Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale 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 2002/25

SAMSUNG S3CC9PB microcontroller

(Référence S3CC9PBX01)

SÉCURITÉ TI CERTIFICATION

Décembre 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

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

CERTIFICAT 2002/25

SAMSUNG S3CC9PB microcontroller

(Référence S3CC9PBX01)

Développeur : Samsung Electronics

Critères Communs

EAL4 Augmenté

(ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

Conforme au profil de protection PP/9806

Commanditaire : Samsung Electronics

Centre d'évaluation : Serma Technologies

Le 9 décembre 2002,

Le Directeur central de la sécurité
des systèmes d'information
Henri Serres

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information publié au journal officiel de la République française le 19 avril 2002.

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.

Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Chapitre 1

Présentation

Executive Summary

1.1 Objet

Purpose

1 Ce document est le rapport de certification du micro-circuit S3CC9PB (Référence S3CC9PBX01).

This document is the certification report of the S3CC9PB microcontroller (reference S3CC9PBX01).

2 Ce produit est développé par Samsung Electronics :

The developer of the product is Samsung Electronics:

- Samsung Electronics
  449-711, San#24 Nongseo-Ri,Giheung-Eup
  Yongin-City, Gyeonggi-Do
  Corée.

3 Ce produit est fabriqué sur le site Samsung de Kiheung :

The product is manufactured in the Samsung Kiheung site:

- Samsung Electronics
  449-711, San#24 Nongseo-Ri,Giheung-Eup
  Yongin-City, Gyeonggi-Do
  Corée.

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

This evaluation has been performed in conformance with Common Criteria [CC] and with the methodology defined in the CEM [CEM].

5 La cible d'évaluation atteint le niveau d'assurance EAL 4 augmenté des composants d'assurance suivants tirés de la partie 3 des Critères Communs :

The target of the evaluation reaches the EAL 4 assurance level augmented with the following Common Criteria Part 3 components:

- ADV_IMP.2 "Implementation of the TSF",
- ALC_DVS.2 "Sufficiency of security measures",
- AVA_VLA.4 "Highly resistant".

6 La cible d'évaluation est conforme au profil de protection «Smartcard Integrated Circuit» enregistré auprès de la DCSSI sous la référence PP/9806 [PP/9806].

The target of the evaluation is compliant with the protection profile «Smartcard Integrated Circuit» registered by the DCSSI with the reference PP/9806 [PP/9806].

1.2 Contexte de l'évaluation

Evaluation Context

7 L'évaluation s'est déroulée de décembre 2001 à novembre 2002.

The evaluation has been carried out from december 2001 to november 2002.

8 Le commanditaire de l'évaluation est Samsung Electronics :

The sponsor of the evaluation is Samsung Electronics:

- Samsung Electronics
  449-711, San#24 Nongseo-Ri,Giheung-Eup
  Yongin-City, Gyeonggi-Do
  Corée.

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

The evaluation has been performed by the Information Technology Security Evaluation Facility of Serma Technologies:

- Serma Technologies
  30 Avenue Gustave Eiffel
  33608 Pessac Cedex
  France.

Chapitre 2

Description de la cible d'évaluation

Description of the Target of Evaluation

2.1 Périmètre de la cible d'évaluation

Scope of the Target of Evaluation

10 La cible d'évaluation est le micro-circuit S3CC9PB (référence S3CC9PBX01) développé par Samsung Electronics en technologie CMOS.

The target of evaluation is the S3CC9PB (reference S3CC9PBX01) microcontroller developped by Samsung Electronics with CMOS technologie.

11 Le micro-circuit est destiné à être utilisé dans une carte à puce, indépendamment de son interface physique et de la façon dont il est encarté. Une carte à puce peut être composée d'autres éléments (tels que des batteries ou une antenne) mais ces éléments ne sont pas inclus dans la cible d'évaluation.

