



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2012/72

**Microcontrôleurs SAMSUNG S3CT9KW,
S3CT9KC et S3CT9K9 Revision 2.0
embarquant la bibliothèque RSA/ECC
optionnelle TORNADO 2MX2 v2.1**

Paris, le 10 octobre 2012

*Le directeur général de l'Agence nationale
de la sécurité des systèmes d'information*

[ORIGINAL SIGNE]

Patrick PAILLOUX



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 présumées 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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2012/72

Nom du produit

**Microcontrôleurs SAMSUNG S3CT9KW, S3CT9KC et
S3CT9K9 Revision 2.0 embarquant la bibliothèque
RSA/ECC optionnelle TORNADO 2MX2 v2.1**

Référence/version du produit

Revision 2.0

Conformité à un profil de protection

**[PP0035] : Security IC platform Protection Profile
Version 1.0**

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

**EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5**

Développeur

Samsung Electronics Co., Ltd.
San#24 Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do 449-711
République de Corée

Commanditaire

Samsung Electronics Co., Ltd.
San#24 Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do 449-711
République de Corée

Centre d'évaluation

CEA - LETI
17 rue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables



SOG-IS



Le produit est reconnu au niveau EAL4.

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 modifié. Ce décret indique que :

- L'agence nationale 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 disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. LE PRODUIT	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Identification du produit</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Cycle de vie</i>	8
1.2.5. <i>Configuration évaluée</i>	10
2. L’EVALUATION	11
2.1. REFERENTIELS D’EVALUATION	11
2.2. TRAVAUX D’EVALUATION	11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	11
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	11
3. LA CERTIFICATION	13
3.1. CONCLUSION.....	13
3.2. RESTRICTIONS D’USAGE.....	13
3.3. RECONNAISSANCE DU CERTIFICAT	14
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	14
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	14
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	15
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	16
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	18

1. Le produit

1.1. Présentation du produit

Les produits évalués sont les « Microcontrôleurs SAMSUNG S3CT9KW, S3CT9KC et S3CT9K9 Revision 2.0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.1 » développés par Samsung Electronics Co., Ltd.

Les trois produits faisant l'objet de ce certificat diffèrent uniquement par la quantité de mémoire EEPROM disponible. Les tailles de mémoire EEPROM correspondant à chaque modèle sont précisées dans le chapitre suivant.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, 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.

1.2. Description du produit

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

Cette cible de sécurité est strictement conforme au profil de protection [PP0035].

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF]. Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire EEPROM (non effaçable) située à l'offset 0x500000 :

- identification des microcontrôleurs :
 - o 0x1420/0x140C/0x1409, désignant respectivement les modèles S3CT9KW, S3CT9KC et S3CT9K9, par lecture de deux octets à l'adresse 0x500004 ;
- révision :
 - o 0x02 pour la révision 2.0 par lecture d'un octet à l'adresse 0x50002A ;
- identification des logiciels embarqués :
 - o *TORNADO 2MX2 Secure RSA/ECC library* : 0x0021 pour la version 2.1 par lecture de deux octets à l'adresse 0x50002C ;
 - o *TRNG library* : 0x02 pour la version 2 par lecture d'un octet à l'adresse 0x50002F.

Ces éléments ont été vérifiés par l'évaluateur.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité et en confidentialité des données utilisateur et des logiciels embarqués exécutés ou stockés dans les différentes mémoires de la TOE ;
- la bonne exécution des services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support au chiffrement cryptographique à clés asymétriques ;
- le support à la génération de nombres non prédictibles.

1.2.3. Architecture

Les microcontrôleurs S3CT9KW/S3CT9KC/S3CT9K9 sont constitués des éléments suivants :

- une partie matérielle comprenant :
 - o un processeur SecuCalm RISC 16bit ;
 - o des mémoires :
 - 384Ko de ROM ;
 - 8,5Ko de RAM dont 2,5Ko réservés pour les calculs cryptographiques ;
 - respectivement 144, 80 et 36 Ko d'EEPROM pour les modèles S3CT9KW, S3CT9KC et S3CT9K9 ;
 - o des modules de sécurité : protection de la mémoire (MPU), génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes ... ;
 - o des modules fonctionnels : gestion des entrées/sorties en mode contact (UART ISO 7816) et sans contact (ISO 14443 type A et B), génération de nombres aléatoires – TRNG (*True Random Number Generator*¹) –, coprocesseurs cryptographiques AES, 3DES et accélérateur de calculs arithmétiques TORNADO 2MX2 ;
 - o un DRNG (*Digital Random Number Generator*²) qui ne fait pas partie de la TOE ;
- une partie logicielle composée :
 - o des logiciels de test du microcontrôleur (*Test ROM code*) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;
 - o de la bibliothèque de calcul arithmétique pour la cryptographie asymétrique *TORNADO 2MX2 Secure RSA/ECC library*, version 2.1 ; cette bibliothèque est optionnelle et elle peut être désactivée avant la livraison du microcontrôleur ;
 - o d'une bibliothèque pour le TRNG conforme aux exigences du référentiel [AIS 31] ;

