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-2013/12

Memory Management Unit des microcontrôleurs SAMSUNG S3FT9KF/ S3FT9KT/ S3FT9KS en révision 1

Paris, le 29 mars 2013

Le directeur général de l'agence nationale 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 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

Référence du rapport de certification

ANSSI-CC-2013/12

Nom et version du produit

Memory Management Unit des microcontrôleurs SAMSUNG S3FT9KF/ S3FT9KT/ S3FT9KS en révision 1

Conformité à un profil de protection

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 7

Développeurs

Samsug Electronics Co. Ltd
Chip Card & Microcontroller
San#24 Nongseo-dong, Giheung-gu,
Gyeonggi-Do, 449-711
République de Corée

Trusted Labs
5 rue du Baillage
78000 Versailles,
France

Commanditaire

Samsung Electronics Co. Ltd
Chip Card & Microcontroller
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

CCRA

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

1.1. Présentation du produit

Le produit évalué est la « Memory Management Unit des microcontrôleurs SAMSUNG S3FT9KF/ S3FT9KT/ S3FT9KS en révision 1 » développée par Samsung Electronics Co, Ltd et Trusted Labs.

La seule différence entre les microcontrôleurs S3FT9KF, S3FT9KT et S3FT9KS réside dans la taille de la mémoire FLASH : 264 Ko pour S3FT9KF, 232 Ko pour S3FT9KT et 212 Ko pour S3FT9KS, la fonctionnalité *« Memory Management Unit* [1] » (MMU) étant strictement identique pour ces trois produits.

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 des produits

La cible de sécurité [ST] définit la fonctionnalité de sécurité évaluée et son environnement d'exploitation.

1.2.1. Identification des produits

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments suivants de son environnement d'exploitation, en l'occurrence les éléments d'identification des microcontrôleurs dans lequel elle est implantée :

- microcontrôleurs : **SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, *Revision* 1** ;
- librairies logicielles : *Test ROM v1.0, Secure Boot loader v0.0, TORNADO™2MX2Secure RSA/ECC Library v3.0 (option library), DRNG library v1, TRNG library v1* et *DTRNG library v1*.

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire FLASH (non effaçable) :

- identification des microcontrôleurs :
  - **0x140F** pour S3FT9KF par lecture de deux octets à l'adresse 0x400004 ;
  - **0x141D** pour S3FT9KT par lecture de deux octets à l'adresse 0x400004 ;
  - **0x141C** pour S3FT9KS par lecture de deux octets à l'adresse 0x400004.
- révision : **0x01** pour la révision 1 par lecture d'un octet à l'adresse 0x40002A ;
- identification des logiciels embarqués :

[1] Unité de gestion de la mémoire.

- *Test ROM* : **0x10** pour la révision 1.0 par lecture d'un octet à l'adresse 0x40002B ;
- *Secure Boot loader* : **0x00** pour la révision 0.0 par lecture d'un octet à l'adresse 0x400030 ;
- *TORNADO™2MX2Secure RSA/ECC Library (option library)* : **0x030C** pour la révision 3.0 par lecture de deux octets à l'adresse 0x40002C ;
- *DRNG library* : **0x01** pour la révision 1 par lecture d'un octet à l'adresse 0x40002E ;
- *DTRNG/TRNG library* : **0x11** (DTRNG version 1, TRNG version 1) par lecture d'un octet à l'adresse 0x40002F.

Ces éléments ont été vérifiés par l'évaluateur.

1.2.2. Services de sécurité

Les services de sécurité fournis spécifiquement par la cible d'évaluation sont détaillés au chapitre « *IT Security Requirements* » de la [ST], ils sont résumés ci-après :

- gestion des accès (lecture/écriture/exécution) aux zones mémoire des microcontrôleurs ;
- génération d'alarme sous forme d'interruption en cas d'accès non-autorisé.

La cible d'évaluation garantit qu'un logiciel embarqué sur les microcontrôleurs ne peut accéder à une zone mémoire en dehors de son espace autorisé. Elle peut, par exemple, être utilisée pour assurer une isolation entre applications.

