PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

SERVICE CENTRAL DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Rapport de certification 2000/09

Microcircuit S3C8975 pour carte à puce

Décembre 2000

Ce document constitue le rapport de certification du produit “Microcircuit S3C8975 pour carte à puce”.

Ce rapport de certification est disponible sur le site internet du Service Central de la Sécurité des Systèmes d'Information à l'adresse suivante :

www.scssi.gouv.fr

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

Secrétariat général de la défense nationale
SCSSI
Centre de Certification de la Sécurité des Technologies de l’Information
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Mél: ssi20@calva.net

Ce document est folioté de 1 à 26 et certificat.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

CERTIFICAT 2000/09

Microcircuit S3C8975 pour carte à puce

Développeur : Samsung Electronics

EAL1 augmenté

Commanditaire : Samsung Electronics

Le 15 décembre 2000,

Le Commanditaire :
Le Directeur R&D Smart Card Ics
M. Chilhee CHUNG

L'Organisme de certification :
Le Directeur chargé de la sécurité des systèmes d'information
M. 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
SCSSI
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

IT Security Certified

Common Criteria

Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit “Microcircuit S3C8975 pour carte à puce” développé par Samsung Electronics.

2 Le niveau d’assurance atteint est le niveau EAL1 augmenté du composant d’assurance AVA_VLA.2 “Analyse de vulnérabilités indépendante” tel que décrit dans la partie 3 des Critères Communs [3].

3 Ce produit est basé sur le profil de protection “Smartcard Integrated Circuit” enregistré auprès du SCSSI dans le catalogue des profils de protection certifiés sous la référence PP/9806 [7]. Il ne peut cependant pas s’y réclamer conforme car le niveau d’assurance atteint est différent de celui annoncé dans le profil de protection qui vise un niveau EAL4 augmenté.

Chapitre 2

Résumé

2.1 Contexte de l'évaluation

4 L'évaluation a été menée conformément aux Critères Communs ([1] à [3]) et à la méthodologie définie dans le manuel CEM [4].

5 Elle s'est déroulée consécutivement au développement du produit de septembre 2000 à novembre 2000. La durée de l'évaluation a pu être considérablement réduite du fait qu'une préparation à l'évaluation avait été conduite préalablement au démarrage de l'évaluation.

6 Le commanditaire de l'évaluation est (ci-après "le commanditaire") :

- Samsung Electronics
  San#24 Nongseo-Ri, Kiheung-Eup
  Yongin-City, Kyunggi-Doh
  449-900, Corée.

7 Le commanditaire est aussi développeur de la cible d'évaluation.

8 Dans le cadre de cette évaluation, une entité de Samsung Electronics localisée en France a apporté son concours ; il s'agit de :

- Samsung Semiconductor France
  Centre d'affaires La Boursidière
  RN 186, Bâtiment Champagne, BP 202
  92357 Le Plessis Robinson, France.

9 L'évaluation a été conduite par le centre d'évaluation de la sécurité des technologies de l'information (ci-après "CESTI") suivant :

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

2.2 Description de la cible d'évaluation

10 La cible d'évaluation est le produit "Microcircuit S3C8975 pour carte à puce" : elle se compose du microcircuit S3C8975 et de son logiciel dédié.

11 Elle est destinée à être utilisée dans le cadre d'applications bancaires, de télévision à péage, de transport, de santé, de télécommunications, …

12 Les logiciels applicatifs (système d'exploitation, application spécifique, …) qui seront embarqués sur le microcircuit S3C8975 ne font pas l'objet de la présente évaluation et certification.

13 Ce produit est basé sur le profil de protection "Smartcard Integrated Circuit" enregistré auprès du SCSSI dans le catalogue des profils de protection certifiés sous la référence PP/9806 [7]. Il ne peut cependant pas s'y réclamer conforme car le niveau d'assurance atteint est différent de celui annoncé dans le profil de protection.