The single chip microcontroller unit is to be used in a smart card product, independent of the physical interface and the way it is packaged. Generally, a smart card product may include other elements (such as batteries or antenna,...), but these are not in the scope of the target of evaluation.

12 La cible d'évaluation est constituée des éléments suivants :

The target of evaluation is composed of the following parts:

- Une partie matérielle :
  Hardware part:
  - un processeur CalmRISC 16 bit conçu en technologie Harvard qui consiste à séparer la mémoire des programmes de la mémoire des données. Les instructions et les données peuvent être ainsi chargées simultanément.
    a CalmRISC16 CPU following Harvard style ; it has separate program memory and data memory. Both instruction and data can be fetched simultaneously without causing a stall, using separate paths for memory access.
  - des mémoires de type ROM pour les programmes (160K bytes), des mémoires de type EEPROM pour les programmes et données (6K bytes), des mémoires de type RAM pour les données (6K bytes).
    160K bytes of program memory (ROM), 64K bytes of program/data memory (EEPROM), 6K bytes of data memory (RAM).
  - des modules de sécurité : détecteurs d'évènements anormaux avec notification et redémarrage possible du micro-circuit, timers, données sécuritaires en zone protégée, module de protection de la mémoire (contrôle d'accès).
    security modules: abnormal condition detectors with flag/reset action, timers, data security, memory protection unit (access control).
  - des modules fonctionnels : gestion des entrées/sorties en mode asynchrone (ISO 7816), générateur d'aléas, accélérateur DES/3-DES, co-processeur pour cryptographie à clés publiques.

fonctionnal modules: ISO 7816 compatible asynchronous serial I/O interface, Random Number Generator, DES/3-DES Accelerator, Crypto-coprocessor for public key cryptography.

- une partie logicielle en ROM intégrant des logiciels de tests du micro-circuit et des librairies (gestion du système, services cryptographiques). La version du micro-circuit évalué est S3CC9PBX01 (Test-ROM en version 1.0 et librairie crypto en version 1.0).
  A software part in ROM including test software of the microcontroller and library (system management, cryptographics services). The version of the evaluated microcontroller is S3CC9PBX01 (Test-ROM version 1.0, Crypto Library version 1.0).

13 Le micro-circuit nécessite un logiciel embarqué pour tester certaines caractéristiques de sécurité lors des phases de développement et d'évaluation. En phase d'utilisation finale, ce logiciel de test n'est plus accessible.

The microcontroller requires embedded software to test the device and demonstrate certain security characteristics during the development and evaluation phases. In the end-usage phase the embedded test software is not available.

2.2 Mode d'utilisation de la cible d'évaluation

Target of Evaluation Mode of Operation

14 La micro-circuit est évalué dans les modes suivants :

The microcontroller is evaluated in the following modes:

- mode "test" : c'est le mode dans lequel se trouve la cible d'évaluation jusqu'aux tests finaux. L'administrateur de test a accès uniquement à la zone "test" de la ROM. La cible d'évaluation est testée à l'aide d'une partie du logiciel dédié dans l'environnement sécurisé du développeur. Ce mode est bloqué de façon irréversible lors du passage en mode user ;
  test configuration: It is the target of evaluation configuration up to the final tests. The Test administrator has only access to the Test-ROM. The target of evaluation is tested with a part of the dedicated software within the secure developer premises. This test configuration is locked when the TOE is delivered to the next user, and the part cannot be reversed to the «test» configuration ;
- mode "user" : mode d'utilisation final. Les fonctionnalités de test développeur sont inhibées. L'utilisateur n'a accès qu'à la zone "user" de la ROM. Le logiciel embarqué pilote complètement les fonctionnalités du micro-circuit.
  user configuration: final TOE configuration. The developer test functionalities are unavailable. The user has only access to the User-ROM. The TOE functionality is driven exclusively by the embedded software.