Le schéma ci-après synthétise l'architecture matérielle des microcontrôleurs S3CT9KW, S3CT9KC et S3CT9K9 :

¹ Générateur physique de nombres aléatoires.

² Générateur numérique de nombres aléatoires.

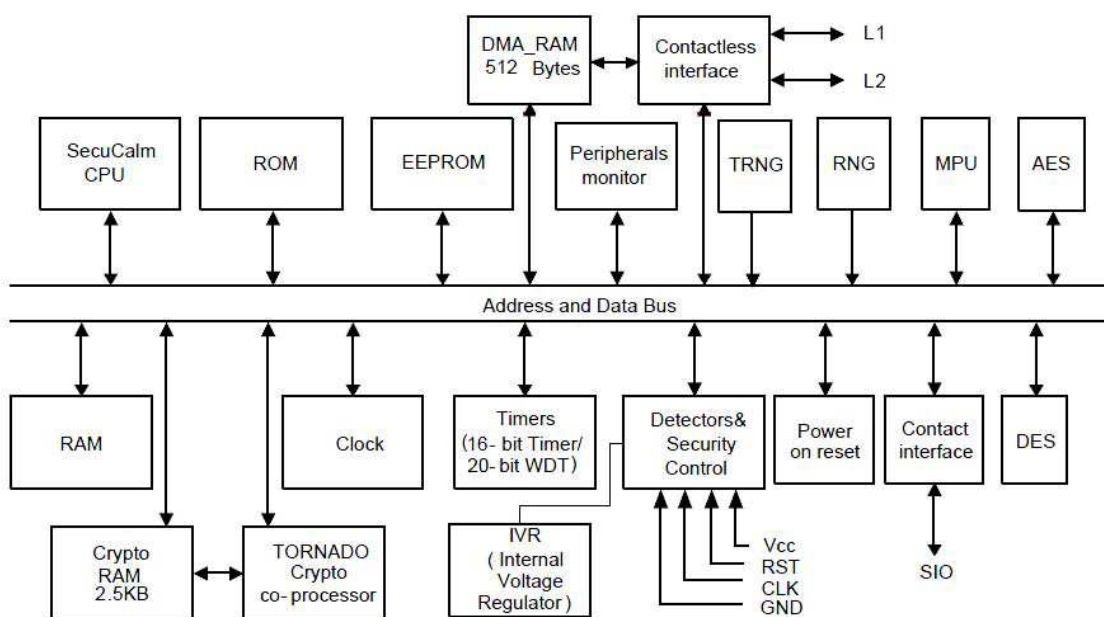


Figure 1 : Architecture des microcontrôleurs S3CT9KW/S3CT9KC/S3CT9K9

1.2.4. Cycle de vie

Le cycle de vie des produits peut être représenté par le schéma suivant :

