PREMIER MINISTRE

Schéma Français d'Évaluation et de Certification de la Sécurité des Technologies de l'Information

CERTIFICAT 2001/18

Plate-forme ST19 (technologie 0.6µ) : Micro-circuit ST19SF04A

Développeur : STMicroelectronics SA

EAL4 Augmenté

conforme au profil de protection PP/9806

Commanditaire : STMicroelectronics SA

Le 26 novembre 2001,

Le Commanditaire :
Le Group Vice-President Memory Products,
General Manager Smartcard Products Division
Maurizio Felici

L'Organisme de certification :
Le Directeur central de la sécurité des systèmes d'information
Henri Serres

Ce produit a été évalué par un centre d'évaluation de la sécurité des TI conformément aux Critères Communs pour l'évaluation de la sécurité des TI version 2.1 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 1.0.

Ce certificat ne s'applique qu'à la version évaluée du produit dans sa configuration d'évaluation et selon les modalités décrites dans le rapport de certification associé. L'évaluation a été conduite en conformité avec les dispositions du Schéma français d'évaluation et de certification de la sécurité des TI. Les conclusions du centre d'évaluation enregistrées dans le rapport technique d'évaluation sont cohérentes avec les éléments de preuve fournis.

Ce certificat ne constitue pas en soi une recommandation du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise. Ce certificat n'exprime directement ou indirectement aucune caution du produit par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Organisme de certification :
Secrétariat Général de la Défense Nationale
DCSSI
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

IT Security Certified

Chapitre 1

Résumé

1.1 Objet

1 Ce document représente le rapport de certification du micro-circuit ST19SF04A, bâti sur la plate-forme ST19 de STMicroelectronics et fabriqué sur le site de STMicroelectronics à Agrate (Italie).

2 Ce micro-circuit est destiné à recevoir des applications qui seront installées dans sa mémoire au cours de sa fabrication. Ces logiciels applicatifs (le système d'exploitation de la carte ainsi que les applications éventuelles) ne font pas partie de l'évaluation. Le micro-circuit est ensuite inséré dans un support plastique pour constituer une carte à puce.

3 Le développeur du micro-circuit est STMicroelectronics :

- STMicroelectronics
  ZI de Rousset BP2
  13106 Rousset Cedex
  France.

4 Le site de production des micro-circuits ST19SF04A pour cette évaluation est le suivant :

- STMicroelectronics
  Via C. Olivetti 2
  20041 Agrate Brianza
  Italie.

5 La société Dupont Photomasks a également participé au développement de la cible d'évaluation en tant que développeur et fabricant des réticules :

- Dupont Photomasks
  ZI de Rousset
  13106 Rousset Cedex
  France.

6 L'évaluation a été menée conformément aux Critères Communs [CC] et à la méthodologie définie dans le manuel CEM [CEM].

7 Le niveau d'assurance atteint est le niveau EAL4 augmenté des composants d'assurance suivants décrits dans la partie 3 des Critères Communs [CC] :

- AVA_VLA.4 "Résistance élevée",
- ALC_DVS.2 "Caractère suffisant des mesures de sécurité",

- ADV_IMP.2 “Implémentation de la TSF”,
- ALC_FLR.1 “Correction d’erreurs élémentaire”.

8 Ce produit est conforme au profil de protection “Smartcard Integrated Circuit” enregistré auprès de la DCSSI sous la référence PP/9806, version 2.0 de Septembre 1998 [PP/9806].

9 L’évaluation a été conduite par le Centre d’Evaluation de la Sécurité des Technologies de l’Information de Serma Technologies :

- Serma Technologies
  30, avenue Gustave Eiffel
  33608 Pessac Cedex
  France.

1.2 Contexte de l’évaluation

10 Le micro-circuit ST19SF04A développé par STMicroelectronics SA et produit à Rousset (France) a fait l’objet d’une certification en décembre 2000 [2000/12]. Ce certificat est maintenu dans le cadre du programme de maintenance PM 2000/01 associé à la plate-forme ST19.

11 La réévaluation du micro-circuit ST19SF04A fabriqué à Agrate (Italie) est donc basée sur les résultats de l’évaluation précédente [2000/12] et sur les travaux de maintenance.

12 Le commanditaire de l’évaluation est STMicroelectronics SA :

- STMicroelectronics SA
  ZI de Rousset BP2
  13106 Rousset Cedex
  France.

Chapitre 2

Description de la cible d'évaluation

2.1 Périmètre de la cible d'évaluation

13 La cible d'évaluation, bâtie sur la plate-forme ST19, comporte :

- le micro-circuit ST19SF04A, mask set K4F1 (site de fabrication d'Agrate),
- son logiciel dédié : UFB. Ce logiciel contient notamment des fonctionnalités de tests actives pendant la phase de test du micro-circuit. A l'issue de cette phase, ils ne sont plus accessibles.

14 Pour l'évaluation, le produit a été utilisé avec un logiciel embarqué développé par STMicroelectronics SA appelé "Card Manager" (version QZF). Ce logiciel ne fait pas partie de l'évaluation.

