



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-2015/59

ST31H320 A01 including optional cryptographic library NESLIB

Paris, le 28 décembre 2015

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

Contre-amiral Dominique RIBAN
[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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2015/59

Nom du produit

**ST31H320 A01 including optional cryptographic
library NESLIB**

Référence/version du produit

A01

Conformité à un profil de protection

**Security IC Platform Protection Profile
with Augmentation Packages, version 1.0,
certifié BSI-CC-PP-0084-2014 le 19 février 2014**

avec conformité à

“Package 1: Loader dedicated for usage in Secured Environment only”

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

**ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1,
ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5**

Développeur(s)

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France

Commanditaire

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France

Centre d'évaluation

Serma Technologies

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables



SOG-IS



Le produit est reconnu au niveau EAL2.

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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Identification du produit</i>	6
1.2.3. <i>Services de sécurité</i>	6
1.2.4. <i>Architecture</i>	7
1.2.5. <i>Cycle de vie</i>	7
1.2.6. <i>Configuration évaluée</i>	8
2. L’EVALUATION	9
2.1. REFERENTIELS D’EVALUATION	9
2.2. TRAVAUX D’EVALUATION	9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	9
2.4. ANALYSE DU GENERATEUR D’ALEAS	9
3. LA CERTIFICATION	10
3.1. CONCLUSION	10
3.2. RESTRICTIONS D’USAGE	10
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	11
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	12
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	13
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	15

1. Le produit

1.1. Présentation du produit

Le produit évalué est le microcontrôleur sécurisé « *ST31H320 A01 including optional cryptographic library NESLIB* » développé par *STMICROELECTRONICS*.

Comme décrit dans la cible de sécurité [ST] au paragraphe « *TOE overview* », ce produit se décline en différentes configurations selon la taille de mémoire non volatile *FLASH* et l'activation du coprocesseur cryptographique NesCrypt. Ces configurations sont également décrites dans le document *Datasheet* (voir [GUIDES]).

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.2. Description du produit

1.2.1. Introduction

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

Cette cible de sécurité est strictement conforme au profil de protection [PP0084], avec le package « *Loader dedicated for usage in secured environment only* ».

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments suivants (voir [ST] au paragraphe « *TOE identification* » et [GUIDES]) :

- *IC Maskset name* : K8N0A
- *IC version* : C
- *Master product identification number* : 00DE
- *Firmware version* : 2.0.2
- *OST version* : 4.0
- (optionel) *NesLib crypto library version* : 4.2.10

Toutes ces valeurs sont disponibles à travers les interfaces logiques du produit, selon les méthodes et formats décrits dans [GUIDES]. De plus, « K8N0A », valeur *IC Maskset name*, est gravée sur la surface du composant.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection physique ;

- l'intégrité logique du produit ;
- des contrôles d'accès aux mémoires ;
- la gestion des violations sécuritaires ;
- la non-observabilité des informations sensibles ;
- le chargement et la gestion de la mémoire FLASH ;
- 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 ;
- le service optionnel de bibliothèque cryptographique NesLib v4.2 offrant des implémentations RSA, SHA, ECC ainsi que la génération sécurisée de nombres premiers et de clés RSA.

1.2.4. Architecture

Le produit est constitué d'une partie matérielle et d'une partie logicielle, toutes deux décrites dans la cible de sécurité au paragraphe *TOE description*.

La partie matérielle comporte principalement :

- un processeur ARM SecurCore SC000 ;
- des coprocesseurs cryptographiques pour accélérer les calculs AES, Triple DES et de cryptographie asymétrique ;
- un générateur physique d'aléa (TRNG) ;
- des mémoires (RAM, Flash) ;
- des modules de sécurité : unité de protection des mémoires (MPU), générateur d'horloge, surveillance et contrôle de la sécurité, contrôle d'intégrité ;
- des modules fonctionnels : compteurs, gestion des entrées/sorties en mode contact.

La partie logicielle est composée de :

- un logiciel dédié (OST), participant au démarrage du composant (*boot sequence*) ;
- un logiciel dédié (*Firmware*), assurant la gestion du cycle de vie, le chargement de la mémoire Flash (*Secure Flash loader*), et l'interfaçage avec l'application (*drivers*) ;
- optionnellement, une bibliothèque cryptographique (NesLib), offrant des services RSA (dont la génération de clés), courbes elliptiques, hachage, génération de nombres premiers, génération d'aléa déterministe (DRBG).

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité (voir [ST]) ; il est conforme au cycle de vie de 7 phases décrit dans [PP0084].