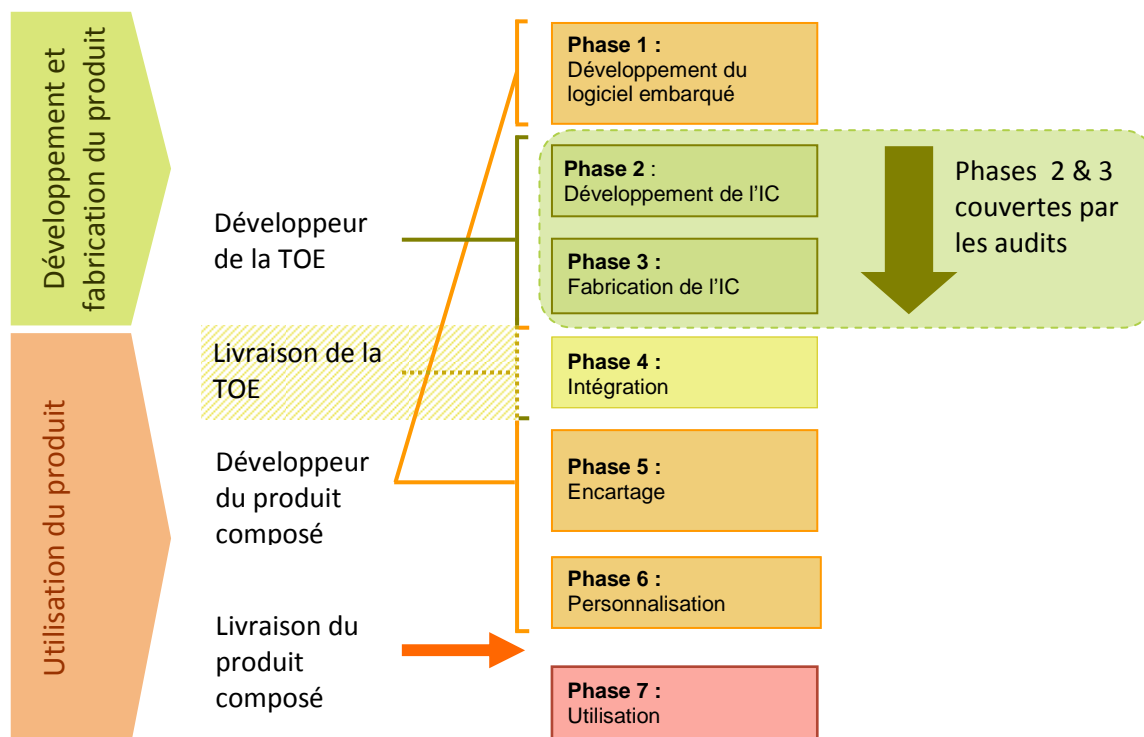


Figure 2 : Cycle de vie du produit

Les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous forme de wafers en début de phase 4.

La phase 2 correspond à la phase de développement du microcircuit et comprend notamment les étapes suivantes :

- conception du circuit ;
- développement du logiciel dédié.

La phase 3, qui couvre la fabrication du microcircuit, comprend les étapes suivantes :

- intégration et fabrication du masque ;
- fabrication du microcircuit ;
- test du microcircuit ;
- préparation ;
- pré-personnalisation si nécessaire.

La TOE est développée sur les sites suivants :

Giheung Plant (Phase 2 & 3)

San #24, Nongseo-Dong, Giheung-Gu
Yongin-City, Gyeonggi-Do
République de Corée

HANAMICRON Plant (Phase 3)

#95-1 Wonnam-Li, Umbong-Myeon
Asan-City, Choongcheongnam-Do
République de Corée

Hwasung Plant (Phase 3)

San #16, Banwol-Dong
Hwasung-City, Gyeonggi-Do
République de Corée

Eternal Plant (Phase 3)

No.1755, Hong Mei South Road,
Shanghai
République Populaire de Chine

PKL Plant (Phase 3)

493-3, Sungsung-Dong
Cheonan-City, Choongcheongnam-Do
République de Corée

Les produits comportent eux-mêmes une gestion de leur cycle de vie, prenant la forme de deux configurations :

- configuration « *TEST mode* » : à la fin de la fabrication, le microcontrôleur est testé à l'aide du logiciel de test présent en ROM. Cette configuration est ensuite bloquée de manière irréversible lors du passage en configuration « *NORMAL mode* » ;
- configuration « *NORMAL mode* », qui supporte deux sous-modes d'exécution pour le processeur :
 - o le sous-mode « *PRIVILEGE* », activé lors de l'exécution de routines d'interruption, permet d'accéder aux registres de contrôle et de sécurité et de configurer la MPU (*Memory Protection Unit*) ; lorsque le processeur a terminé l'exécution de la routine il retourne automatiquement en mode « *USER* » ;
 - o le sous-mode « *USER* » : mode normal d'utilisation du microcontrôleur, dans lequel aucun registre de contrôle ou de sécurité n'est accessible.

1.2.5. Configuration évaluée

Le certificat porte sur les microcontrôleurs définis au 1.2.1 et les bibliothèques logicielles qu'ils embarquent. Toute autre application, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre de l'évaluation.

Au regard du cycle de vie détaillé au chapitre 1.2.4, le produit évalué est celui obtenu à l'issue de la phase 3.

Pour les besoins de l'évaluation, seul le modèle S3CT9KW, Revision 2.0, contenant les bibliothèques logicielles décrites au 1.2.1, a été évalué. Le CESTI a jugé que ce modèle, dans cette version, était représentatif des trois produits qui font l'objet de cette certification.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 22 août 2012, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « réussite ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Les produits embarquent deux générateurs d'aléas : un TRNG construit à partir d'un support matériel (source) et un DNRG (hors TOE) construit à partir d'un TRNG et d'un post-traitement logiciel.