Les services de sécurité complémentaires fournis par les produits « SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 1 » sont détaillés dans le rapport de certification [ANSSI-CC-2012/27].

1.2.3. Architecture

L'architecture matérielle des produits « SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 1 », détaillée au chapitre « *1.2 TOE Overview and TOE Description* » de la [ST], peut être représentée par la figure 1.

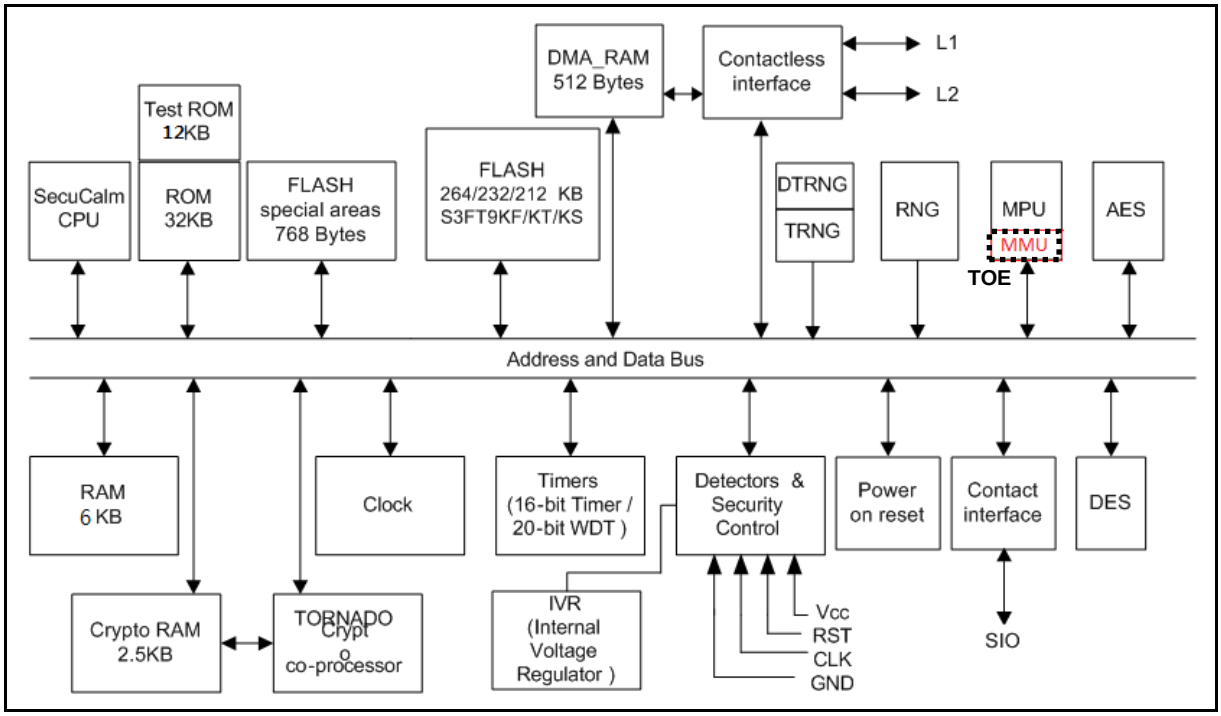

Figure 1: Architecture des produits

La cible d'évaluation (définie en pointillé sur la figure 1) est la fonctionnalité « *Memory Management Unit* » du module MPU. Elle permet à l'unité centrale (CPU) des microcontrôleurs d'accéder aux zones mémoire par l'intermédiaire de canaux.
Chaque canal autorise l'accès à une zone mémoire définie par une adresse de base, une adresse limite et des droits d'accès :

- droit d'exécution ;
- droits de lecture ou de lecture et écriture.

Le module MMU fournit les canaux suivants :

- 3 canaux pour les accès à la mémoire FLASH contenant du programme exécutable ;
- 1 canal pour les accès à la mémoire RAM contenant du programme exécutable ;
- 2 canaux pour les accès à la mémoire FLASH contenant des données ;
- 3 canaux pour les accès à la mémoire RAM contenant des données.