Les sites impliqués dans le cycle de vie pour les phases 2, 3 et 4 sont indiqués la cible de sécurité (voir Table 16 de [ST]).

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit le développeur de l'application à embarquer dans le microcontrôleur.

Dans la cible de sécurité, le développeur a opté pour la conformité au « *Package 1 : loader dedicated for usage in secured environment only* » du profil de protection [PP0084]. Le

chargement de l'application par l'utilisateur en configuration *Issuer*¹ doit être réalisé dans un environnement sécurisé.

1.2.6. Configuration évaluée

Le certificat porte sur le produit ST31H320 A01 dans les différentes configurations offertes (tailles mémoire, activation NesCrypt, voir §1.1 et [GUIDES]).

¹ Egaleme nt appelé *ADMIN* dans plusieurs documents de STMicroelectronics, dont la cible de sécurité.

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].

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 [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau `AVA_VAN` a été déterminé en suivant l'échelle de cotation du guide [JIWG 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 18 décembre 2015, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau `AVA_VAN.5` visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS 31] et il répond aux exigences de la classe PTG.2.

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [REF] il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

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 « ST31H320 A01 including optional cryptographic library NESLIB » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.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 « ST31H320 A01 including optional cryptographic library NESLIB » 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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord¹, 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 signataires², des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 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, 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	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	Minimally complex internals
	ADV_SPM						1	1		
	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 procedures
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
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR								1	Basic flaw remediation
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	3	Compliance with implementation standards - all parts
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	3	Rigorous analysis of coverage
	ATE_DPT			1	1	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]	<p>Cible de sécurité de référence pour l'évaluation : ST31H320 A01 including optional cryptographic library NESLIB, Security Target, SMD_ST31H320_ST_14_001 Rev A01.5, décembre 2015, STMicroelectronics.</p> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : ST31H320 A01 including optional cryptographic library NESLIB, Security Target for composition, SMD_ST31H320_ST_14_002 Rev A01.5, décembre 2015, STMicroelectronics.</p>
[RTE]	<p>Rapport technique d'évaluation : Evaluation Technical Report LOUPIAC Project, LOUPIAC_ETR_v1.2, 18 décembre 2015, Serma Technologies.</p> <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : ETR Lite for Composition LOUPIAC Project, LOUPIAC_ETRliteComp_v1.2, 18 décembre 2015, Serma Technologies.</p>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none">- ST31 – K8N0 Configuration List, SMD_ST31H310_C_CFGL_15_003 Rev 1.0, 15 décembre 2015, STMicroelectronics ;- NesLib 4.2.10 for ST31 on ST31H320 configuration list, SSS_Neslib4210ST31_H320_CFGL_15_001, juillet 2015, STMicroelectronics.

<p>[GUIDES]</p>	<ul style="list-style-type: none"> - ST31H platform ST31H320, Datasheet – preliminary data, DS_ST31H320 Rev 0.4, août 2015, STMicroelectronics ; - ARM Cortex SC000 Technical Reference Manual, ARM_DDI_0456 Rev A, septembre 2010, ARM ; - ARMv6-M Architecture Reference Manual, ARM_DDI_0419 Rev C, septembre 2010, ARM ; - ST31G and ST31H Secure MCU platforms, Security guidance, AN_SECU_ST31G_H Rev 2, novembre 2015, STMicroelectronics ; - ST31 firmware, User manual, UM_ST31_FW Rev 5, août 2015, STMicroelectronics ; - NesLib 4.2 library, User manual, UM_NESLIB_4.2 Rev 1.0, juillet 2015, STMicroelectronics ; - ST31G and ST31H Secure MCU platforms NesLib 4.2 security recommendations, AN_SECU_ST31_NESLIB_4.2 Rev1, août 2015, STMicroelectronics ; - NesLib 4.2.10 for ST31 platforms, release note, RN_ST31_NESLIB_4.2.10 Rev 1, août 2015, STMicroelectronics ; - ST31H320 Flash memory loader installation guide, User manual, UM_31H_FL Rev 3, juillet 2015, STMicroelectronics ; - ST31G and ST31H - AIS31 Compliant Random Number - User Manual, UM_31G_31H_AIS31 Rev 1.0, janvier 2015, STMicroelectronics ; - ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, AN_31_AIS31 Rev 2, février 2013, STMicroelectronics.
<p>[PP0084]</p>	<p>Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0084-2014.</i></p>

Annexe 3. Références liées à la certification

	Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[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 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr .
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 September 2011, BSI (Bundesamt für Sicherheit in der Informationstechnik).

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.