PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2004/07

Micro-circuit SAMSUNG S3CC9RB

Paris, le 11 mai 2004

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[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 présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.
Toutefois, la certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Table des matières

Préface

La certification

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 Premier ministre 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 selon les ITSEC et les Critères Communs sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Le site international concernant la certification selon les Critères Communs est accessible à l'adresse Internet :

www.commoncriteriaportal.org

Accords de reconnaissance des certificats

L'**accord de reconnaissance** européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

La direction centrale de la sécurité des systèmes d'information passe aussi des **accords de reconnaissance** avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties.

L'accord du Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires de l'accord[1], des certificats délivrés dans le cadre du schéma Critères Communs. La reconnaissance mutuelle s'applique au niveau EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

Les sites des organismes nationaux de certification des pays signataires de l'accord Common Criteria Recognition Arrangement sont :

Pays	Organisme certificateur	Site web
France	DCSSI	www.ssi.gouv.fr
Royaume-Uni	CESG	www.cesg.gov.uk
Allemagne	BSI	www.bsi.bund.de
Canada	CSE	www.cse-cst.gc.ca
Australie-Nouvelle Zélande	AISEP	www.dsd.gov.au/infosec
Etats-Unis	NIAP	www.niap.nist.gov
Japon	NITE	www.nite.go.jp

[1] En novembre 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède et la Turquie.

1. Le produit évalué

1.1. Contexte

Le produit évalué est le micro-circuit S3CC9RB dérivé du micro-circuit S3CC9PB déjà certifié sous la référence 2002/25 (cf. [2002/25]). Ces composants appartiennent à la famille des micro-circuits pour cartes à puce 16-bits CalmRisc (technologies Harvard) de Samsung.
Le micro-circuit S3CC9RB diffère du micro-circuit S3CC9PB essentiellement par la taille des mémoires. Le centre d'évaluation a donc réutilisé les résultats de l'évaluation du micro-circuit S3CC9PB.

1.2. Identification du produit

Le produit évalué est le micro-circuit S3CC9RB (référence S3CC9RB-X01). Ce micro-circuit inclut des librairies logicielles stockées en ROM :

- Test_Rom en version 1.0,
- librairie cryptographique en version 1.0.

1.3. Le développeur

SAMSUNG Electronics

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

1.4. Description du produit évalué

Le produit évalué est le micro-circuit S3CC9RB développé et fabriqué par SAMSUNG Electronics.

Le micro-circuit comporte deux modes d'utilisation :

- un mode « Test » dans lequel le micro-circuit fonctionne sous le contrôle d'un logiciel de test. Ce mode n'est utilisable que par le personnel autorisé de l'équipe du développement au sein d'un environnement sécurisé. En sortie de phase de test, le mode "test" est inhibé de façon irréversible ;
- un mode « utilisateur » dans lequel le micro-circuit fonctionne sous le contrôle du logiciel embarqué de la carte à puce. Les utilisateurs finaux ne peuvent utiliser le micro-circuit que dans ce mode.

Le micro-circuit seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou des applications et à être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (applications bancaires, télévision à péage, transport, santé,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.4.1. Architecture

Le produit évalué est constitué des éléments suivants :

- Une partie matérielle comportant :
  - un processeur CalmRISC16 (16 bit CPU),
  - 320KB de mémoire ROM pour le stockage des programmes,
  - 64KB de mémoire EEPROM pour le stockage des programmes et des données,
  - 6KB de mémoire statique RAM,
  - un accélérateur de calcul cryptographique DES/3DES,
  - un co-processeur SuperMAPII pour cryptographie à clés publiques,
  - un générateur de nombres aléatoires 16-bit,
  - un module de gestion des entrées/sorties en mode asynchrone (ISO 7816),
  - des détecteurs d'évènements anormaux avec notification et redémarrage possible du micro-circuit.
- Une partie logicielle comportant :
  - le logiciel dédié « Test_Rom » en version 1.0,
  - une librairie cryptographique en version 1.0.

Une description détaillée de l'architecture de l'application se trouve dans le document [HLD].