Le TRNG a fait l'objet d'une analyse par le CESTI. Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [REF] il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

Ce générateur de nombres aléatoires a en outre fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation : il atteint le niveau « P2 – *High level* ».

Les guides associés aux différents générateurs, notamment : « *S3CT9KW AIS31 TRNG library application note* » et « *Security Application Note S3CT9KW* » (voir [GUIDES]) doivent être scrupuleusement appliqués.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que les produits « Microcontrôleurs SAMSUNG S3CT9KW, S3CT9KC et S3CT9K9 Revision 2.0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.1 » soumis à l'évaluation répondent aux caractéristiques de sécurité spécifiées dans leur cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance des produits « Microcontrôleurs SAMSUNG S3CT9KW, S3CT9KC et S3CT9K9 Revision 2.0 embarquant la bibliothèque RSA/ECC optionnelle TORNADO 2MX2 v2.1 » à des attaques qui sont 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 que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], en particulier celles du document « *TND_RSA_SigCRT_Secure Guide For S3CT9KW RSA/ECC Library* » portant sur l'utilisation de la bibliothèque cryptographique TORNADO 2MX2 en version 2.1.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², des certificats Critères Communs. La reconnaissance 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 Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

² Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	4	Semi-formal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - <i>Security Target of Samsung S3CT9KW/ S3CT9KC/ S3CT9K9</i>, référence: ST_v2.1, version 2.1, Samsung. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - <i>Security Target Lite of Samsung S3CT9KW/ S3CT9KC/ S3CT9K9</i>, référence: ST_Lite_v2.2, version 2.2, Samsung.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - <i>KICKAPOO Evaluation Technical Report : RTE</i>, référence: LETI.CESTI.KIC.RTE.001 – v1.1, version 1.1, CEA LETI.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - <i>Project <KICKAPOO> Life Cycle Definition (Class ALC_CMC.4/ALC_CMS.5)</i>, référence: ALC_CMC_CMS_v2.4, version 2.4, Samsung.
[GUIDES]	<p>Guide du produit :</p> <ul style="list-style-type: none"> - <i>Security Application Note S3CT9KW</i>, référence: SAN_v2.2, version 2.2, Samsung. - <i>S3CT9KW/KC/K9 Chip Delivery Specification</i>, référence: DS_v1.1, version 1.1, Samsung. - <i>TORNADO-2Mx2 RSA/ECC Library API Manual</i>, référence: RSA/ECC Manual_v2.1, version 2.10, Samsung. - <i>S3CT9KW AIS31 TRNG library application note</i>, référence: TRNG_AN_v1.2, version 1.2, Samsung. - <i>SecuCalm CPU CORE, architecture reference</i>, référence: Secu_Calm, version AR14, Samsung. - <i>Hardware User's manual</i>, référence: UM_v1.21, version 1.21, Samsung. - <i>USER'S MANUAL ERRATA Samsung 16-bit CMOS Microcontroller for Smart Card S3CT9KW/KC/KA/K9/K7/K3/PC/PA/P7/P3/AC/AA/A7</i>, référence: UM_v1.21_errata_v2.0, version 2.0, Samsung. - <i>TND_RSA_SigCRT_Secure Guide For S3CT9KW RSA/ECC Library</i>, référence: add_guide_RSA/ECC_v2.1_v1.0, version 2.1, Samsung.
[BSI-DSZ-CC-0639-2010]	<p><i>Samsung S3CT9KW 16-bit RISC Microcontroller for Smart Card, Revision 0 with optional RSA/ECC v1.0 Library including specific IC Dedicated Software</i>, référence: BSI-DSZ-CC-0639-2010, BSI (Bundesamt für Sicherheit in der Informationstechnik).</p>



[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certifié par le BSI sous la référence BSI-PP-0035-2007.</i>
----------	--

Annexe 3. Références liées à la certification

<p>Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.</p>
[CC]	<p>Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.</p>
[CC IC]	<p>Common Criteria Supporting Document – Mandatory Technical Document – The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.</p>
[JIWG AP]	<p>Mandatory Technical Document – Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</p>
[SOG-IS]	<p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</p>
[REF]	<p>Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.</p> <p>Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr.</p>
[AIS 31]	<p><i>Functionality classes and evaluation methodology for physical random number generator</i>, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).</p>