Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/37

Micro-circuit S3CJ9QD (référence S3CJ9QDX01 rev.6)

Paris, le 27 octobre 2005.

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2005/37

Micro-circuit S3CJ9QD (référence S3CJ9QDX01 rev.6)

Développeur : SAMSUNG Electronics Co. Ltd.

Critères Communs version 2.2

EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, AVA_VLA.3)

Commanditaire : Samsung

Centre d'évaluation : Serma Technologies

Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA :
ADV_IMP.2, ALC_DVS.2, AVA_VLA.3

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 sont publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

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 suivante :

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 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. (article 9 du décret 2002-535)
Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[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.
[2] En mai 2005, 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, la Turquie, la République Tchèque, Singapour et l'Inde.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le micro-circuit S3CJ9QD (référence S3CJ9QDX01 rev.6) développé par la société Samsung. Ce micro-circuit inclut les librairies logicielles suivantes :

- Test code version 2.0 (en ROM) ;
- "normal" cryptographic library version 3.0N (en ROM) ;
- "secure" cryptographic library version 3.2S (en EEPROM).

Pour les besoins de l'évaluation, un système d'exploitation a été inclus en ROM : User test code version 1.0.

1.2. Développeur

Le développeur est :

SAMSUNG Electronics Co. Ltd.

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

1.3. Description du produit évalué

Ce produit 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.

1.3.1. Architecture

Le produit évalué est constitué des éléments matériels suivants :

- un processeur 32-bit (ARM SC200 RISC core) ;
- des mémoires volatiles (10 kbytes SRAM) et non volatiles (256 Ko de ROM et 128 Ko d'EEPROM) ;
- un module de contrôle d'accès aux mémoires (MPU) ;
- des détecteurs d'évènements anormaux ;
- un dispositif de masquage des données stockées en mémoire ;
- des contre-mesures anti-SPA et anti-DPA ;
- un accélérateur de calcul cryptographique matériel DES ;
- un co-processeur cryptographique RSA (exponentiation modulaire) ;
- un contrôleur d'intégrité des données ;
- un générateur de nombres aléatoires ;
- un module de gestion des entrées/sorties ;
- des horloges.

Le produit évalué est constitué des éléments logiciels suivants :

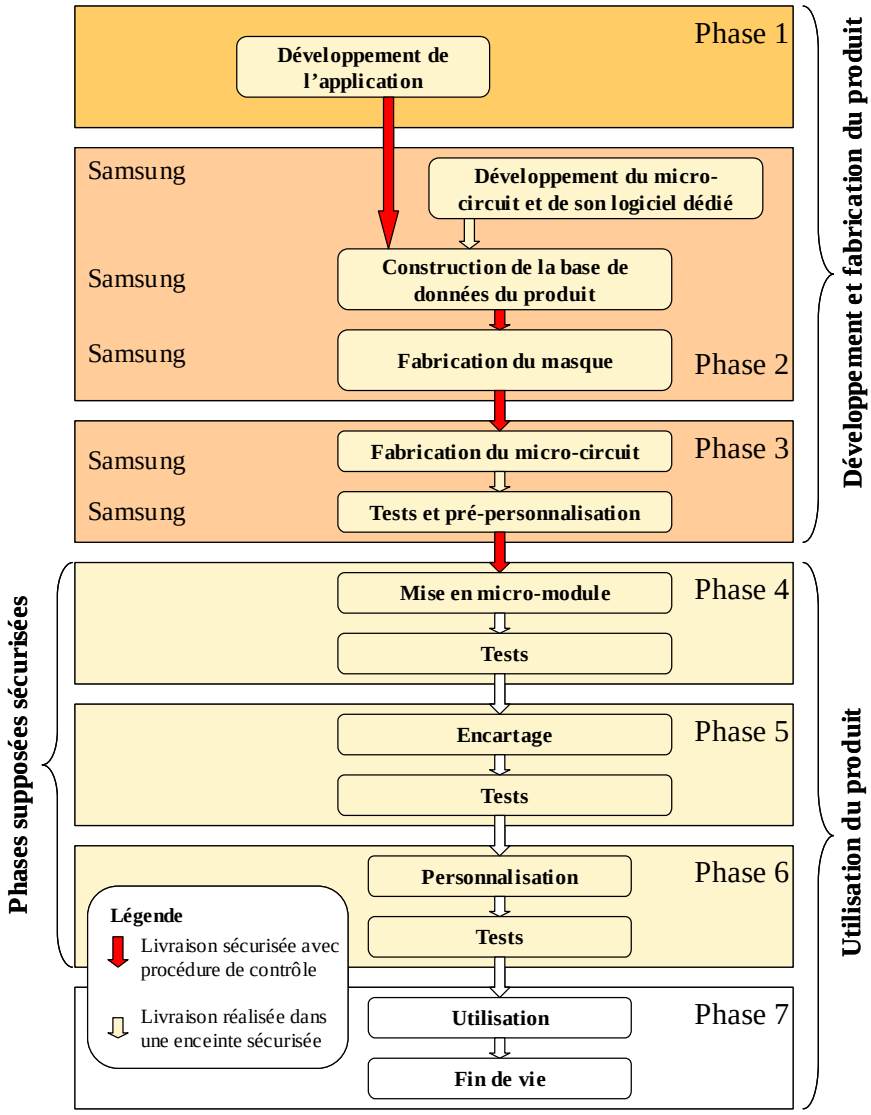
- un logiciel dédié gravé en ROM (utilisé uniquement dans le mode « Test ») ;