2.3 Fonctions de sécurité

Security Functions

15 Les fonctions de sécurité de la cible d'évaluation sont décrites dans la cible de sécurité [ST] :

The security functions of the target of evaluations are described in the security tagret [ST]:

- Notification et réaction suite aux violations de la sécurité ;
  Security violation recording and reaction ;

- Horloge interne variable ;
  Internal variable clock ;
- Contrôle d'accès aux registres de sécurité ;
  Security register access control ;
- Accès à une adresse non valide ;
  Invalid address access ;
- Contrôle d'accès au code exécuté en EEPROM ;
  Access rights for the code executed in EEPROM ;
- Non reversibilité du mode user en mode test ;
  Non reversibility of test configuration and user configuration ;
- Brouillage des bus d'adresses et de données ;
  Address/Data bus scrambling ;
- Protocole de communication en mode test et commande de test ;
  Test mode communication protocol and test commands ;
- Test ;
  Test ;
- Filtrage haute fréquence ;
  High frequency filter ;
- Filtrage du bruit sur le signal d'horloge ;
  Clock noise filter ;
- Filtrage du bruit sur le signal du "reset" ;
  Reset noise filter ;
- Synthèse du coeur processeur ;
  Synthetisable processor core ;
- Chiffrement des données ;
  Data encryption standard engine ;
- Co-processeur cryptographique ;
  Cryptographic coprocessor ;
- Générateur d'aléas.
  Random number generator.

2.4 Guides d'utilisation

Guidance Document

16 La cible d'évaluation est livrée avec les guides d'utilisation et d'administration suivants :

The available guidance documents for the target of evaluation are:

- Guidance Documents, Version 1.5, issued on October 22, 2002 ;
- User's Manual- S3CC9PB 16-Bit RISC Microcontroller for Smart Card - revision 1.0 ;
- User's Manual Errata - S3CC9PB 16-Bit RISC Microcontroller for Smart Card - revision 1.0 ;
- Programmer's Guide - S3CC9PB 16-Bit RISC Microcontroller for Smart Card - version 0.48, issued on March 14th, 2002 ;
- Security Application Note - S3CC9PB 16-Bit RISC Microcontroller for Smart Card - version 1.2, issued on October 22th, 2002 ;
- Test Administrator Guidance - S3CC9PB 16-Bit RISC Microcontroller for Smart Card - version 1.31, issued on April 3rd, 2002.

Chapitre 3

Résultats de l'évaluation

Evaluation Results

3.1 Exigences de sécurité d'assurance

Security Assurance Requirements

17 La cible d'évaluation a été évaluée au niveau EAL 4 augmenté des composants d'assurance suivants, tirés de la partie 3 des Critères Communs [CC] : ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4.

The target of evaluation has been evaluated at the EAL4 assurance level augmented with the following Common Criteria Part 3 components: ADV_IMP.2, ALC_DVS.2 and AVA_VLA.4.

Assurance class	Assurance components
Security Target	ASE Security target evaluation
Configuration management	ACM_AUT.1 Partial CM automation ACM_CAP.4 Generation support and acceptance procedures ACM_SCP.2 Problem tracking CM coverage
Delivery and operation	ADO_DEL.2 Detection of modification ADO_IGS.1 Installation, generation , and start-up procedures
Development	ADV_FSP.2 Fully defined external interfaces ADV_HLD.2 Security enforcing high-level design **ADV_IMP.2 * Implementation of the TSF** ADV_LLD.1 Descriptive of low-level design ADV_RCR.1 Informal correspondance demonstration ADV_SPM.1 Informal TOE security policy model
Guidance documents	AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
Life cycle support	**ALC_DVS.2 * Sufficiency of security measures** ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: high-level design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_MSU.2 validation of analysis AVA_SOF.1 Strength of TOE security functions **AVA_VLA.4 * Highly resistant**

* EAL4 augmentations

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

For all the above assurance requirements, a «pass» verdict has been issued by the evaluator.

