



**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-2022/21

## ST31N600 A01

Paris, le 21 octobre 2022

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

Guillaume POUPARD

[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](mailto:certification@ssi.gouv.fr)

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

Référence du rapport de certification	<b>ANSSI-CC-2022/21</b>
Nom du produit	<b>ST31N600 A01</b>
Référence/version du produit	<b>A01</b>
Conformité à un profil de protection	<b><i>Security IC Platform Protection Profile with Augmentation Packages, version 1.0</i></b> 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	<b>Critères Communs version 3.1 révision 5</b>
Niveau d'évaluation	<b>EAL 6 augmenté ALC_FLR.1</b>
Développeur	<b>STMICROELECTRONICS</b> 190, avenue Celestin Coq ZI de Rousset 13106 Rousset Cedex France
Commanditaire	<b>STMICROELECTRONICS</b> 190, avenue Celestin Coq ZI de Rousset 13106 Rousset Cedex France
Centre d'évaluation	<b>THALES / CNES</b> 290 allée du Lac, 31670 Labège, France
Accords de reconnaissance applicables	  Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.

## 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](http://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	Analyse 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 .....	13

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est le microcontrôleur « ST31N600 A01 » 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.

## 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* ».

De plus, cette cible se base sur le document « *SmartCard Integrated Circuit Platform Augmentation* », voir [AUG].

### 1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont décrits au chapitre « *1.5 TOE overview* » de la cible de sécurité [ST].

### 1.2.3 Architecture

Le produit est constitué d'une partie matérielle et d'une partie logicielle toutes deux décrites dans la cible de sécurité [ST] au chapitre « *1.6 TOE description* ».

### 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 du tableau ci-après.

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 « *user manual* » (voir [GUIDES]).

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	N/A	N/A

### 1.2.5 Cycle de vie

Le cycle de vie du produit est décrit au chapitre « 1.7 TOE life cycle » de la cible de sécurité [ST] ; il est conforme à celui décrit dans [PP0084].

Les sites impliqués dans le cycle de vie du produit (phases 2, 3 et 4) sont indiqués dans la table 15 de la cible de sécurité [ST]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site sont mentionnés dans [SITES].

### 1.2.6 Configuration évaluée

Le certificat porte sur le microcontrôleur tel que défini au chapitre 1.2.4. Toute autre application, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre de l'évaluation.

Au regard du cycle de vie mentionné au chapitre 1.2.5, le produit évalué est celui obtenu à l'issue de la phase 3 lorsque le produit est livré sous forme de wafer, ou à l'issue de la phase 4 lorsque le produit est livré en boîtiers (micro-modules, etc.).

## 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

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** ».

### 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 [ANA\_CRY].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto] ou [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.

### 2.4 Analyse du générateur d'aléa

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

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto] ou [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. Afin que les mécanismes analysés soient conformes aux exigences de ce référentiel, les recommandations identifiées [GUIDES] doivent être suivies (voir AN\_SECU).

Dans le cas où le générateur d'aléa serait utilisé à des fins cryptographiques, il est obligatoire de le combiner à un mécanisme algorithmique de génération de pseudo-aléa, de nature cryptographique, afin de fournir des données aléatoires cryptographiquement satisfaisantes, comme énoncé dans les documents [ANSSI Crypto] ou [SOG-IS Crypto].

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 [CC-NOTE-24]. Il est conforme à PTG.2.

### 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'accord<sup>1</sup>, 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 :



<sup>1</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.eu](http://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 signataires<sup>2</sup>, 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 :



Le présent certificat est reconnu par le CCRA au niveau EAL2 augmenté de ALC\_FLR.1.