14 Le détail des fonctions de sécurité évaluées résumées ci-après est disponible dans la cible de sécurité [5] :

- réaction à des violations potentielles de la sécurité,
- contrôle d'accès et protection des mémoires,
- irréversibilité des phase de vie,
- non-observabilité des opérations du composant,
- autotest.

2.3 Conclusions de l'évaluation

15 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [3].

16 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL1 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élémentaire tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

17 L'utilisation de la cible d'évaluation de manière sûre est soumise aux recommandations figurant au chapitre 6 du présent rapport.

Chapitre 3

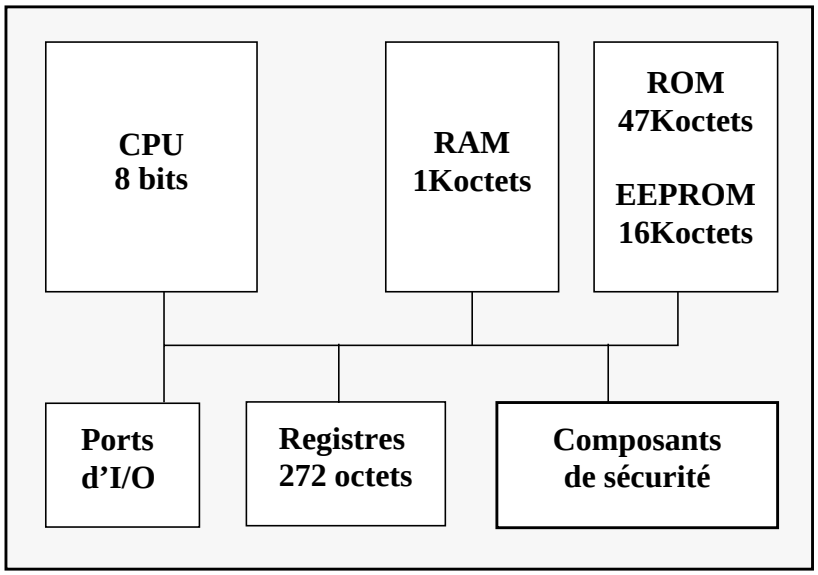
Identification de la cible d'évaluation

3.1 Objet

18 La cible d'évaluation est le "Microcircuit S3C8975 pour carte à puce" développée par Samsung Electronics. Elle comporte le microcircuit S3C8975 et son logiciel dédié.

19 Ce microcircuit est destiné à recevoir les logiciels fournis par les développeurs d'application, masqués dans la mémoire de programme (ROM) au cours de la fabrication du microcircuit. Ces logiciels applicatifs (le système d'exploitation de la carte ainsi que les applications éventuelles) ne font pas partie de l'évaluation. Le microcircuit est ensuite inséré dans une carte porteur de format carte de crédit ou tout autre support.

20 Le microcircuit électronique S3C8975 dispose d'une unité centrale de 8 bits associée à une mémoire de travail de 1Koctet (RAM), d'une mémoire de programme de 47Koctets (ROM), d'une mémoire non volatile de 16Koctets (EEPROM) et de registres occupant un espace global de 272 octets. Il dispose également de différents composants de sécurité (détecteurs, NMI, …).



Tab. 3.1 - Modèle d'architecture du microcircuit S3C8975

3.2 Historique du développement

21 Le composant S3C8975 a été développé et produit par Samsung Electronics sur le site de Yongin-City en Corée.

3.3 Cycle de vie de la cible d'évaluation

22 Le cycle de vie d'une carte à puce est constitué des phases suivantes :

- phase 1 : développement des logiciels embarqués (systèmes d'exploitation, logiciels applicatifs),
- phase 2 : développement du microcircuit et du logiciel dédié,
- phase 3 : production du microcircuit,
- phase 4 : mise en micro-modules (ateliers de micro-électronique),
- phase 5 : encartage,
- phase 6 : personnalisation,
- phase 7 : utilisation du produit final.

23 La construction de la cible d'évaluation est constituée des phases 2 et 3, y compris la livraison des logiciels embarqués entre les phases 1 et 2 et la livraison du microcircuit entre les phases 3 et 4.

