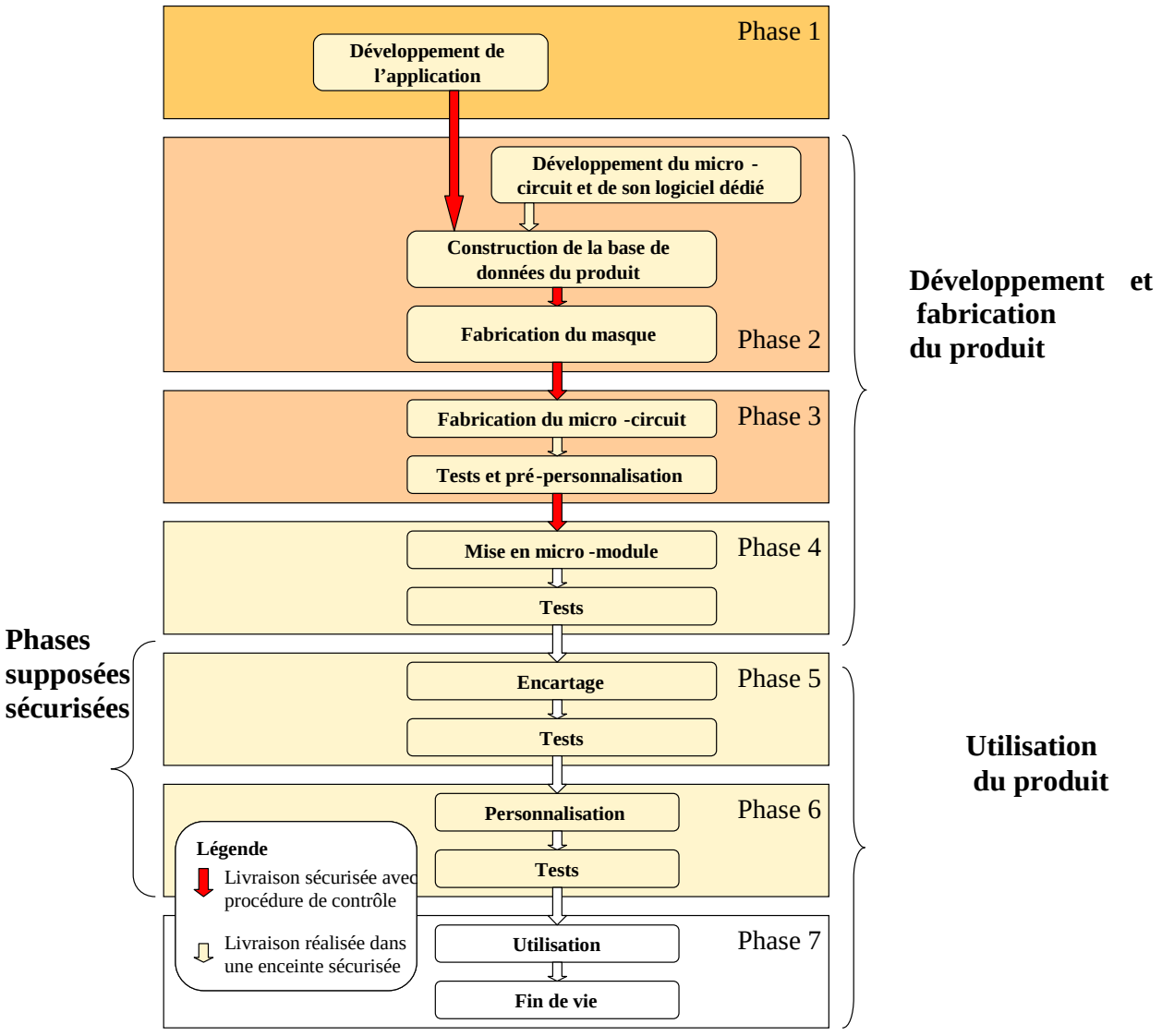

Figure 2: Cycle de vie

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

STMicroelectronics Smartcard IC division 190 Avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex France	**STMicroelectronics** 5A Serangoon North Avenue 5 554574 Singapour Singapour
STMicroelectronics Green Square, Lamboekstraat 5, Building B, 3d Floor, 1831 Diegem/Machelem, Belgique	**STMicroelectronics** 101 Boulevard des Muriers BP97 20 180 Casablanca Maroc
STS Microelectronics 16 Tao hua Rd. Futian free trade zone 518048 Shenzhen P.R. Chine	**STMicroelectronics** 629 Lorong 4/6 Toa Payoh 319521 Singapour Singapour
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
CMP Georges Charpak 880 Avenue de Mimet 13542 Gardanne France	**Smartflex** 20, Tampines Street 92 Singapore 528875 Singapour
STS Microelectronics 9 Mountain Drive, LISP II, Brgy La Mesa Calamba, 4027 Philippines	**Nedcard** Bijsterhuizen 25-29 6604 LM Wijchen Pays-Bas
STS Microelectronics 7 Loyang Drive Singapore 508938 Singapour	**Disco HI-Tec Europe GmbH** Liebigstrasse 8, D-85551 Kirchheim bei München, Allemagne

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, 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 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.

1.2.4. Configuration évaluée

Le certificat porte sur la TOE définie plus haut au paragraphe 1.2.1 et configurée en mode « *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 UZQ 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 4** [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 [CCDB AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [CCDB 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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 avril 2013, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques 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 [AIS31] 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 le produit « Microcontrôleur sécurisé ST31-K330A révision E pour version contact seulement, incluant optionnellement la librairie cryptographique Neslib révision 3.2 », soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit « Microcontrôleur sécurisé ST31-K330A révision E pour version contact seulement, incluant optionnellement la librairie cryptographique Neslib révision 3.2 » 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

3.3.1. Reconnaissance européenne (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 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 semi-formal 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 procedures
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