1.4.2. Cycle de vie

Le cycle de vie du produit inspiré du cycle de vie décrit dans le PP/9806 [PP9806] est le suivant :

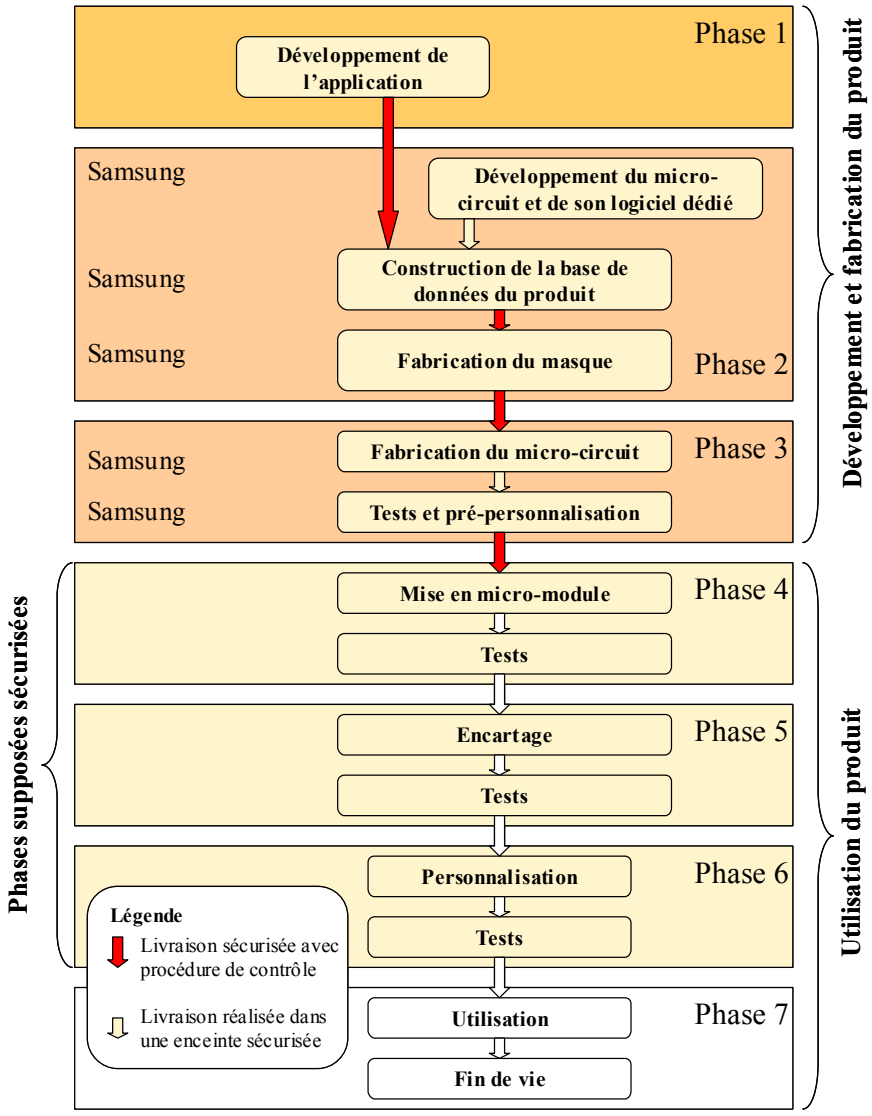

Figure 1 - Cycle de vie standard d'une carte à puce

1.4.3. Périmètre et limites du produit évalué

Ce rapport de certification présente les travaux d'évaluation relatifs au micro-circuit et à la librairie logicielle identifiés au §1.2. Toute autre application éventuellement embarquée pour les besoins de l'évaluation ne fait donc pas partie du périmètre d'évaluation.
En regard du cycle de vie, le produit évalué est le produit qui sort de la phase de fabrication, tests et pré-personnalisation (phase 3).

1.5. Utilisation et administration

1.5.1. Utilisation

Le produit évalué n'est pas un produit mettant en œuvre une application particulière. Il s'agit d'une plate-forme matérielle offrant différents services pour les logiciels embarqués. De fait, il n'y a pas réellement d'utilisation à proprement parler. Le document « The application of CC to Integrated Circuits » [CC_IC] suggère de considérer les utilisateurs du micro-circuit

comme étant les développeurs des applications ainsi que tous les acteurs intervenant dans les phases dites d'administration de la carte (phase 4 à 6) qui interviendront notamment dans la configuration et la personnalisation des applications embarquées. Néanmoins, pour la présente évaluation, les développeurs d'application sont considérés comme étant des administrateurs et non des utilisateurs.

1.5.2. Administration

Le guide « The application of CC to Integrated Circuits » [CC_IC] suggère que les administrateurs du produit soient considérés comme étant les différents intervenants des phases 4 à 7 du cycle de vie qui configurent (personnalisation) le produit final. Ces opérations sont en grande partie liées au type d'applications embarquées. Dans le cadre d'un micro-circuit, seules les interfaces d'administration propres au micro-circuit sont évaluées. Par ailleurs, les phases 4 à 6, dites d'administration, sont couvertes par une hypothèse dans la cible de sécurité qui suppose que les opérations associées à ces phases sont réalisées dans des conditions ne remettant pas en cause la sécurité du produit. Ces conditions n'ont pas été évaluées.