24 Les phases 4 à 7 sont les phases d'exploitation de la cible d'évaluation.

3.4 Description du matériel

25 La cible d'évaluation est composée du microcircuit S3C8975 référencé S3C8975X01-DP. C'est un microcircuit 8 bits en technologie CMOS.

26 Il dispose de différents mécanismes de sécurité participant à la réalisation des fonctions dédiées à la sécurité pour lesquelles l'évaluation a été demandée.

3.5 Description du logiciel

27 La cible d'évaluation contient également un logiciel dédié référencé S3C8975 TEST-ROM code, version 1.0. Ce logiciel contient des fonctionnalités de tests actives pendant la phase de test du microcircuit. A l'issue de cette phase, elles ne sont plus accessibles.

28 La cible d'évaluation a été livrée à l'évaluateur avec un software embarqué propriétaire qui permet d'exploiter les fonctions de sécurité. Ce logiciel ne fait pas partie de l'évaluation.

3.6 Description de la documentation

29 La documentation d'exploitation de la cible d'évaluation est la suivante :

- le manuel utilisateur [9] ;
- les notes d'application sécuritaires [10].

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

30 Les caractéristiques de sécurité évaluées sont consignées dans la cible de sécurité [5] qui est la référence pour l'évaluation. Les paragraphes ci-après reformulent les éléments essentiels de ces caractéristiques.

4.2 Hypothèses

31 La cible d'évaluation doit être utilisée dans un environnement qui satisfait aux hypothèses énoncées dans le profil de protection [7].

32 Ces hypothèses couvrent les aspects suivants :

- protection du logiciel embarqué pendant son développement,
- livraison de la cible d'évaluation entre les différentes étapes de son cycle de vie (phases 4 à 7),
- utilisation de la cible d'évaluation pendant les phases de production (phases 4 à 6),
- protection des données sensibles de la cible d'évaluation échangées avec les équipements avec lesquels elle dialogue (terminaux, …).

33 Le détail de ces hypothèses est disponible dans la cible de sécurité [7].

4.3 Menaces

34 Les biens à protéger au sein de la cible d'évaluation sont définis comme étant les données applicatives du microcircuit, le logiciel dédié, les données de spécification et de conception du microcircuit.

35 Les menaces couvertes par la cible d'évaluation ou par son environnement sont celles définies par le profil de protection [7]. Elles peuvent être résumées comme suit :

- modification non autorisée de la conception du circuit, des logiciels dédiés et des données applicatives du microcircuit,
- divulgation non autorisée de la conception du circuit, des logiciels dédiés, des données applicatives du microcircuit, des informations de tests et des outils de développement.

4.4 Politiques de sécurité organisationnelles

36 La cible de sécurité, tout comme le profil de protection [7] ne définit pas de politique de sécurité organisationnelle.

4.5 Fonctions de sécurité évaluées

37 Les fonctions de sécurité évaluées sont disponible dans la cible de sécurité [5]. Ces fonctions de sécurité peuvent être résumées comme suit :

- détection de l'utilisation de la cible d'évaluation en dehors de ses spécifications de fonctionnement et réaction associée,
- détection d'une tentative de modification physique de la cible d'évaluation et réaction associée,
- brouillage de la consommation de courant,
- configuration des droits d'accès aux mémoires et détection des accès illégaux,
- irréversibilité des phases du cycle de vie de la cible d'évaluation.

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

38 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation [6] produit par Serma Technologies.

5.2 Principaux résultats de l'évaluation

39 Le produit répond aux exigences des Critères Communs pour le niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [3].

5.2.1 ASE : Evaluation de la cible de sécurité

40 Les critères d'évaluation sont définis par les sections ASE_DES.1.iE, ASE_ENV.1.iE, ASE_INT.1.iE, ASE_OBJ.1.iE, ASE_PPC.1.iE, ASE_REQ.1.iE, ASE_SRE.1.iE et ASE_TSS.1.iE de la classe ASE, telle que spécifiée dans la partie 3 des Critères Communs [3].