	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 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	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**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 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 : - ST31 - K330A version E (contact mode only) with optional cryptographic library Neslib 3.2 – Security Target, reference SMD_SC31Zxxx_ST_13_001, version v1.03 du 22 mars 2013. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST31 - K330A version E (contact mode only) with optional cryptographic library Neslib 3.2 – Public Security Target, reference SMD_SC31Zxxx_ST_13_002, version v1.0, 25 mars 2013.
[RTE]	Rapport technique d'évaluation : - Full Evaluation technical report Project CHABLIS reference : CHABLIS_ETR, version v1.1 du 17 avril 2013 ; - ST31-K330A project: Evaluation technical report Lite reference: ST31-K330A-ETRLiteComp_v1.1, version v1.1 du 19 avril 2013.
[CONF]	Liste de configuration : - ST31-K330A - Configuration list référence SMD_ST31-K330A_E_CFGL_13_001, version v1.0, 23th January 2013. Liste de la documentation : - ST31-K330 Evaluation Documentation Report reference : SMD_ST31-K330_DR_12_001, version v1.0, 3rd April 2013.
[GUIDES]	Guide d'utilisation du produit : - ARM SC000 Technical Reference Manual, reference : ARM DDI 0456 version A, September 2010 ; - ARM v6-M Architecture Reference Manual, reference : ARM DDI 0419, version C, September 2010 ; - ST31 - K330 platform - Sx31Zxxx, Mx31Zxxx - Secure dual interface microcontroller with enhanced security and up to 52 Kbytes of EEPROM – Datasheet, reference: DS_SR31Z052, revision 1.0, February 2013 ; - ST31 - K330 platform 90nm F10 CMOS die description, reference: DD_31Z052, revision 2, June 2012 ; - ST31 - K330 Security guidance, reference:AN_SECU_ST31_K330, revision 1.0, April 2013 ; - ST31 - AIS31 Compliant Random Number user manual, reference: UM_31_AIS31, revision 2, February 2013 ; - ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note AN_31_AIS31, revision 2, February 2013 ; - ST31 NesLib cryptographic library User manual, reference

	UM_31_NESLIB_3.2, revision 3, March 2013 ; - Application Note - Recommendations for use of EEPROM and code signature in ST31-K330 secure microcontrollers, reference AN_31_EEPROM, revision 1, February 2013 ; - ST31-K330 and ST33-K8H0 secure microcontrollers – Power supply glitch detector characteristics, reference: AN_31_GLITCH version 2, March 2013.
[BSI_PP_0035-2007]	Protection Profile - Security IC Platform Protection Profile, version v1.0 du 15 juin 2007. *Certifié par le BSI 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, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.
[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.
[CCDB AP]	CCDB-2012-04-002 - Application of attack potential to smart-cards, version 2.8, April 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, voir http://www.ssi.gouv.fr.
[AIS31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).