



**PREMIÈRE
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CC-2022/42

Cryptographic library NESLIB 6.7.4 on ST31N600 A01

Paris, le 23 Décembre 2022

Le Directeur général adjoint de l'Agence
nationale de sécurité des systèmes d'information

Emmanuel NAEGELEN

[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@ssi.gouv.fr

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

Référence du rapport de certification	ANSSI-CC-2022/42
Nom du produit	Cryptographic library NESLIB 6.7.4 on ST31N600 A01
Référence/version du produit	Version 6.7.4
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 aux packages : <i>"Authentication of the security IC"</i> <i>"Loader dedicated for usage in Secured Environment only"</i> <i>"Loader dedicated for usage by authorized users only"</i>
Critère d'évaluation et version	Critères Communs version 3.1 révision 5
Niveau d'évaluation	EAL5 augmenté ASE_TSS.2,ALC_DVS.2, AVA_VAN.5, ALC_FLR.1
Développeur	STMICROELECTRONICS Lambroekstraat, 5 Building B, 1831 Diegem, Belgique
Commanditaire	STMICROELECTRONICS Lambroekstraat, 5 Building B, 1831 Diegem, Belgique
Centre d'évaluation	THALES / CNES 290 allée du Lac, 31670 Labège, France
Accords de reconnaissance applicables	  <p>Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.</p>

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit.....	6
1.2.1	Introduction	6
1.2.2	Services de sécurité.....	6
1.2.3	Architecture	6
1.2.4	Identification du produit.....	6
1.2.5	Cycle de vie	7
1.2.6	Configuration évaluée	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation	8
2.2	Travaux d'évaluation	8
2.3	Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	8
2.4	Analyse du générateur d'aléa.....	8
3	La certification	9
3.1	Conclusion.....	9
3.2	Restrictions d'usage	9
3.3	Reconnaissance du certificat.....	9
3.3.1	Reconnaissance européenne (SOG-IS).....	9
3.3.2	Reconnaissance internationale critères communs (CCRA).....	10
ANNEXE A.	Références documentaires du produit évalué	11
ANNEXE B.	Références liées à la certification	12

1 Le produit

1.1 Présentation du produit

Le produit évalué est le microcontrôleur ST31N600 A01, sur lequel est embarqué la librairie « *Cryptographic library NESLIB 6.7.4* » développée 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, etc.) 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 « *authentication of the security IC* » ;
- le package « *loader dedicated for usage in secured environment only* » ;
- le package « *loader dedicated for usage by authorized users only* ».

1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont décrits dans la cible de sécurité [ST] à la section « *1.6 TOE Description* ».

1.2.3 Architecture

Le produit est constitué du microcontrôleur ST31N600 A01 certifié, voir [CER] ainsi que de la librairie cryptographique NESLIB 6.7.4.

La TOE comprend la librairie cryptographique NESLIB 6.7.4 en composition sur le composant ST31N600 A01 comme décrit dans la cible de sécurité [ST] à la section « *1.5 TOE Overview* ».

1.2.4 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 ci-après :

Éléments de configuration		Données d'identification lues
Identification du microcontrôleur ST31N600 A01	<i>IC masket name</i>	K470B
	<i>IC version B</i>	42
	<i>Master Identification number</i>	0200
Identification des logiciels embarqués	Firmware version 3.1.2	03010202
Identification des bibliothèques	<i>Neslib Cryptographic Library Version 6.7.4</i>	01060704

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans le guide [AGD_UM_Neslib] (voir [GUIDES]).

1.2.5 Cycle de vie

Le cycle de vie du produit est conforme au profil de protection [PP0084]. Il est rappelé dans la cible de sécurité [ST], à la section « 1.7 TOE life cycle ».

Les sites impliqués dans le développement de la librairie (en phase 1), puis les sites impliqués pour son chargement (en phase 3) sont décrits dans la table 16 de [ST] et rappelés ci-après :

- ST Grenoble [AUDIT_Grenoble] ;
- ST Rousset [AUDIT_Rousset] ;
- ST Tunis [AUDIT_Tunis] ;
- ST Zaventem [AUDIT_ZAV].

Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site sont mentionnés dans [SITES].

La livraison de la TOE peut s'effectuer soit après la phase 3 si la TOE est livrée sous forme de *wafer* ou de *dice*, soit après la phase 4 si la TOE est livrée sous forme de produit.

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

1.2.6 Configuration évaluée

Le certificat porte sur la librairie NESLIB 6.7.4 dans la configuration décrite au chapitre 1.2.4. Toutes autres applications, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne font donc pas partie du périmètre de l'évaluation.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « ST31N600 A01 », voir [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « réussite ».

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

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto] mais l'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence des vulnérabilités exploitables pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER]).

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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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 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 microcontrôleur 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 puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

3.3.2 Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

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 :



² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none">- <i>Cryptographic library NESLIB 6.7.4 on ST31N600 A01 Security Target</i>, référence SMD_NL-ST31N600_ST_20_001 Rev 01.3, avril 2022. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none">- <i>Cryptographic library NESLIB 6.7.4 on ST31N600 A01 Security Target for composition</i>, référence SMD_NL-ST31N600_ST_20_002 Rev 01.3, avril 2022.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none">- <i>Evaluation Technical Report – Project BRUGES</i>, référence BRU_ETR, version 3.0, 15 décembre 2022. <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none">- <i>Evaluation Technical Report for composite evaluation</i>, référence BRU_ETRLite, version 2.0, 19 décembre 2022.
[CONF]	<p><i>Neslib 6.7.4 for ST31N600 Configuration List</i>, référence SSS_NesLib 6.7_CFGL_21_001_v02-02, 19 avril 2022.</p>
[GUIDES]	<p>Voir guides du composant [CER] ;</p> <p>[AGD_UM_Neslib] <i>Cryptographic library NesLib 6.7 - User Manual</i>, référence UM_NesLib_6.7, révision 4, décembre 2021 ;</p> <p><i>NesLib 6.7 security recommendations for ST31N platform secure microcontrollers</i>, référence AN_SECU_ST31N_NESLIB_6.7, révision 5, mars 2022 ;</p> <p><i>NesLib 6.7.4 for ST31N platforms - Release Note</i>, référence RN_ST31N_NesLib_674, révision 1, août 2021.</p>
[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none">- Audit générique : STM-2021_ALC_GEN ;- [AUDIT_Grenoble] : STM2020-v2_GNB_STAR_v1.0 / 1.0 ;- [AUDIT_Rousset] : STM2021_RST_STAR_v1.0 / 1.0 ;- [AUDIT_Tunis] : STM-2021_TNS_STAR_v1.0 / 1.0 ;- [AUDIT_ZAV] : STM2020-v2_ZVT_STAR_v1.0.
[CER]	<p>Rapport de certification ANSS-CC-2022/21, ST31N600 A01. Certifié par l'ANSSI le 21 octobre 2022.</p>
[PP0084]	<p><i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages</i>, version 1.0, 13 janvier 2014. Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-PP-0084-2014.</p>

ANNEXE B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	<i>Common Criteria for Information Technology Security Evaluation:</i> <ul style="list-style-type: none">- <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;- <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;- <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[JIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.1, juin 2020.
[COMP] *	<i>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices</i> , version 1.5.1, mai 2018.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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