41 La cible d'évaluation est le produit "Microcircuit S3C8975 pour carte à puce", développée par Samsung Electronics.

42 Les travaux d'évaluation de la cible de sécurité ont pu être limités du fait de sa conformité à un profil de protection [7] certifié.

5.2.2 ACM_CAP.1 : Numéros de version

43 Les critères d'évaluation sont définis par la section ACM_CAP.1.iE de la classe ACM, telle que spécifiée dans la partie 3 des Critères Communs [3].

44 Le développeur a clairement identifié la cible d'évaluation avec une référence unique. La cible d'évaluation est composée du microcircuit S3C8975 référencé S3C8975X01-DP et du logiciel dédié référencé S3C8975 TEST-ROM code, version 1.0.

45 L'évaluateur a vérifié que la cible d'évaluation portait cette référence unique.

5.2.3 ADO_IGS.1 : Procédures d'installation, de génération et de démarrage

46 Les critères d'évaluation sont définis par les sections ADO_IGS.1.iE de la classe ADO, telle que spécifiée dans la partie 3 des Critères Communs [3].

47 Pour ce type de cible d'évaluation, les procédures d'installation, de génération et de démarrage correspondent aux opérations permettant de passer du mode test au mode utilisateur. Dans le cas présent, ces procédures sont appliquées par le développeur, et font partie de la phase de conception de la cible d'évaluation.

48 Aucune tâche particulière n'a été conduite par l'évaluateur pour couvrir cet aspect.

5.2.4 ADV_FSP.1 : Spécifications fonctionnelles informelles

49 Les critères d'évaluation sont définis par les sections ADV_FSP.1.iE de la classe ADV, telle que définie dans la partie 3 des Critères Communs [3].

50 Le développeur a fourni la documentation spécifiant les fonctions de sécurité de la cible d'évaluation et leurs interfaces externes.

51 L'évaluateur a examiné ces spécifications et montré qu'elles représentent une description complète et homogène des fonctionnalités de sécurité du produit.

5.2.5 ADV_RCR.1 : Démonstration de correspondance informelle

52 Les critères d'évaluation sont définis par la section ADV_RCR.1.1E de la classe ADV, telle que spécifiée dans la partie 3 des Critères Communs [3].

53 Le développeur a fourni une documentation qui indique les correspondances entre les différents niveaux de représentation des fonctions de sécurité de la cible d'évaluation.

54 L'évaluateur a vérifié que les fonctionnalités de sécurité définies au niveau des spécifications globales de la cible d'évaluation sont complètement et correctement décrites au niveau des spécifications de sécurité informelles.

5.2.6 AGD_ADM.1 : Guide de l'administrateur

55 Les critères d'évaluation sont définis par la section AGD_ADM.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [3].

56 Le développeur a fourni trois documents d'administration des fonctions de sécurité du produit :

- les notes d'application [8] à l'usage de l'administrateur de test;
- le manuel utilisateur [9] à l'usage du développeur de logiciel embarqué ;
- les notes d'application sécuritaires [10] à l'usage du développeur de logiciel embarqué.

57 L'administrateur de test et le développeur de logiciel embarqué sont les deux types d'administrateur de la cible d'évaluation.

58 L'évaluateur s'est assuré de l'absence d'incohérence dans cette documentation et a vérifié que ces procédures permettent une administration sûre du produit.

5.2.7 AGD_USR.1 : Guide de l'utilisateur

59 Les critères d'évaluation sont définis par la section AGD_USR.1.1E de la classe AGD, telle que spécifiée dans la partie 3 des Critères Communs [3].

60 Aucune fonction de sécurité de la cible d'évaluation est considérée comme une fonction d'utilisation : elles sont toutes considérées comme des fonctions d'administration.

61 Aucune tâche particulière n'a été conduite par l'évaluateur pour couvrir cet aspect.

5.2.8 ATE_IND.1 : Tests indépendants - conformité

62 Les critères d'évaluation sont définis par les sections ATE_IND.2.iE de la classe ATE, telle que spécifiée dans la partie 3 des Critères Communs [3].