En cas d'accès non-autorisé, un signal d'interruption est envoyé au CPU.

La figure fonctionnelle ci-dessous décrit les éléments qui interagissent avec la MMU dans le cadre de l'établissement d'un canal d'accès aux mémoires RAM ou FLASH.

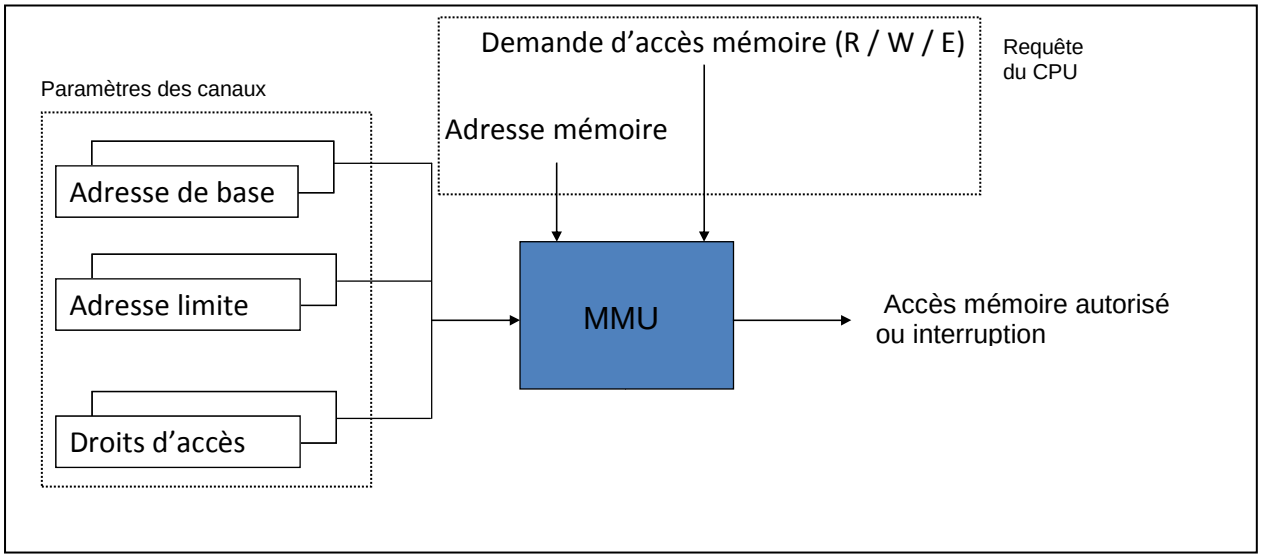

Figure 2: Schéma fonctionnel de la cible d'évaluation

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

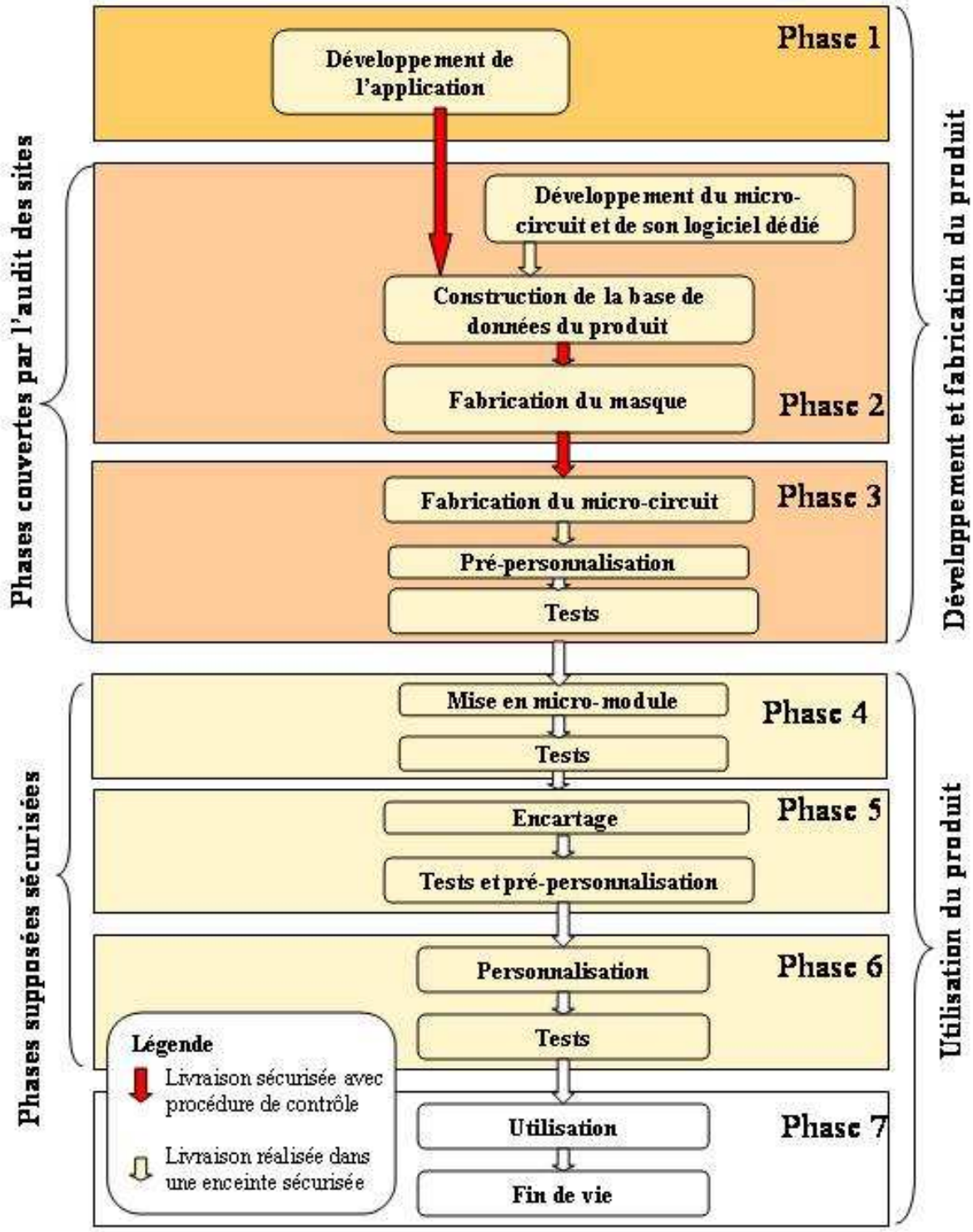

Figure 3: Cycle de vie

Au regard du cycle de vie, le produit est évalué en sortie de la phase 3 du cycle de vie.

Les produits S3FT9KF/ S3FT9KT/ S3FT9KS ont été développés et fabriqués par Samsung Electronics Co. sur ses sites (voir [ANSSI-CC-2012/27]).

La cible d'évaluation a été développée sur le site supplémentaire suivant :

Trusted Labs

5 rue du Baillage
78000 Versailles
France

1.2.5. Configuration évaluée

Le certificat porte sur la configuration telle que présentée au chapitre « 1.2.3 Architecture ».

L'évaluateur a jugé que le microcontrôleur S3FT9KF en révision 1 est représentatif des trois microcontrôleurs supportant la fonctionnalité qui fait l'objet de ce rapport de certification et donc les tests n'ont porté que sur ce composant.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], au document [METHODES-FORMELLES], et à la note [ANSSI-CC-NOTE.12].

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

L'évaluation s'appuie sur les résultats d'évaluation du produit «SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 0 » certifié le 14 juin 2012 sous la référence ANSSI-CC-2012/27 ([ANSSI-CC-2012/27]) et maintenu le 1er octobre 2012 en révision 1 ([ANSSI-CC-2012/27-M01]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 22 mars 2013, 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

Le produit ne comporte pas de mécanismes cryptographiques entrant dans le périmètre d'évaluation.