19 Les travaux d'évaluation qui ont été menés sont décrits dans le Rapport Technique d'Evaluation [RTE].

The evaluation tasks which have been done are described in the Evaluation Technical Report [RTE].

20 Dans le cadre des travaux d'évaluation, un audit organisationnel du site de développement de Samsung Electronics (Giheung plant) à Yongin-City, Gyeonggi-Do (Corée) a été réalisé. Cet audit a permis de s'assurer de l'application de mesures de sécurité suffisantes pour protéger la cible d'évaluation et la documentation associée lors de son développement et de sa fabrication.

During the evaluation, a visit has been performed on the development site of Samsung Electronics (Giheung plant) in Yongin-City, Gyeonggi-Do (Korea). This visit gives confidence in the application of sufficient security measures to protect the target of the evaluation and its associated documentation.

3.2 Tests fonctionnels et de pénétration

Functional and penetration testing

21 Le développeur a fourni sa documentation de test fonctionnel du produit. Ces tests sont réalisés par Samsung Electronics sur son site de Giheung, Yongin-City, Gyeonggi-Do (Corée).

The developer of the target of evaluation has provided its test documentation. Functional testing is performed by Samsung Electronics in the site of Giheung, Yongin-City, Gyeonggi-Do (Korea).

22 L'évaluateur a réalisé de son côté des tests fonctionnels pour s'assurer par échantillonnage que les fonctions de sécurité fonctionnent effectivement.

The evaluator has performed independent tests to check by sampling that the TOE security functions perform as specified.

23 L'évaluateur a 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. Ces objectifs sont décrits dans la cible de sécurité [ST], ils concernent principalement les aspects suivants :

The evaluator lead a vulnerability analysis, confirmed by penetration testing, to ensure that an attacker with a high attack potential (AVA_VLA.4 assurance requirements) cannot bypass the security objectives for the target of evaluation. These security objectives are described in the security target [ST], it can be summarised as follow:

- la cible d'évaluation doit se prémunir contre les attaques physiques,
  the TOE must prevent physical tampering with its security critical parts,
- la cible d'évaluation doit se prémunir contre le clonage fonctionnel,
  the TOE functionality needs to be protected from cloning,
- la cible d'évaluation doit assurer la continuité de ses fonctions de sécurité,
  the TOE must ensure the continued correct operation of its security functions,
- la cible d'évaluation ne doit pas contenir d'erreur de conception, d'implémentation ou d'exécution,

the TOE must not contain flaws in design, implementation or operation,

- la cible d'évaluation doit se prémunir contre toute divulgation non autorisée de ses mécanismes de sécurité physique,
  the TOE shall ensure that the hardware security mechanisms are protected against unauthorized disclosure,
- la cible d'évaluation doit se prémunir contre toute divulgation non autorisée des informations sensibles contenues dans ses mémoires,
  the TOE shall ensure that sensitive information stored in memories is protected against unauthorized access,
- la cible d'évaluation doit se prémunir contre toute modification non autorisée des informations sensibles contenues dans ses mémoires,
  the TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification,
- la cible d'évaluation doit fournir des services de calculs cryptographiques tels que la génération d'aléas, le chiffrement/déchiffrement DES et triple DES, le chiffrement/déchiffrement RSA,
  the TOE Shall ensure cryptographic calculations such as generation of random numbers, DES, Triple DES and RSA encryption/ decryption.

3.3 Cotation des mécanismes cryptographiques

Evaluation of cryptographic mechanisms

24 La cible d'évaluation ne dispose pas de fonctions utilisant des mécanismes de nature cryptographique pour assurer sa propre sécurité.

The target of evaluation does not use for its own security any functions based on cryptographic mechanisms.