- deux librairies cryptographiques offrant les mêmes services cryptographiques : la première, dite « normale », est gravée en ROM ; la seconde, dite « sécurisée » est chargée en EEPROM. Seule la librairie sécurisée a été considérée dans l'analyse de vulnérabilité.

Le produit inclut également un co-processeur Jazelle qui permet d'exécuter des programmes Java Card. Ce co-processeur n'a pas été évalué.

1.3.2. Cycle de vie

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



1.3.3. Périmètre et limites du produit évalué

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).

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.

2. L'évaluation

2.1. Référentiels d'évaluation

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

2.2. Commanditaire

SAMSUNG Electronics Co. Ltd.

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

2.3. 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

2.4. Rapport technique d'évaluation

L'évaluation s'est déroulée du 29 octobre 2004 au 24 août 2005.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.5. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
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

2.6. Evaluation du produit

2.6.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL4[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_VLA.3	Moderately resistant

2.6.2. L'évaluation de l'environnement de développement

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 analysées par l'évaluateur permettent de maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation lors du développement.

L'évaluateur a analysé le plan de gestion de configuration fourni par le développeur qui précise l'utilisation du système de gestion de configuration. Le système permet de générer notamment la liste de configuration [CONF] qui identifie tous les éléments gérés par le système.

Des procédures de génération permettent par ailleurs de s'assurer que les bons éléments sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures analysées a été effectuée lors de la visite du site de Samsung à Giheung-Eup (cf Annexe 1).

[1] Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite

2.6.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP), conception de haut-niveau (HLD), conception de bas-niveau (LLD), implémentation (IMP).

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- 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)
- 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)
- Cryptographic key destruction (FCS_CKM.4)

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_SPM.1	Informal TOE security policy model	Réussite
ADV_FSP.2	Fully defined external interfaces	Réussite

ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.6.4. L'évaluation des procédures de livraison et d'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 micromodule, encartage).

L'évaluateur a analysé les procédures de livraison du produit entre les différents sites impliqués.
Ces procédures permettent de connaître l'origine de la livraison et de détecter une modification du produit au cours de cette livraison.

Le produit est un micro-circuit générique (sans logiciel applicatif embarqué). Par conséquent, il ne comporte pas de phase d'installation, génération et démarrage spécifique. Les exigences du composant d'assurance ADO_IGS.1 sont donc non applicables.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		**Verdicts**
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

2.6.5. L'évaluation de la documentation d'exploitation

Utilisation
Le produit évalué ne met pas en œuvre une application particulière. Il s'agit d'une plate-forme matérielle et logicielle offrant différents services pour les logiciels embarqués dans l'optique d'une utilisation de type « carte à puce ». De fait, il n'y a pas réellement d'utilisation à proprement parler. Les utilisateurs du micro-circuit peuvent être vus (cf. document [CC IC]) comme étant les développeurs des applications ainsi que tous les acteurs intervenant dans les phases dites d'administration du micro-module et de la carte (phases 4 à 6) qui interviendront notamment dans la configuration et la personnalisation des applications embarquées.