15 Le générateur de nombres non-prédictibles présent sur le micro-circuit ne fait pas partie de cette évaluation.

16 Pour l'évaluation, le micro-circuit est livré en mode "user" uniquement.

2.2 Cycle de vie

17 Le micro-circuit ST19SF04A a été développé par STMicroelectronics SA sur le site de Rousset (France).

18 La production des micro-circuits est effectuée sur les sites de Rousset (France) et d'Agrate (Italie). La présente évaluation ne porte que sur les micro-circuits produits à Agrate.

19 Les tests des micro-circuits sont effectués uniquement sur le site de Rousset.

2.3 Fonctions de sécurité évaluées

20 Les fonctions de sécurité évaluées sont les suivantes :

- démarrage du micro-circuit dans un état sûr,
- contrôle du cyle de vie du micro-circuit,
- contrôle de l'intégrité des mémoires,
- inhibition du mode "Test",
- partitionnement et contrôle d'accès aux mémoires,
- protection contre les attaques physiques,
- détection des évènements de sécurité,
- non-observabilité des opérations critiques.

2.4 Documentation disponible

21 La documentation disponible suivante est à destination des développeurs des applications visant à être masquées sur le micro-circuit :

- ST19SFxx IC Data Sheet ;
- Security Application Manual [SAM].

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

Classes d'Assurance	Composants d'Assurance
Cible de sécurité	ASE_INT.1 : Introduction de la ST ASE_DES.1 : Description de la TOE ASE_ENV.1 : Environnement de sécurité ASE_OBJ.1 : Objectifs de sécurité ASE_PPC.1 : Annonce de conformité à un PP ASE_REQ.1 : Exigences de sécurité des TI ASE_SRE.1 : Exigences de sécurité des TI explicitement énoncées ASE_TSS.1 : Spécifications globales de la TOE
Gestion de configuration	ACM_AUT.1 : Automatisation partielle de la CM ACM_CAP.4 : Aide à la génération et procédures de réception ACM_SCP.2 : Couverture du suivi des problèmes par la CM
Livraison et exploitation	ADO_DEL.2 : Détection de modifications ADO_IGS.1 : Procédures d'installation, de génération et de démarrage
Développement	ADV_FSP.2 : Définition exhaustive des interfaces externes ADV_HLD.2 : Conception de haut niveau - identification des sous-sytèmes dédiés à la sécurité ADV_IMP.2 : Implémentation de la TSF ADV_LLD.1 : Conception de bas niveau descriptive ADV_RCR.1 : Démonstration de correspondance informelle ADV_SPM.1 : Modèle informel de politique de sécurité de la TOE
Guides	AGD_ADM.1 : Guide de l'administrateur AGD_USR.1 : Guide de l'utilisateur

Classes d'Assurance	Composants d'Assurance
Support au cycle de vie	ALC_DVS.2 : Caractère suffisant des mesures de sécurité ALC_FLR.1 : Correction d'anomalies élémentaire ALC_LCD.1 : Modèle de cycle de vie défini par le développeur ALC_TAT.1 : Outils de développement bien définis
Tests	ATE_COV.2 : Analyse de la couverture ATE_DPT.1 : Tests : conception de haut niveau ATE_FUN.1 : Tests fonctionnels ATE_IND.2 : Tests indépendants - échantillonnage
Estimation des vulnérabilités	AVA_MSU.2 : Validation de l'analyse AVA_SOF.1 : Évaluation de la résistance des fonctions de sécurité de la TOE AVA_VLA.4 : Résistance élevée

22 Pour tous les composants d'assurance ci-dessus, un verdict «Réussite» a été émis par l'évaluateur.

23 Le détail des travaux d'évaluation menés est disponible dans le Rapport Technique d'Evaluation [RTE].

24 Le micro-circuit ST19SF04A produit à Rousset (France) étant certifié et maintenu, une partie des verdicts de la présente évaluation s'appuient sur les travaux menés lors de cette précédente évaluation et dans le cadre de la maintenance.

25 La seule modification de la cible de sécurité [ST] est l'ajout du site de production de STMicroelectronics d'Agrate (Italie) dans la description de la cible d'évaluation.

26 Le site de production d'Agrate (Italie) ayant déjà été audité dans la cadre du programme de maintenance, l'évaluateur s'est appuyé sur ces travaux.

3.2 Intégration au programme de maintenance PM 2000/01

27 Le programme de maintenance PM 2000/01 répond aux exigences des Critères Communs définies par les composants AMA_AMP.1 "Plan de maintenance de l'assurance", AMA_CAT.1 "Rapport de classification de composants de la TOE", AMA_SIA.2 "Examen de l'analyse d'impact sur la sécurité" et AMA_EVD.1 "Éléments de preuve du processus de maintenance" tel que décrits dans la partie 3 des Critères Communs [CC-3].

28 Le développeur a fourni une nouvelle version du plan de maintenance décrivant la cible d'évaluation et les caractéristiques de sécurité correspondant au micro-circuit ST19SF04A référencé par sa liste de configuration.