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

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 le produit « Memory Management Unit des microcontrôleurs SAMSUNG S3FT9KF/ S3FT9KT/ S3FT9KS en révision 1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans la cible de sécurité [ST] pour le niveau d'évaluation EAL 7.

3.2. Restrictions d'usage

Ce certificat porte sur la « Memory Management Unit des microcontrôleurs SAMSUNG S3FT9KF/ S3FT9KT/ S3FT9KS en révision 1» spécifiée au chapitre 1.2 du présent rapport de certification. Il donne une appréciation de la résistance de cette fonctionnalité à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée et du périmètre réduit de cette évaluation.

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].

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'accord[1], 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 signataires[2], 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 7	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**	**6**	Complete semi-formal functional specification with additional formal specification
	ADV_IMP				**1**	1	**2**	2	**2**	Complete mapping of the implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**3**	Minimally complex internals
	ADV_SPM						**1**	1	**1**	Formal TOE security policy model
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**6**	Complete semiformal modular design with formal high-level design presentation
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	**5**	Advanced support
	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_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**2**	Measurable life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**3**	Compliance with implementation standards – all parts
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	**3**	Rigorous analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**4**	Testing: implementation representation
	ATE_FUN		**1**	1	1	1	**2**	2	**2**	Ordered functional testing

	ATE_IND	**1**	**2**	2	2	2	2	**3**	**3**	Independent testing - complete
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]	Cible de sécurité de référence pour l'évaluation : - *Memory Management Unit of Samsung S3FT9KF/ S3FT9KT/ S3FT9KS16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, version 1.5, 20th march 2013, reference ST_Cahokia7_v1.5_20_March_2013.pdf,* Samsung Electronics Co, Ltd. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Memory Management Unit of Samsung S3FT9KF/ S3FT9KT/ S3FT9KS16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, version 1.5, 20th march 2013, reference ST_Cahokia7_Lite.pdf,* Samsung Electronics Co, Ltd.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report CAYUSE, Ref. LETI.CESTI.CA7.RTE.001, 22nd march 2013, v1.1,* CEA-LETI.
[CONF]	Liste de configuration du produit - *Project CAHOKIA7 Life Cycle Definition (Class ALC_CMC.5/CMS.5), version 3.2, 27th march 2013, SAMSUNG.*
[GUIDES]	Guides du produit : - *S3FTKX 16-Bit CMOS MICROCONTROLLERS for Smart Card, reference S3FT9KX_UM_REV1.20, rev 1.20, november 2011*, Samsung Electronics Co, Ltd ; - *Security Application Note for S3FT9KF/KT/KS, version 1.4, 10th november 2011*, Samsung Electronics Co, Ltd.
[PP0035]	*Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007*. Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* sous la référence BSI-PP-0035-2007.
[ANSSI-CC-2012/27]	Certificat ANSSI-CC-2012/27 délivré par l'ANSSI le 14 juin 2012 sous le titre : «*SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 0 »*.
[ANSSI-CC-2012/27-M01]	Rapport de maintenance ANSSI-CC-2012/27-M01 délivré par l'ANSSI le 1er octobre 2012 sous le titre : «*SAMSUNG S3FT9KF/S3FT9KT/S3FT9KS, revision 1* ».

Annexe 3. Références liées à la certification

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.	
[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, 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.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	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.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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 3.0, 8 Janvier 2010, Management Committee.
[ANSSI-CC-NOTE.12]	« Note d'application - Modélisation formelle des politiques de sécurité d'une cible d'évaluation », 25 mars 2008, référence ANSSI-CC-NOTE/12.1, voir http://www.ssi.gouv.fr.
[METHODES-FORMELLES]	« Remarques relatives à l'emploi des méthodes formelles (déductives) en sécurité des systèmes d'information », 14 avril 2008, Eric Jaeger, voir http://www.ssi.gouv.fr.