



**PREMIER
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-2025/08

ST31R480 with RNG software library (B01)

Paris, le 11 Avril 2025

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

Vincent STRUBEL

[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.

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 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.cyber.gouv.fr.

TABLE DES MATIERES

1	Résumé	5
2	Le produit.....	7
2.1	Présentation du produit.....	7
2.2	Description du produit	7
2.2.1	Introduction	7
2.2.2	Services de sécurité.....	7
2.2.3	Architecture	7
2.2.4	Identification du produit	7
2.2.5	Cycle de vie	8
2.2.6	Configuration évaluée	8
3	L'évaluation.....	9
3.1	Référentiels d'évaluation	9
3.2	Travaux d'évaluation	9
3.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	10
3.4	Analyse du générateur d'aléa.....	10
4	La certification	11
4.1	Conclusion	11
4.2	Restrictions d'usage.....	11
4.3	Reconnaissance du certificat	12
4.3.1	Reconnaissance européenne (SOG-IS).....	12
4.3.2	Reconnaissance internationale critères communs (CCRA).....	12
ANNEXE A.	Références documentaires du produit évalué	13
ANNEXE B.	Références liées à la certification.....	15

1 Résumé

Référence du rapport de certification	ANSSI-CC-2025/08
Nom du produit	ST31R480 with RNG software library
Référence/version du produit	B01
Type de produit	Cartes à puce et dispositifs similaires
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 : "Authentication of the security IC", "Loader dedicated for usage in Secured Environment only" "Loader dedicated for usage by authorized users only"
Critère d'évaluation et version	Critères Communs version 3.1 révision 5
Niveau d'évaluation	EAL6 augmenté ALC_FLR.2, ASE_TSS.2
Référence du rapport d'évaluation	<i>Evaluation Technical Report, SYN ST31R480 B01</i> Référence ST31R480_B01_ETR version 3.0, 25 mars 2025
Fonctionnalité de sécurité du produit	voir 2.2.2 Services de sécurité
Exigences de configuration du produit	voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation	voir 4.2 Restrictions d'usage
Développeur	STMICROELECTRONICS 190 avenue Célestin Coq, ZI de Rousset-Peynier 13106 Rousset Cedex, France
Commanditaire	STMICROELECTRONICS 190 avenue Célestin Coq, ZI de Rousset-Peynier

13106 Rousset Cedex, France

Centre d'évaluation

THALES / CNES

290 allée du Lac,
31670 Labège, France

Accords de reconnaissance applicables



SOG-IS



Ce certificat est reconnu au niveau EAL2
augmenté de ALC_FLR.2.

2 Le produit

2.1 Présentation du produit

Le produit évalué est « ST31R480 with RNG software library, B01 » 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, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

2.2 Description du produit

2.2.1 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* ».

2.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont décrits à la section 1.5 « *TOE overview* » de la cible de sécurité.

2.2.3 Architecture

La constitution du produit est décrite dans la cible de sécurité [ST] au chapitre 1.6 « *TOE description* ». La Figure 1 notamment présente l'architecture du *hardware*.

2.2.4 Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF], ainsi que dans la Table 1 au chapitre 1.4 « *TOE identification* » de la cible de sécurité.

La version certifiée du produit est identifiable par les valeurs indiquées dans la cible de sécurité [ST] au chapitre 1.4 « *TOE identification* » ; la procédure d'identification pour lire ces valeurs sur le produit est spécifiée dans les guides [GUIDES].

2.2.5 Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité [ST] au chapitre 1.7 « *TOE life cycle* ». Il est conforme à celui décrit dans le [PP0084]. Le produit a été développé sur les sites mentionnés dans la Table 16 de la cible [ST]. Hors certification de site, les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés sont mentionnés dans [SITES].

2.2.6 Configuration évaluée

Le certificat porte sur le microcontrôleur et son *Dedicated Software*, identifiés dans la cible de sécurité [ST] au chapitre 1.4 « *TOE identification* », dans ses configurations permises par les [GUIDES]. Les différentes variantes présentées en Table 2 de la cible de sécurité sont toutes couvertes par le certificat.

Au regard du cycle de vie, le certificat porte sur le produit livré à l'issue de la phase 3 comme de la phase 4.

3 L'évaluation

3.1 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 et dispositifs similaires, 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).

3.2 Travaux d'évaluation

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

3.3 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 [ANA_CRY].