Pour la présente évaluation, les développeurs d'application ont également été considérés comme administrateurs du produit, de même que l'administrateur des tests en phase 3.

2. L'évaluation

2.1. Centre d'évaluation

SERMA Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Téléphone : +33 (0)5 57 26 08 64

Adresse électronique : m.dus@serma.com

L'évaluation s'est déroulée d'avril 2003 à février 2004.

2.2. Commanditaire

SAMSUNG Electronics

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

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation respectent les exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].

2.5.1. Développement du produit

Le micro-circuit S3CC9RB étant très similaire au micro-circuit S3CC9PB déjà évalué et certifié (cf. [2002/25]), les résultats de l'évaluation précédente ont été ré-utilisés en partie. Seul le niveau de la représentation de l'implémentation a été de nouveau intégralement évalué.
Les documents fournis pour la classe ADV – développement – répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.2. Documentation

Du point de vue de l'évaluation, les administrateurs sont les développeurs d'applications embarquées ainsi que l'administrateur du mode tests en sortie de production (phase 3).
Du point de vue de l'évaluation, les utilisateurs sont les utilisateurs finaux de la carte à puce. Ils ne sont donc pas pris en compte dans le cadre de l'évaluation du micro-circuit nu.
Le micro-circuit S3CC9RB étant très similaire au micro-circuit S3CC9PB déjà évalué et certifié (cf. [2002/25]), les résultats de l'évaluation précédente ont été ré-utilisés en partie.
Les guides administrateur [ADM] répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.3. Livraison et installation

Conformément au guide pour l'évaluation « The application of CC to IC » (cf. [CC_IC]), les livraisons considérées sont :

- la livraison du code des applications embarquées au fabricant du micro-circuit,
- la livraison des informations nécessaires au fabricant de réticules,
- la livraison des réticules au fabricant du micro-circuit,
- la livraison des micro-circuits au responsable de l'étape suivante (mise en micro-module, encartage).

Excepté le développement des applications embarquées, toutes les opérations sont réalisées sur le site de Samsung Electronics en Corée (449-711, San#24 Nongseo-Ri,Giheung-Eup, Yongin-City, Gyeonggi-Do, Corée).
Les procédures de livraison et d'installation sont les mêmes que pour le produit S3CC9PB déjà évalué et certifié (cf. [2002/25]) ce qui a permis de conclure qu'il n'y avait pas nécessité de réaliser des travaux pour la classe d'assurance ADO.

2.5.4. L'environnement de développement

Le système de gestion de configuration est utilisé conformément au plan de gestion de configuration [ACM].
La liste de configuration [LGC] identifie les éléments tracés par le système de gestion de configuration. Les éléments de configuration identifiés dans la liste de configuration sont maintenus par le système de gestion de configuration. Les procédures de génération de l'application sont efficaces pour s'assurer que les bons éléments de configuration sont utilisés pour générer le micro-circuit.
Le produit est développé sur le site de Samsung Electronics situé à :

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

Les mesures de sécurité décrites dans les procédures fournissent le niveau nécessaire de protection pour maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.
La vérification de la mise en œuvre des procédures avait été réalisée lors de l'évaluation du micro-circuit S3CC9PB (cf. [2002/25]). Néanmoins, au vu de changements dans l'environnement de développement et dans le mode de gestion de configuration, une visite a de nouveau été effectuée sur le site de Giheung-Eup (cf Annexe 1). Le rapport de visite se trouve sous la référence [Visite].

Les documents fournis pour la classe ACM – gestion de la configuration – et ALC – support au cycle de vie – répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.5. Tests fonctionnels

Dans le cadre de l'évaluation du micro-circuit S3CC9PB (cf. certificat [2002/25]), l'évaluateur avait vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit étaient reliées à au moins un test fonctionnel dans la documentation de test. Il avait vérifié aussi que toutes les caractéristiques fonctionnelles de chaque fonction de sécurité, telles qu'elles sont décrites dans la conception de haut niveau [HLD], étaient couvertes par les tests du développeur. La documentation de test du micro-circuit S3CC9RB étant très similaire, la plupart des résultats de l'évaluation de cette documentation ont été ré-utilisés. Les tests eux-mêmes ont été menés à nouveau sur le produit S3CC9RB.

2.5.6. Estimation des vulnérabilités

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement prises en compte dans la conception du produit.
L'évaluateur a également réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré.
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élevé**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du micro-circuit S3CC9RB.