Dans le cadre de cette évaluation, ces rôles sont rappelés dans la cible de sécurité [ST] : les utilisateurs sont définis comme étant les personnes pouvant mettre en œuvre les fonctionnalités du micro-circuit, de sa bibliothèque logicielle et de son logiciel applicatif. Cette définition comprend tous les utilisateurs utilisant le produit en mode « user » : l'émetteur de la carte mais également le développeur du logiciel embarqué, le responsable de l'encartage et la personne en charge d'intégrer la carte dans son système d'utilisation finale.

Administration
Le guide « The application of CC to Integrated Circuits » [CC IC] spécifie les administrateurs du produit comme étant les différents intervenants des phases 4 à 7 du cycle de vie et qui configurent le produit final (personnalisation). 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 le profil de protection, 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 l'évaluation, l'évaluateur a considéré comme administrateurs du produit les intervenants des phases 4 à 6 et comme utilisateurs ceux de la phase 7.
L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		**Verdicts**
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.6.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.
L'évaluateur a réalisé ses tests fonctionnels indépendants sur des cartes représentatives de l'ensemble des 14 configurations évaluées.

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		**Verdicts**
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

2.6.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

La fonction d'authentification de l'administrateur en mode test a fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé **élevé (SOF-high)**.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests de pénétration.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de niveau **moyen**.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.3	Moderately resistant	Réussite

2.6.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (Art. 8 du décret 2002-535)

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit micro-circuit S3CJ9QD (référence S3CJ9QDX01 rev.6) à des attaques qui demeurent fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée qu'au travers de l'évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de cette évaluation.

En particulier, il est important de noter les deux points suivants :

1) dans la configuration évaluée, la librairie cryptographique dite « sécurisée » est chargée en EEPROM ; son comportement en ROM n'a pas été évalué ;
2) seule cette librairie a été considérée dans l'analyse de vulnérabilité ; la résistance aux attaques de la librairie cryptographique dite « normale » (gravée en ROM) n'a pas été évaluée.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation résumés ci-dessous et suivre les recommandations se trouvant dans les guides fournis [GUIDES] :

- la communication entre la carte et le terminal doit être sécurisée (en termes de protocole et de procédure),
- les méthodes et terminaux utilisés en phase d'utilisation doivent garantir l'intégrité et la confidentialité des données.

3.3. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

3.4. Reconnaissance internationale (CC RA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, les augmentations suivantes n'entrent pas dans le cadre de l'accord : ADV_IMP.2, ALC_DVS.2, AVA_VLA.3.

Annexe 1. Visite du site de développement de la société SAMSUNG à Giheung-Eup

Le site de développement de la société SAMSUNG situé à Giheung-Eup, a fait l'objet d'une visite par l'évaluateur du 21 au 23 mars 2005 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le micro-circuit S3CJ9QD (référence S3CJ9QDX01 rev.6).

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ACM_AUT.1 et ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 2. Niveaux d'assurance prédéfinis EAL

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 3. Références documentaires du produit évalué

[CONF]	Configuration Management Documentation (Class ACM), version 1.3 du 10 août 2005.
[GUIDES]	- Guidance Documents (Class AGD), version 1.1 du 11 août 2005. - User's Manual, Revision 2, référence 21-S3-CJ9QD-082004. - S3CJ9QD Security Application Note, Revision 4.0, référence SAN_S3CJ9QD (revision 4.0). - Application Note : RSA Crypto Library with TORNADO v3.2S, revision 1.4. - Design Concept : RSA Crypto Library with TORNADO v3.2S, revision 1.4. - Test administrator guidance documentation, v1.3.
[RTE]	Blackfoot project: Evaluation Technical Report, référence BLACKFOOT_ETR_v1.0.fm, version 1.0 du 24/08/05.
[ST]	Blackfoot Security Target (S3CJ9QD), version 1.4 du 10 août 2005. Blackfoot Security Target Lite (S3CJ9QD), version 1.0 du 1er octobre 2005.
[Visite]	Evaluation report Classes ACM, ADO, ALC, Annex A, référence BLACKFOOT_ACM-ALC-ADO_v2.0.fm du 20/06/05.
[PP/9806]	« Smartcard integrated circuit Protection Profile version 2.0 ».

Annexe 4. 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.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[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.

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