Cette analyse a identifié des non-conformités par rapport aux référentiels [ANSSI Crypto] et [SOG-IS Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme aux référentiels [ANSSI Crypto] et [SOG-IS Crypto], pour les mécanismes cryptographiques qui le permettent.

3.4 Analyse du générateur d'aléa

Le produit comporte un générateur physique d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport aux référentiels [ANSSI Crypto] et [SOG-IS Crypto].

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. 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 les documents [ANSSI Crypto] et [SOG-IS Crypto], 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'aléa n'a pas révélé de faiblesse. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

Ce générateur d'aléa a aussi été analysé conformément à la méthode d'évaluation [AIS20/31] et suivant les dispositions décrites dans la note d'application [NOTE-24].

4 La certification

4.1 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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2025/07, a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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 3.

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].

4.3 Reconnaissance du certificat

4.3.1 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 :



4.3.2 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 :



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

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>ST31R480 B01 with Random Number Generator software library, Security Target, SMD_ST31R480_ST_23_003 Rev B01.4.</i> <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>ST31R480 B01 with Random Number Generator software library, Security Target for composition, SMD_ST31R480_ST_23_004 Rev B01.4.</i>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - <i>Evaluation Technical Report, SYN ST31R480 B01, Référence ST31R480_B01_ETR, version 3.0, 25 mars 2025.</i> <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, SYN ST31R480 A01, Référence ST31R480_B01_ETRLite, version 2.0, 7 mars 2025.</i>
[ANA_CRY]	<p><i>Analysis of Cryptographic Mechanisms, SYN ST31R480 A01/B01, ST31R480_CRY, version 1.0, 8 janvier 2025.</i></p>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - <i>ST31R480 B01 Configuration List, ST31R480_CFGL_B01, v1.0, 12 mai 2024;</i> - <i>Random number generator library RNGLIB 2.0.X, configuration items list, SE_ST31R_RNGLIB_ConfigItem, v2.0, 29 août 2024 ;</i> - <i>RngLib v2.0.x for ST31R480 configuration list, SE_RNGLIB_ST31R_CFGL_24_001, v2.0, 2 octobre 2024 ;</i> - <i>Firmware ST31R480 Configuration List, SE_FW_ST31R480_CFGL_24_002, v5.0, 3 octobre 2024 ;</i> - <i>Firmware V3 Configuration Items List, SE_FW_ST31R480_CFGL_24_001, v4.0, 2 octobre 2024 ;</i> - <i>ST31R480 A01 and B01 - Document report, SMD_ST31R480_DR_A01_B01, v1.0.</i>
[GUIDES]	<p>Voir Table 15 « <i>Guidance documentation</i> » dans la cible de sécurité [ST]</p>
[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> - STM_2024_ALC_GEN_v1.1 - STM_2023_CB-JY-LH_STAR_v1.1 - STM_2023_DNP_STAR_v1.1 - STM_2022_DPE_STAR_v1.1 - STM_2023_FEI_STAR_v1.0 - STM_2022_AMK1_STAR_v1.0 - STM_2023_TPY-AMK6_STAR_v1.0 - STM_2023_BSK_STAR_v1.0

	<ul style="list-style-type: none">- STM_2022_CAL_STAR_v1.0- STM_2022_CAT-PAL_STAR_v1.1- STM_2023_RST_CMP_STAR_v1.2- STM_2022_GNB_STAR_v1.2- STM_2023_LYG_STAR_v1.0- STM_2022_RNS_STAR_v1.1- STM_2023_STS-QA Lab_STAR_v1.0- STM_2023_SOP_STAR_v1.0- STM_2022_TNS_STAR_v1.0- STM_2022_Teradyne_STAR_v1.1- STM_2023_Pantos_STAR_v1.0- STM_2024_ST_Crolles_STAR_v1.0- STM_2024_ST_Ljubljana_STAR_v1.0
[PP0084]	<p><i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014.</i></p> <p>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, 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 3.2.1, février 2024.
[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.
[SOG-IS Crypto]	<i>SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms</i> , version 1.3, février 2023.
[AIS20/31]	<i>A proposal for: Functionality classes for random number generators, AIS20/AIS31</i> , version 2.0, 18 septembre 2011, BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>).

[NOTE-24]	Note d'application – Evaluation de générateurs d'aléa selon AIS20/31 dans le schéma français, référence ANSSI-CC-NOTE-24, version en vigueur.
-----------	---

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