3.2. Niveau d'évaluation

Le micro-circuit S3CC9RB a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL4**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

Pour tous les composants, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	[2002/25]
ADO_IGS.1	Installation, generation, and start-up procedures	[2002/25]

[1] Annexe 4 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

Class ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
ADV_SPM.1	Informal TOE security policy model	[2002/25]
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	N/A
Class ALC	**Life cycle support**	
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	[2002/25]
ALC_TAT.1	Well-defined development tools	Réussite
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_MSU.2	Validation of analysis	[2002/25]
AVA_SOF.1	Strength of TOE security function evaluation	[2002/25]
AVA_VLA.4	Highly resistant	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** suivantes[1]. Les opérations sur ces exigences sont décrites dans la cible de sécurité [ST].

- User authentication before any action (FIA_UAU.2)
- User Identification before any action (FIA_UID.2)
- User attribute definition (FIA_ATD.1)
- TOE Security Functions testing (FPT_TST.1)
- Stored data integrity monitoring and action (FDP_SDI.1)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Security management roles (FMT_SMR.1)
- Static attribute initialisation (FMT_MSA.3)
- Complete access control (FDP_ACC.2)

[1] Annexe 3 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- Security attributes based access control (FDP_ACF.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Potential violation analysis (FAU_SAA.1)
- Unobservability (FPR_UNO.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- Cryptographic operation (FCS_COP.1)
- Cryptographic Key Generation (FCS_CKM.1)

3.4. Résistance des fonctions

Seules les fonctions d'authentification de l'administrateur en mode test ont fait l'objet d'une estimation du niveau de résistance.
Le niveau de résistance des fonctions de sécurité est jugé **élevé** (**SOF-High**).

3.5. Analyse des mécanismes cryptographiques

Le produit a fait l'objet d'une analyse des mécanismes cryptographiques dans le cadre de l'évaluation (cf Annexe 2).

3.6. Conformité à un profil de protection

Le produit évalué est conforme au profil de protection PP/9806 [PP/9806].

3.7. Reconnaissance européenne (SOG-IS)

Ce certificat a été émis dans les conditions de l'accord du SOG-IS. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].

3.8. Reconnaissance internationale (CC RA)

Ce certificat a été émis dans les conditions de l'accord du CC RA. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].
Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA [CC RA] : ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4 (Tableau 1).

3.9. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.10) ainsi que les recommandations se trouvant dans les guides administrateur [ADM].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

3.10. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST § 4.2] :

Objectifs de sécurité sur l'environnement concernant le système en phase d'utilisation

Ces objectifs de sécurité concernent le système dans lequel sera utilisé le micro-circuit avec son application embarquée (extraits de la cible de sécurité [ST § 4.2.6]) :

- la communication entre un produit développé sur le micro-circuit sécurisé et d'autres produits doit être sécurisée (en termes de protocole et de procédure) ;
- le système (terminal, communication,…) doit garantir la confidentialité et l'intégrité des données sensibles qu'il stocke ou qu'il traite.

3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le micro-circuit S3CC9RB identifié au paragraphe 1.2 et décrit au paragraphe 1.4 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Rapport de visite du site de Giheung-Eup

Le site de développement de Samsung Electronics situé au 449-711, San#24 Nongseo-Ri, Giheung-Eup, Yongin-City, Gyeonggi-Do en Corée, a fait l'objet, dans le cadre de l'évaluation du micro-circuit S3CC9RB, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4),
- la livraison : **ADO** (ADO_DEL.2),
- le support au cycle de vie : **ALC** (ALC_DVS.2).

La visite par le centre d'évaluation, accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 2. Analyse des mécanismes cryptographiques

Le micro-circuit S3CC9RB offre les services cryptographiques suivants :

- un accélérateur de calcul cryptographique DES/3DES,
- un co-processeur SuperMAPII pour cryptographie à clés publiques,
- un générateur de nombres aléatoires 16-bit,

Ces services ne concourent pas à la sécurité propre du micro-circuit. Il s'agit de services pour le logiciel embarqué. Pour cette raison, ces services ne sont pas analysés d'un point de vue cryptographique. Cependant le générateur aléatoire est traité comme un cas particulier et a fait l'objet d'une analyse.

Cette analyse montre que dans le cas où le générateur d'aléas serait utilisé à des fins cryptographiques, il est fortement conseillé d'utiliser un mécanisme de post-traitement afin de fournir des données aléatoires cryptographiquement satisfaisantes.

Annexe 3. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont données à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles du produit.