Chapitre 4

Certification

Certification

4.1 Verdict

Verdict

25 Le micro-circuit satisfait aux exigences du niveau EAL 4 augmenté des composants d'assurance suivants extrtaits de la partie 3 des Critères Communs [CC] :

The microcontroller satisfies to the requirements of the EAL 4 assurance level augmented with the following Common Criteria Part 3 components [CC]:

- ADV_IMP.2 "Implementation of the TSF",
- ALC_DVS.2 "Sufficiency of security measures",
- AVA_VLA.4 "Highly resistant".

26 La cible d'évaluation est également conforme au profil de protection PP/9806.

The target of the evaluation is also compliant with the protection profile PP/9806.

4.2 Restrictions

Restriction

27 Le micro-circuit doit être utilisé dans sa configuration précisée au chapitre 2 et conformément aux procédures d'utilisation et d'administration prescrites dans la cible de sécurité [ST].

The microcontroller shall be used in the configuration described in the chapter 2 and shall be used in the environment described in the security target [ST].

28 Les recommandations du développeur décrites dans les guides d'utilisation doivent impérativement être respectées.

The requirements present in the user and administrator guidance shall be respected.

29 Dans le cas où le générateur d'aléas serait utilisé à des fins cryptographiques, il est fortement conseillé de le combiner à un mécanisme algorithmique de génération de pseudo-aléa afin de fournir des données aléatoires cryptographiquement satisfaisantes.

If the random number generator is used for cryptographics operations, it is higly recommended to combine it with a pseudo random generator algorithm in order to get good random number.

4.3 Certification

Certification

30 Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information, publié au journal officiel de la République française le 19 avril 2002.

This certificate is issued within the scope of the «décret 2002-535» of april 18th, 2002 dealing with the evaluation and the certification of the security provided by IT product and systems. The text of the «décret» was published april 19th, 2002 in the «journal officiel de la République française».

31 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.

Certification is not in itself a recommendation of the product. It does not guaranty that the certified product is totally exempt of exploitable vulnerabilities: it still remains a residual probability that exploitable vulnerabilities have not been discovered.

4.4 Reconnaissance internationale

International recognition

32 Afin d'éviter les certifications multiples d'un même produit dans différents pays, il existe des accords de reconnaissance des certificats ITSEC et Critères Communs.

In order to avoid multiple certification of the same product in different countries, a mutual recognition of ITSEC and CC certificates was agreed.

33 Ce certificat répond aux exigences de l'accord SOGIS :

This certificate meets the requirements of the SOGIS agreement:

34 L'accord SOG-IS [SOG-IS] sur la reconnaissance des certificats ITSEC est applicable depuis mars 1998. Cet accord a été signé par l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse. Cet accord a ensuite été étendu aux certificats Critères Communs pour tous les niveaux d'évaluation (EAL1 - EAL7).

The SOGIS-Agreement [SOG-IS] on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates based on the CC was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	Addition d'un ou de plusieurs composants d'assurance de la partie 3 des CC à une échelle prédéfinie d'assurance ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou par son environnement.
Cible d'évaluation	Produit ou système et documentation associée pour (administrateur et utilisateur) qui est l'objet d'une évaluation.
Cible de sécurité	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)	Paquet de composants d'assurance extraits de la partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	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	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 :
- Part 1 : Introduction and general model, august 1999, version 2.1, réf : CCIMB-99-031 ;
- Part 2 : Security functional requirements, august 1999, version 2.1, réf : CCIMB-99-032 ;
- Part 3 : Security assurance requirements, august 1999, version 2.1, réf : CCIMB-99-033.

[CEM] Méthodologie commune l'évaluation de la sécurité des technologies de l'information :
- Part 2 : Evaluation Methodology, august 1999, version 1.0, réf : CEM-99/045.

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

[ST] APACHE Security Target, version 1.54, issued on October 14, 2002.

[ST-Lite] APACHE Security Target Lite, version 0.1, issued on November 29, 2002.

[RTE] Evaluation Technical Report - S3CC9PB, version 1.1, ref. Apache ETR v1.1, October 25th, 2000.

[SOG-IS] «Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

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