63 L'évaluateur a vérifié, en effectuant un ensemble de tests sur la cible d'évaluation, que le microcircuit se comporte conformément à ses spécifications de sécurité.

5.2.9 AVA_VLA.2 : Analyse de vulnérabilités indépendante

64 Les critères d'évaluation sont définis par les sections AVA_VLA.3.iE de la classe AVA, telle que spécifiée dans la partie 3 des Critères Communs [3].

65 Le développeur a fourni une documentation d'analyse des vulnérabilités potentielles du produit.

66 L'évaluateur a examiné cette fourniture et réalisé sa propre analyse de vulnérabilités indépendante.

67 Il a réalisé des tests de pénétration, basés sur son analyse de vulnérabilités, afin de pouvoir vérifier que le produit résiste aux attaques correspondant à un potentiel de l'attaquant élémentaire tel que défini par le composant AVA_VLA.2 "Analyse de vulnérabilités indépendante".

5.2.10 Verdicts

68 Pour tous les aspects des critères communs identifiés ci-dessus, un avis "réussite" a été émis.

Chapitre 6

Recommandations d'utilisation

69 Le produit "Microcircuit S3C8975 pour carte à puce" est soumis aux recommandations d'utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

- le produit doit être utilisé conformément à l'environnement d'utilisation prévu dans la cible de sécurité [5] ;

- le produit doit être utilisé conformément aux guides [9] et [10].

Chapitre 7

Certification

7.1 Objet

70 Le produit soumis à évaluation satisfait aux exigences du niveau EAL1 augmenté du composant d'assurance AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [3].

71 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau EAL1 et par la compétence, l'opportunité et les ressources correspondant à un potentiel d'attaque élémentaire tel qu'il est spécifié par le composant d'assurance AVA_VLA.2.

7.2 Portée de la certification

72 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.

73 Le certificat ne s'applique qu'à la version évaluée du produit identifiée au chapitre 3.

74 La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

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.
Encartage	Insertion du composant masqué dans un support plastique, en forme de carte.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Logiciel embarqué	Logiciel présent sur une puce.
Masque	Ensemble d'instructions organisées, reconnaissables et exécutables par le processeur d'un microcircuit électronique.
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.
Personnalisation	Inscription dans la mémoire de données du composant masqué des données spécifiques à une application.

Politique de sécurité organisationnelle	Une ou plusieurs règles, procédures, codes de conduite ou lignes directrices de sécurité qu'une organisation impose pour son fonctionnement.
Porteur	Utilisateur final de la carte.
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.

Acronymes

CMOS	Complementary Metal Oxyd Semiconductor
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable and Programmable Read Only Memory
RAM	Random Access Memory
ROM	Read Only Memory

Annexe B

Références

[1] [CC-1] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 1 : Introduction et modèle général CCIB-99-031, version 2.1 Août 1999.

[2] [CC-2] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 2 : Exigences fonctionnelles de sécurité CCIB-99-032, version 2.1 Août 1999.

[3] [CC-3] Critères Communs pour l'évaluation de la sécurité des technologies de l'information Partie 3 : Exigences d'assurance de sécurité CCIB-99-033, version 2.1 Août 1999.

[4] [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.

[5] Cible de sécurité pour S3C8975 version 1.1, 13 octobre 2000 (diffusion contrôlée).

[6] Rapport technique d'évaluation DUNE-2_ETR v1.0, 17 novembre 2000 (diffusion contrôlée).

[7] Profil de protection "Smartcard Integrated Circuit", version 2.0 de septembre 1999, enregistré sous la référence PP/9806 (document public).

[8] Test-Administrator Application Note, 8-bit CMOS Microcontroller for Smart Card, S3C8975, version 1.0, 13 october 2000 (diffusion contrôlée).

[9] User's manual S3C8975, 8-bit CMOS Microcontroller for Smart Card, revision 1 (diffusion contrôlée).

[10] Security Application Note, 8-bit CMOS Microcontroller for Smart Card, S3C8975, version 1.1, 13 october 2000 (diffusion contrôlée).