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-2018/12

S3D350A / S3D300A / S3D264A / S3D232A / S3D200A / S3K350A / S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software

S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A/ S3K300A_rev2_SW10-07-10-20-10-100-103_GU14-16-14-005-102-091-11-22-12-08-00

Paris, le 20 mars 2018

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

Guillaume POUPARD
[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.

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2018/12

Nom du produit

S3D350A / S3D300A / S3D264A / S3D232A / S3D200A / S3K350A / S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software

Référence/version du produit

S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A/ S3K300A_rev2_SW10-07-10-20-10-100-103_GU14-16-14-005-102-091-11-22-12-08-00

Conformité à un profil de protection

Security IC Platform Protection Profile with Augmentation Packages, version 1.0

certifié BSI-CC-PP-0084-2014 le 19 février 2014

avec conformité aux packages

"Authentication of the security IC", "Loader dedicated for usage in Secured Environment only", "Loader dedicated for usage by authorized users only"

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 6 augmenté ASE_TSS.2

Développeur

Samsung Electronics Co. Ltd.

17 Floor, B-Tower, 1-1, Samsungjeonja-ro
Hwaseong-si, Gyeonggi-do 445-330, Corée du Sud

Commanditaire

Samsung Electronics Co.Ltd.

17 Floor, B-Tower, 1-1, Samsungjeonja-ro
Hwaseong-si, Gyeonggi-do 445-330, Corée du Sud

Centre d'évaluation

CEA - LETI

17 avenue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

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 famille de microcontrôleurs « S3D350A / S3D300A / S3D264A / S3D232A / S3D200A / S3K350A / S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, version S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A/ S3K300A_rev2_SW10-07-10-20-10-100-103_GU14-16-14-005-102-091-11-22-12-08-00 » développée par *SAMSUNG ELECTRONICS CO. LTD.*

Les sept microcontrôleurs ont le même *layout*. Les seules différences entre ces microcontrôleurs sont :

- la taille logique de leur mémoire Flash ;
- le mode sans contact qui est désactivé logiquement sur les composants S3K350A et S3K300A.

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, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.2. Description du produit

1.2.1. Introduction

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 [PP0084], avec :

- le package « *authentication of the security IC* » ;
- le package « *loader dedicated for usage in secured environment only* » ;
- le package « *loader dedicated for usage by authorized users only* ».

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[1] ;
- la bonne exécution des services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ou asymétriques ;
- le support à la génération de nombres non prédictibles.

[1] *Target Of Evaluation* – périmètre de l'évaluation.

1.2.3. Architecture

Le produit est constitué d'une partie matérielle et d'une partie logicielle, toutes deux décrites dans la cible de sécurité au chapitre 1.2 « *TOE Overview and TOE Description* ».

La partie matérielle comporte principalement (voir Figure 1) :

- un processeur 32-bit (SC000 CPU) avec firewall (MPU) pour le contrôle d'accès ;
- des mémoires :
  - 36Ko de ROM (4Ko pour le Samsung test mode, 22Ko pour le boot loader, 10Ko pour le System API) ;
  - 232 à 352Ko de Flash, en fonction du microcontrôleur considéré : S3D350A(352Ko), S3D300A(300Ko), S3D264A(264Ko), S3D232A(232Ko), S3D200A(200Ko), S3K350A(352Ko) et S3K300A(300Ko) ;
  - 11Ko de RAM (8,5 Ko SRAM pour un usage général et 2,5Ko pour la Crypto RAM) ;
  - 640 octets de DMA RAM pour l'interface sans contact,
- des modules de sécurité : protection de la mémoire (MPU, *Memory Protection Unit*), génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;
- des modules fonctionnels : gestion des entrées / sorties en mode contact (SIO), interface sans contact (pour les microcontrôleurs S3Dxxxx), générateur de nombres aléatoires – DTRNG[1], coprocesseurs cryptographiques DES et AES et accélérateur de calculs arithmétiques TORNADO™-T.

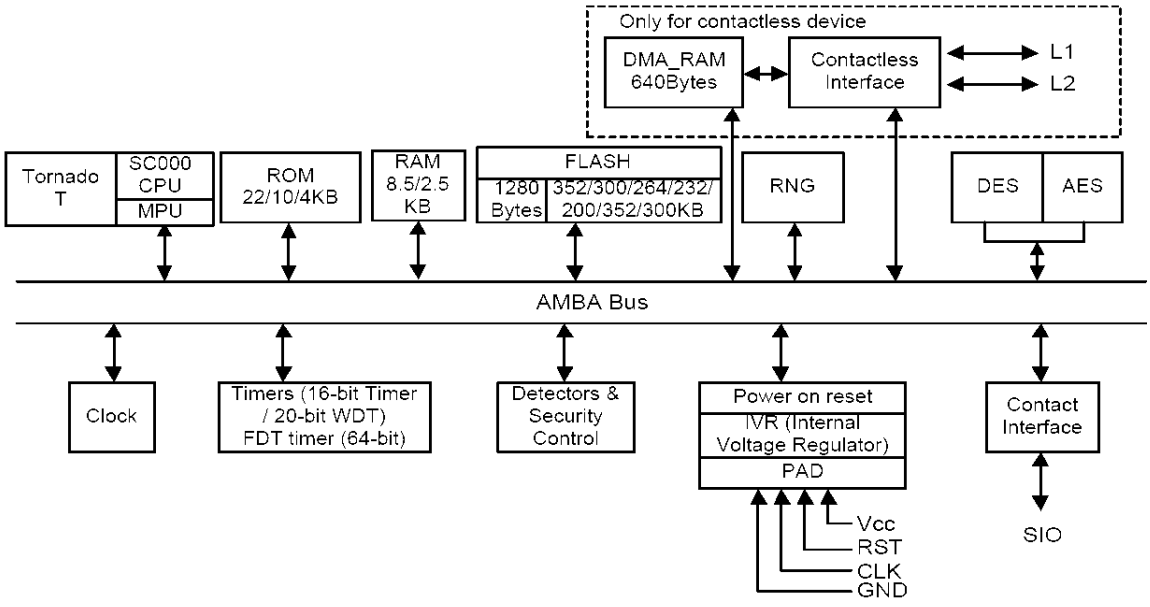

Figure 1 : Architecture du produit

La partie logicielle comporte principalement :

- des logiciels de test du microcontrôleur (Test ROM code version 1.0) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;

[1] *Digital True Random Number Generator* - Générateur physique de nombres aléatoires.

- des bibliothèques optionnelles pour la génération de nombres aléatoires (*DTRNG FRO library* et *EHP DTRNG FRO library*) ;
- des bibliothèques optionnelles pour la cryptographie asymétrique (*AT1 Secure RSA/SHA library* et *AT1 Secure RSA/ECC/SHA Library*) ;
- un *Secure Boot loader* et un System API, permettant le chargement sécurisé du code utilisateur. Le code du System API fait partie de la TOE, mais pas en tant que TSF[1].

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée des microcontrôleurs est identifiable par les éléments donnés dans la table ci-après. Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans le guide « *Chip Delivery Specification S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A/ S3K300A* » (voir [GUIDES]).

Eléments de configuration		Données d'identification lues
Révision matériel, version 2		0x02
Identification des microcontrôleurs	S3D350A	0x0D0305000A
	S3D300A	0x0D0300000A
	S3D264A	0x0D0206040A
	S3D232A	0x0D0203020A
	S3D200A	0x0D0200000A
	S3K350A	0x140305000A
	S3K300A	0x140300000A
Identification des logiciels embarqués	Test ROM code, version 1.0	0x10
	Secure Boot loader and System API code, version 0.7	0x07
Identification des bibliothèques	AT1 Secure RSA/SHA Library version 1.00 (optionnel)	0x312E3030
	AT1 Secure RSA/ECC/SHA Library version 1.03 (optionnel)	0x312E3033
	DTRNG FRO Library, version 1.0 (optionnel)	0x0100
	DTRNG FRO Library, version 2.0 (optionnel pour la conformité à AIS31)	0x0200
	EHP DTRNG FRO Library, version 1.0 (optionnel)	0x0100

L'identification du microcontrôleur est également possible en lisant directement sur la surface du microcontrôleur la donnée 350A, 300A, 264A, 232A ou 200A. Cette identification reste néanmoins partielle car « S3D » ou « S3K » n'est pas mentionné.

[1] *TOE Security Functionality* - Fonctionnalité de sécurité de la TOE.

1.2.5. Cycle de vie

Le cycle de vie du produit est représenté par le schéma suivant :

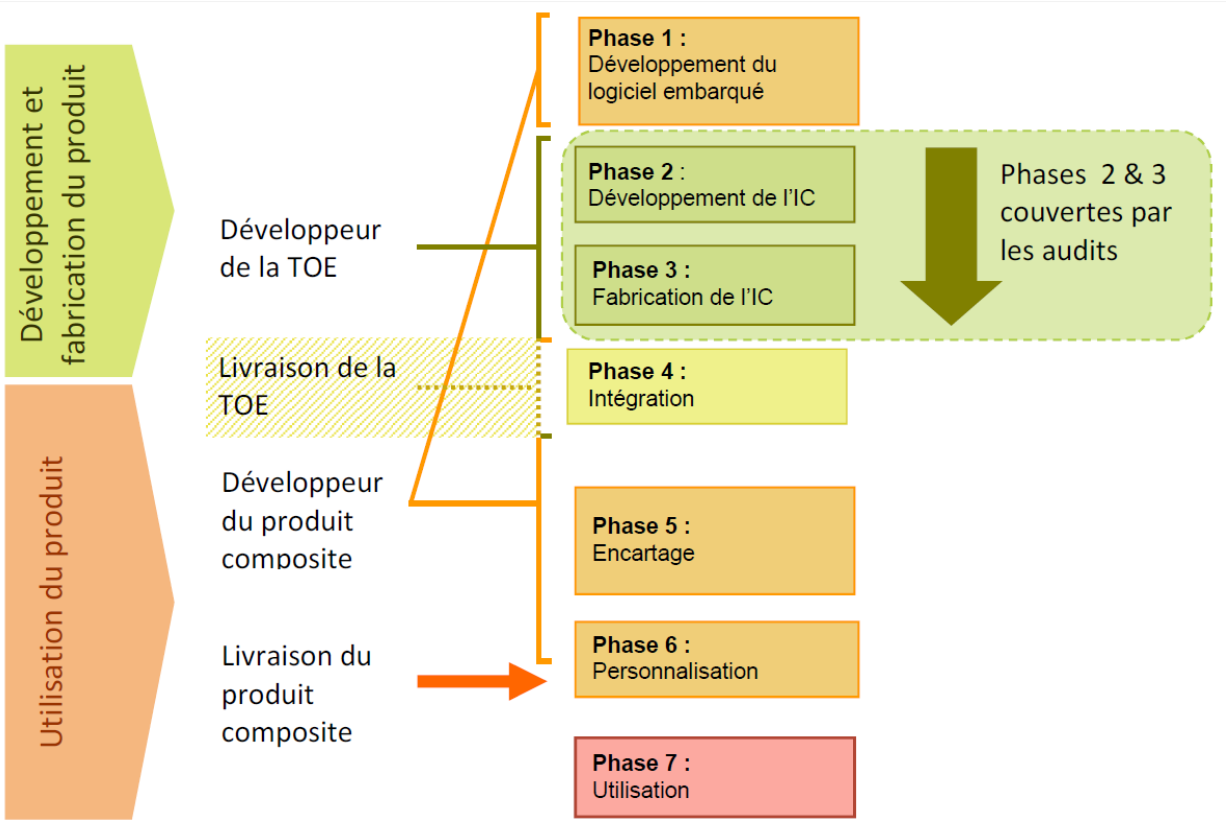

Figure 2 : Cycle de vie du produit

Les phases 2 et 3 correspondent au développement de la TOE. Celle-ci est ensuite livrée sous forme de *wafers*. En option, la TOE peut également être livrée intégrée en boîtiers après la phase 4.

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

- conception du circuit ;
- développement du logiciel dédié.

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

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

La phase 4 correspond aux étapes suivantes :

- packaging de l'IC et test ;
- pré-personnalisation si nécessaire.

Le produit a été développé sur le site suivant :

Nom du Site	Adresse	Fonction
Hwasung Plant/ DSR Building	1, Samsungjeonja-ro, Hwasung-City, Gyeonggi-do, Corée du Sud	Phase 2 : *Smart Card Design Center* Phase 3 : *Test program development*
Hwasung Plant/ NRD Building	San #16, Banwol-Dong, Hwasung-City, Gyeonggi-Do, Corée du Sud	Phase 3 : *Mask Shop*
Giheung Plant/ Line 6, S1	San 24, Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do 446-711 Corée du Sud	Phase 3 : *Wafer Fabrication*
Giheung Plant/ Line 2		Phase 3 : *Inking / Giheung Wafer Stock*
Giheung Plant/ Line 1		Phase 3 : *Grinding*
Onyang Plant/ Warehouse	San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 4 : *Packing, Warehouse*
Onyang Plant/ Line 2		Phase 3&4 : *Stock, Grinding, Sawing, Packaging, Package Testing*
Onyang Plant/ Line 6		Phase 3&4 : *Grinding, Sawing, Packaging, Package Testing*
PKL Plant	493-3, Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, Corée du Sud	Phase 3 : *External Mask Shop*
HANAMICRON plant	#95-1 Wonnam-Li, Umbong-Myeon, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 3&4 : *Grinding, Sawing, Packaging, Package Testing*
Inesa Plant	No. 818 Jin Yu Road Jin Qiao Export Processing Zone Pudong, Shanghai, Chine	Phase 3&4 : *Grinding, Sawing, COB*
		Phase 4 : *Packaging, Warehouse*
Eternal Plant	No.1755, Hong Mei South Road, Shanghai, Chine	Phase 3&4 : *Sawing, COB*
		Phase 4 : *Packing, Warehouse*
TESNA Plant	450-2 Mogok-Dong, Pyeungtaek City, Gyeonggi, Corée du Sud	Phase 3 : Wafer *Testing, Pre-personalization*
ASE Korea	76, Saneopdanji-gil, Paju-si, Gyeonggi-do, Corée du Sud	Phase 3&4 : *Grinding, Sawing, SIP module assembly*

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit le développeur de l'application à embarquer dans le microcontrôleur.

Le produit comporte une gestion de son 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* » : ce mode supporte deux sous-modes d'exécution pour le processeur :
    - le sous-mode « *privilege* » : activé lors de l'exécution de routines d'interruption, il s'agit d'un mode d'exécution interne au processeur qui permet d'accéder aux registres de contrôle et de sécurité, et de configurer la MPU. Lorsque le processeur a terminé l'exécution de la routine, il retourne automatiquement en mode « *user* »,
    - le sous-mode « *user* » : mode normal d'utilisation du microcontrôleur, dans lequel aucun registre de contrôle ou de sécurité n'est accessible.

1.2.6. Configuration évaluée

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils embarquent tels que définis au chapitre 1.2.4. 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 1.2.5, le produit évalué est celui obtenu à l'issue de la phase 3 lorsque le produit est livré sous forme de *wafer*, ou à l'issue de la phase 4 lorsque le produit est livré en boîtiers (micro-modules, etc.).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [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 [JIWG 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 de la famille de produits « S3D350A /S3D300A /S3D264A /S3D232A /S3D200A /S3K350A /S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure RSA and ECC Library including specific IC Dedicated software, version S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A/ S3K300A_rev2_SW10-07-10-10-100_GU14-14-003-09-10-21-12-08-00 » certifiée le 24 août 2017 sous la référence ANSSI-CC-2017/53, voir [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 février 2018, 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 le référentiel technique 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.5 visé.

2.4. Analyse du générateur d'aléas

Le produit embarque un générateur physique de nombres aléatoires, appelé DTRNG FRO, qui a fait l'objet d'une analyse par le CESTI.

Les règles RègleArchiGVA-1 et RègleArchiGVA-2 ainsi que la recommandation RecomArchiGVA-1 de [REF] s'avèrent respectées, lorsque DTRNG FRO est utilisé comme indiqué en §2.3.2 du guide « *S3D350A/S3K170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note* » (voir [GUIDES]). Le document [REF] impose, pour un usage cryptographique, que la sortie d'un générateur matériel de nombres aléatoires subisse un retraitement algorithmique de nature cryptographique ; ce retraitement n'est pas implémenté dans le produit et devra être développé par l'utilisateur le cas échéant.

Le générateur de nombre aléatoire DTRNG FRO, utilisé comme indiqué en §2.3.3 du guide « *S3D350A/S3K170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note* » (voir [GUIDES]), répond aux exigences PTG.2 de la méthodologie [AIS31].

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 la famille de produits « S3D350A / S3D300A / S3D264A / S3D232A / S3D200A / S3K350A / S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, version S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A/ S3K300A_rev2_SW10-07-10-20-10-100-103_GU14-16-14-005-102-091-11-22-12-08-00» soumise à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 6 augmenté de ASE_TSS.2.

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 de la famille de produits « S3D350A / S3D300A / S3D264A / S3D232A / S3D200A / S3K350A / S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, version S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A/ S3K300A_rev2_SW10-07-10-20-10-100-103_GU14-16-14-005-102-091-11-22-12-08-00 » 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 microcircuit 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].

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 puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. 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 EAL 2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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 6+	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	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	Minimally complex internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	5	Complete semiformal 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	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	1	Developer defined 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	2	TOE summary specification with architectural design summary
ATE Tests	ATE_COV		1	2	2	2	3	3	3	Rigorous analysis of coverage
	ATE_DPT			1	1	3	3	4	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	2	Ordered 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]	Cible de sécurité de référence pour l'évaluation : - Security Target of S3D350A /S3D300A /S3D264A /S3D232A /S3D200A /S3K350A /S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, référence ST_KootenaiR2_v2.5, version 2.5, 18/10/2017. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite of S3D350A /S3D300A /S3D264A /S3D232A /S3D200A /S3K350A /S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, référence ST_Lite_S3D350A Family_v2.1, version 2.1, 24/10/2017.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) – KOOTENAI-R2, référence LETI.CESTI.KOOR2.FULL.001-V1.1, version 1.1, 28/02/2018. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation Technical Report (ETR for composition) – KOOTENAI-R2, référence LETI.CESTI.KOOR2.COMPO.001-V1.0, version 1.0, 27/10/2017.
[CONF]	Liste de configuration du produit : Configuration Management (Class ALC_CMC.5/CMS.5), référence Kootenai-R2_ALC_CMC_CMS_V3.2, version 3.2, 19/10/2017.
[CER]	Rapport de certification ANSSI-CC-2017/53, S3D350A /S3D300A /S3D264A /S3D232A /S3D200A /S3K350A /S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure RSA and ECC Library including specific IC Dedicated software, revision 2. *Certifié par l'ANSSI le 24 août 2017 sous la référence ANSSI-CC-2017/53.*
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*

[GUIDES]	Guides du produit, (les guides indiqués en gras ont été mis à jour ou ajoutés depuis la certification précédente, voir [CER]) : - S3D350A/S3K170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note, référence S3D350A_S3K170A_S3K250A_DTRNG_FRO_AN_v1.4, version 1.4, 12/10/2016[1] ; - **S3D350A/S3K170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note, référence S3D350A_S3K170A_S3K250A_DTRNG_FRO_AN_v1.6.pdf, version 1.6, 12/10/2017[2] ;** - S3D350A/S3K170A/S3K250A HW DTRNG FRO and EHP DTRNG FRO Library Application Note, référence S3D350A_S3K170A_S3K250A_EHP_DTRNG_FRO_AN_v1.4 version 1.4, 12/10/2016 ; - **RSA/ECC Library API Manual for S3D350A, S3K250A and S3K170A, référence AT1 RSA ECC Library API Manual v0.05, version 0.05, 17/10/2017[3] ;** - **RSA/ECC Library API Manual for S3D350A, S3K250A and S3K170A, référence AT1 RSA ECC Library API Manual v1.02, version 1.02, 16/10/2017[4] ;** - **User's Manual for S3D350A families (Supported Devices: S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A/ S3K300A/ S3K250A/ S3K232A/ S3K212A/ S3K170A/ S3K140A), référence S3D350A Families_UM_REV0.91, version 0.91, 21/07/2017 ;** - **Security Application Note for S3D350A Family, S3K250A Family, S3K170A Family, référence SAN_S3D350A_Series_v1.1, version 1.1, 13/10/2017 ;** - **Chip Delivery Specification S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/S3K350A/ S3K300A, référence S3D350A Family_DV22, version 2.2, octobre 2017 ;** - Bootloader Specification for S3D350A Series (Supported Devices: S3D350A Family, S3K250A Family, S3K170A Family, référence S3D350A Series_Bootloader_Specification_v1.2, version 1.2, 09/03/2017 ; - System API application note for S3D350A Families (Supported Devices: S3D350A Family, S3K250A Family, S3K170A Family), référence S3D350A Families_AN08_SystemAPI_v0.8, version 0.8, 09/03/2017 ; - SC000 Reference Manual, référence SC000_Reference_Manualv0.0, version 0.0, 13/10/2016.

[1] Guide pour la bibliothèque « DTRNG FRO Library, version 1.0 ».
[2] Guide pour la bibliothèque « DTRNG FRO Library, version 2.0 », incluant la conformité à l'AIS31.
[3] Guide pour la bibliothèque « AT1 Secure RSA/SHA Library version 1.00 ».
[4] Guide pour la bibliothèque « AT1 Secure RSA/SHA Library version 1.03 ».

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.