3.3 Tests fonctionnels et de pénétration

3.3.1 Tests développeur

29 Le test des micro-circuits est réalisé par STMicroelectronics sur son site de Rousset (France).

30 L'évaluation des tests fonctionnels realisés par STMicroelectronics ayant déjà été menée lors de l'évaluation précédente du micro-circuit ST19SF04A, l'évaluateur s'est appuyé sur les verdicts précédents.

3.3.2 Tests évaluateur

31 De la même façon, l'évaluateur ayant déjà échantillonné les tests fonctionnels réalisés par STMicroelectronics, il s'est appuyé sur les verdicts précédents.

32 L'évaluateur a également mené une analyse de vulnérabilités, confirmée par des tests de pénétration, pour s'assurer qu'un attaquant disposant d'un potentiel d'attaque élevé (composant AVA_VLA.4) ne peut pas remettre en cause les objectifs de sécurité de la cible d'évaluation suivants sous reserve du respect des recommandations listées au chapitre 4 :

- la cible d'évaluation doit se prémunir contre les attaques physiques,
- la cible d'évaluation doit se prémunir contre le clonage fonctionnel,
- la cible d'évaluation doit assurer la continuité de ses fonctions de sécurité,
- la cible d'évaluation ne doit pas contenir d'erreurs de conception, d'implémentation ou dans son exécution,
- la cible d'évaluation doit se prémunir contre toute divulgation non autorisée de ces mécanismes de sécurité,
- la cible d'évaluation doit se prémunir contre toute divulgation non autorisée des informations sensibles contenues dans les mémoires,
- la cible d'évaluation doit se prémunir contre toute modification non autorisée des informations sensibles contenues dans les mémoires.

33 Les informations sensibles désignent :

- les données applicatives chargées en EEPROM telles que les données de pré-personalisation,
- le logiciel dédié du micro-circuit.

Chapitre 4

Certification

4.1 Verdict

34 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL4 augmenté des composants d'assurance suivants décrits dans la partie 3 des Critères Communs [CC] :

- AVA_VLA.4 "Résistance élevée",
- ALC_DVS.2 "Caractère suffisant des mesures de sécurité",
- ADV_IMP.2 "Implémentation de la TSF",
- ALC_FLR.1 "Correction d'erreurs élémentaire".

4.2 Recommandations

35 La cible d'évaluation "ST19SF04A", bâtie sur la plate-forme ST19 et produit sur le site de STMicroelectronics à Agrate (Italie), est soumise aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

a) le développeur du logiciel embarqué doit respecter les recommandations du guide de programmation du micro-circuit [SAM]. Pour garantir la confidentialité du code exécuté, il doit impérativement prendre les mesures suffisantes pour garantir le caractère imprédictible de l'exécution du code embarqué.

b) le développeur du logiciel embarqué doit garantir la confidentialité des informations de conception du micro-circuit qui lui sont transmises.

c) le système dans lequel sera utilisé le micro-circuit doit garantir la confidentialité et l'intégrité des données sensibles qui sont installées dans les mémoires.

4.3 Certification

36 La certification ne constitue pas en soi une recommandation du produit. Elle ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

37 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 2. La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

38 Ce produit figure désormais au programme de maintenance PM 2000/01 des composants certifiés batis sur la plate-forme ST19.

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement.
Cible d'évaluation	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	Un paquet composé de composants d'assurance tirées de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Une expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	Un ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection	Un ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Annexe B

Références

[CC] Critères Communs pour l'évaluation de la sécurité des technologies de l'information :
- Partie 1 : Introduction et modèle général CCIMB-99-031, version 2.1 Août 1999.
- Partie 2 : Exigences fonctionnelles de sécurité CCIMB-99-032, version 2.1 Août 1999.
- Partie 3 : Exigences d'assurance de sécurité CCIMB-99-033, version 2.1 Août 1999.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information :
- Partie 2 : Méthodologie d'évaluation CEM-99/045, version 1.0 Août 1999.

[PP/9806] Profil de protection PP/9806, "Smartcard Integrated Circuit, Version 2.0", septembre 1998.

[2000/12] Rapport de certification 2000/12 «Plate-forme ST19 (technologie 0.6µ) : Micro-circuit ST19SF04ABxyz», SCSSI, décembre 2000.

[ST] Cible de sécurité «ST19SFxx Platform Security Target», version 1.5, réf. ST.AZUR.001/0006V1_5, STMicroelectronics.

[RTE] Rapport d'évaluation «Maintenance of platform ST19SFxx: phase 2», Serma Technologies, réf. AZUR2_AMA_SIA v2.0, Serma Technologies, 20 juillet 2001 (diffusion contrôlée).

[SAM] Security Application Manual, Version 1.2, réf. APM.19.SECU/ 0006V1.2, 30 juin 2000 (diffusion contrôlée).

Ce rapport de certification est disponible sur le site internet de la Direction centrale de la sécurité des systèmes d'information à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau Certification
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

certification.dcssi@sgdn.pm.gouv.fr