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-2025/33

MIFARE® Plus® EV2 on ST31R480 A01 (version 1.0.3)

Paris, le 29/9/2025 | 11:50 CEST

Vincent Strubel

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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@ssi.gouv.fr

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

Référence du rapport de certification **ANSSI-CC-2025/33**
Nom du produit **MIFARE® Plus® EV2 on ST31R480 A01**
Référence/version du produit **version 1.0.3**
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 CC:2022, révision 1**
Niveau d'évaluation **EAL5 augmenté** ASE_TSS.2, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2
Référence du rapport d'évaluation *Evaluation Technical Report Hasselt / MIFARE Plus EV2 on ST31R480 A01* référence Hasselt_ETR version 1.0 24 juillet 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** 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

CCRA

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 « MIFARE® Plus® EV2 on ST31R480 A01, version 1.0.3 » développé par STMICROELECTRONICS.

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 au chapitre « *1.6 TOE Description* » de la cible de sécurité [ST].

2.2.3 *Architecture*

Le produit est constitué d'une partie matérielle et d'une partie logicielle toutes deux décrites dans la cible de sécurité [ST] aux chapitres « *1.5 TOE Overview* » et « *1.6 TOE Description* ».

2.2.4 *Identification du produit*

La version certifiée du produit est identifiable dans la cible de sécurité [ST] par les éléments du tableau « *Table 1. TOE components* » au chapitre « *1.4 TOE identification* ».

2.2.5 *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 17 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].

2.2.6 *Configuration évaluée*

Le certificat porte sur le microcontrôleur tel que défini au chapitre 2.2.4. 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.

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 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

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 dans le cadre d'un schéma national reconnu au titre de l'accord du SOG-IS.

Cette évaluation a ainsi pris en compte, les résultats de l'évaluation du microcontrôleur « ST31R480 A01 », voir [CER_IC].

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 au référentiel [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 au référentiel [SOG-IS Crypto], pour les mécanismes cryptographiques qui le permettent.

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-2025/33 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'accord[1], 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 signataires[2] , 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]	Cible de sécurité de référence pour l'évaluation : - *MIFARE® Plus® EV2 on ST31R480 A01 Security Target*, référence SMD_MFPEV2_ST31R480_ST_24_001, version 01.1, 8 juillet 2025 Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MIFARE® Plus® EV2 on ST31R480 A01 Security Target for composition*, référence SMD_MFPEV2_ST31R480_ST_24_002, version 01.1, juillet 2025.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report Hasselt / MIFARE Plus EV2 on ST31R480 A01*, référence Hasselt_ETR, version 1.0, 24 juillet 2025. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation Technical Report for composite evaluation Hasselt*, référence Hasselt_ETRLite, version 1.0, 24 juillet 2025.
[ANA_CRY]	*Analysis of Cryptographic Mechanisms Hasselt, référence HASSELT_CRY, version 1.0, 7 juillet 2025.*
[GUIDES]	- *MIFARE Plus EV2 library v1.0 for the ST31R platform devices – User manual, référence UM_ST31R_MFP_EV2_1.0, version 2, 28 mai 2025.* - *Technical note MIFARE Plus EV2 interface specification*, référence TN_MIFARE_PLUS_EV2, version 3, 25 août 2022. - *User manual MIFARE Plus EV2 library on ST31R-K4H0 : Guidance and operational manual*, référence UM_ST31R_GOM_MFP_EV2, version 2, 12 mai 2025. - *Release note MIFARE Plus EV2 library 1.0.3 on ST31R480*, référence RN_ST31R_MFP_EV2_1.0.3, version 1, 2 juin 2025.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - STM_2024_ALC_GEN_v1.1 ; - STM_2022_GNB_STAR_v1.2 ; - STM_2023_RST_CMP_STAR_v1.3 ; - STM_2022_TNS_STAR_v1.0 ; - STM_2024_ST Zaventem_STAR_v1.0.
[CER_IC]	Produit ST31R480 A01 Certifié par l'ANSSI sous la référence ANSSI-CC-2025/07.
[PP0084]	*Protection Profile, Security IC Platform Protection Profile with Augmentation Packages*, version 1.0, 13 janvier 2014. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-PP-0084-2014.

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 5.4.
[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]	*Information technology — Security techniques — Evaluation criteria for IT security* - *Part 1: Introduction and general model :* ISO/IEC 15408-1:2022 ; - *Part 2: Security functional components:* ISO/IEC 15408-2:2022 ; - *Part 3: Security Assurance components:* ISO/IEC 15408-3:2022 ; - *Part 4: Framework for the specification of evaluation methods and activities*: ISO/IEC 15408-4:2022 ; - *Part 5: Pre-defined packages of security requirements*: ISO/IEC 15408-5:2022. Equivalent à la version CCRA: *Common Criteria for Information Technology Security* Evaluation, version CC:2022, révision 1, parties 1 à 5, références CCMB-2022-11-001 à CCMB-2022-11-005.
[CEM]	*Information technology — Security techniques — Evaluation criteria for IT security, ISO/IEC 18045:2022* Equivalent à la version CCRA: *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology,* version *CC:2022,* révision 1, référence CCMB-2022-11-006.
[CC-Errata]	*Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)*, référence 002, version 1.1, 22 juillet 2024.
[CC2022-Transition]	*Transition policy to CC:2022 and CEM:2022*, reference CCMC-2023-04-001, 20 avril 2023.
[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 and similar devices*, version 3.2.1, février 2024.

[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[CCRA]	*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.
[SOG-IS Crypto]	*SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*, version 1.3, février 2023.

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