---

<sup>2</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://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"> <li>- ST31N600 A01 <i>Security Target</i>, référence SMD_ST31N600_ST_20_001, revision A01.3, décembre 2021.</li> </ul> <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"> <li>- ST31N600 A01 <i>Security Target for composition</i>, référence SMD_ST31N600_ST_20_002, revision A01.3, janvier 2022.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- <i>Evaluation Technical Report – Project ST31N600</i>, référence ST31N600_ETR, version 2.0, 26 septembre 2022.</li> </ul> <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"> <li>- <i>Evaluation Technical Report for composition – Project ST31N600</i>, référence ST31N600_ETRLite, version 1.0, 26 septembre 2022.</li> </ul>
[ANA_CRY]	<p><i>Analysis of Cryptographic Mechanisms, Project ST31N600</i>, référence ST31N600_CRY, version 1.1, 6 juillet 2022.</p>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>- ST31N600 Configuration List, référence ST31N600_CFGL_A01_V1_0, version 1.0, 9 novembre 2021 ;</li> <li>- FirmWare - ST31N600 Configuration List, référence SE_FW_ST31N600_CFGL_21_001_v1_4, 13 août 2021.</li> </ul>
[GUIDES]	<p><i>ST31N Platform ST31N600 ST31N500 ST31N400 Datasheet - Secure dual interface microcontroller with enhanced security and up to 608 Kbytes of Flash memory - ST31N datasheet</i>, référence DS_ST31N, version 0.6 , octobre 2021 ;</p> <p><i>ARM Cortex SC000 Technical Reference Manual</i>, référence ARM_DDI_0456, version A, 2019 ;</p> <p><i>ARMv6-M Architecture Reference Manual</i>, référence ARM_DDI_0419, version C, 2019 ;</p> <p><i>User Manual ST31N platform Firmware V3</i>, référence UM_ST31N_FWv3, version 6, 24 août 2021 ;</p> <p><i>Security Guidance of the ST31N secure MCU platform - Application Note</i>, référence AN_SECU_ST31N, version 1, septembre 2021 ;</p> <p><i>ST31N platform Random Number Generation - User Manual</i>, référence UM_ST31N_TRNG, version 2, avril 2021 ;</p> <p>ST31N platform TRNG reference implementation: compliance tests - Application Note, référence AN_ST31N_TRNG, version 1, 2 octobre 2020.</p>
[SITES]	<p>Référence des rapports d'analyse documentaire et d'audit de site pour la réutilisation des audits de site :</p> <ul style="list-style-type: none"> <li>- Analyse documentaire générique : STM-2021_ALC_GEN_v1.0 / 1.0 ;</li> </ul>

	<ul style="list-style-type: none"> <li>- ST Rousset (France): STM2020_RST_STAR_v1.1 / 1.1 ;</li> <li>- ST Gardanne (France): STM2020_RST_STAR_v1.1 / 1.1 ;</li> <li>- ST Zaventem (Belgium): STM2020-v2_ZVT_STAR_v1.0 / 1.0 ;</li> <li>- ST Grenoble (France): STM2020-v2_GNB_STAR_v1.0 / 1.0 ;</li> <li>- ST Rennes (France): STM_2020_V2_RNS_STAR_v1.1 / 1.1 ;</li> <li>- ST Ljubjana (Slovenia) : STM2020_V2_LJU_STAR_v1.0 / 1.0 ;</li> <li>- ST Tunis (Tunisia): STM-2021_TNS_STAR/ 1.0 ;</li> <li>- ST Shenzhen (China): STM2020_STS_STAR_v1.0 / 1.0 ;</li> <li>- ST Sophia (France): STM2020-v2_SOP_STAR_v1.1 / 1.1 ;</li> <li>- ST Loyang (Singapore): STM2020_Loyang_STAR_v1.0 / 1.0 ;</li> <li>- ST Crolles (France) : STM2020_CRL_STAR_v1.0 / 1.0 ;</li> <li>- DNP (Japan): STM_2020_V2_DNP_STAR_v1.0 / 1.0 ;</li> <li>- DPE (Italy): STM2020-v2-DPE_STAR_v1.0 / 1.0 ;</li> <li>- ST Toa Payoh (Singapore): STM2020_TPY_AMK6_STAR / 1.0 ;</li> <li>- ST Ang Mo Kio 6 (Singapore): STM2020_TPY_AMK6_STAR / 1.0 ;</li> <li>- ST Ang Mo Kio 1 (Singapore): STM2021_AMK1_STAR/ v1.0 ;</li> <li>- Amkor ATT 1/3/6 (Taiwan): STM-2021_ATT3_STAR_v1.0 / 1.0 ;</li> <li>- Winstek (Taiwan): STM_2020_V2_Winstek_STAR_v1.2 / 1.2 ;</li> <li>- Feiliks (China): STM2020_V2_FEI_STAR_v1.0 / 1.0 ;</li> <li>- ST Bouskoura (Maroc): STM2020_BSK_STAR_v1.0 / 1.0 ;</li> <li>- ChipBond JY and LH: STM_2021_CB-JY-LH_STAR / v1.0 ;</li> <li>- UTAC Thai Limited 1 (UTL1.2): UTL1.3_STAR_v1.0 / 1.0 ;</li> <li>- UTAC Thai Limited 1 (UTL3.2): AUDIT_STAR_UTL_3.</li> </ul>
[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>
[AUG]	<p><i>Smartcard Integrated Circuit Platform Augmentations</i>, version 1.00 du 8 mars 2002.</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"> <li>- <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ;</li> <li>- <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ;</li> <li>- <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.</li> </ul>
[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.
[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 1.2, janvier 2020.
[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> ).
[CC-NOTE-24]	Evaluations de générateurs d'aléa selon AIS20/31 dans le schéma français.

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