Class FAU	**Security audit**
Security audit analysis	
FAU_SAA.1	*Potential violation analysis* Le produit doit implémenter un seuil de détection élémentaire, défini selon une règle fixée (spécifiée dans la cible de sécurité [ST]).
Class FCS	**Cryptographic support**
Cryptographic key management	
FCS_CKM.1	*Cryptographic key generation* Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiées qui peuvent être basés sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Information flow control policy	
FDP_IFC.1	*Subset information flow control* Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information, lesquelles sont spécifiées dans la cible de sécurité [ST] pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'information.

Information flow control functions	
FDP_IFF.1	*Simple security attributes* Ce composant impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la fonction et décrit comment les attributs de sécurité sont choisis par la fonction.
Stored data integrity	
FDP_SDI.1	*Stored data integrity monitoring* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées.
Class FIA	**Identification and authentication**
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
User authentication	
FIA_UAU.2	User *authentication* before any action Les utilisateurs doivent s'authentifier avant que toute action ne soit autorisée.
User identification	
FIA_UID.2	User identification before any action Les utilisateurs doivent s'identifier avant que toute action ne soit autorisée.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Security management roles	
FMT_SMR.1	*Security* roles Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiées dans la cible de sécurité [ST]).
Class FPR	**Privacy**
Unobservability	
FPR_UNO.1	*Unobservability* Le produit n'autorise pas certains utilisateurs (spécifiés dans la cible de sécurité [ST]) à déterminer si certaines opérations (spécifiées dans la cible de sécurité [ST]) sont en cours d'exécution.
Class FPT	**Protection of the TSF**
TSF physical protection	
FPT_PHP.2	*Notification of physical attack* Le produit doit notifier automatiquement l'intrusion physique sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).

FPT_PHP.3	*Resistance to physical attack* Le produit doit empêcher ou résister à certaines intrusions physiques (spécifiées dans la cible de sécurité [ST]) sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.

Annexe 4. Niveaux d'assurance prédéfinis IS 15408 ou CC

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 5. Références documentaires du produit évalué

[2002/25]	Rapport de certification 2002/25, SAMSUNG S3CC9PB microcontroller (Référence S3CC9PBX01), Décembre 2002 SGDN/DCSSI
[ACM]	Configuration Management Documentation (Class ACM), Version 1.2 Issued on August 14th, 2003 SAMSUNG Electronics
[ADM]	o S3CC9PB/RB/P9/FB - Smart Card IC Security Guide - Application Note, Revision 1.5, SAMSUNG Electronics o S3CC9PB/C9RB/C9P9 - 16-BIT CMOS MICROCONTROLLER for SMART CARD - PROGRAMMER'S GUIDE, Revision 1.3, SAMSUNG Electronics o Test-Administrator Guidance, Version 1.1 Issued on August 18, 2003, SAMSUNG Electronics o Guidance Documents (Class AGD), Version 1.4 Issued on February 16, 2004, SAMSUNG Electronics o S3CC9PB/C9RB/C9P9 user's manual, Revision 2.0 SAMSUNG Electronics o S3CC9PB/RB/P9 USER'S MANUAL ERRATA, Version 1.0, SAMSUNG Electronics
[Visite]	Evaluation reports - Class ALC, Class ADO - Annexe A Référence : APACHE-2_ ALC ADO_ v1.0, SERMA Technologies
[HLD]	High Level Design (Class ADV), Version 1.1 Issued on July 3, 2003, SAMSUNG Electronics
[LGC]	Configuration Management Documentation (Class ACM), § « Configuration List » Version 1.2 Issued on August 14th, 2003 SAMSUNG Electronics

[PP9806]	Common Criteria for Information Technology Security Evaluation - Protection Profile : Smart Card Integrated Circuit Version 2.0, Issue September 1998. Certifié par le centre de certification français sous la référence 9806. *Document publié sur le site : www.ssi.gouv.fr*
[RTE]	Evaluation Technical Report - S3CC9RB - C9P9 - C9FB, (EAL4+ evaluation) Référence : Apache2_ ETR v1.0 SERMA Technologies
[ST]	S3CC9RB Security Target, Version 1.2, February 21, 2003, SAMSUNG Electronics

Annexe 6. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[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, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[IS 15408]	Norme Internationale ISO/IEC 15408:1999, comportant 3 documents : ▪ ISO/IEC 15408-1: Part 1 Introduction and general model ; ▪ ISO/IEC 15408–2: Part 2 Security functional requirements ; ▪ ISO/IEC 15408–3: Part 3 Security assurance requirements ;
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, may 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[CC_IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, Version 1.2, July 2000

Toute correspondance relative à ce rapport 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 cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr