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-2014/44

Microcontrôleurs sécurisés ST23ZR08/ST23ZR04/ST23ZR02, ST23ZC08/ST23ZC04/ST23ZC02 maskset K340A revision interne M

Paris, le 16 octobre 2014

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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2014/44

Nom du produit

Microcontrôleurs sécurisés ST23ZR08/ST23ZR04/ST23ZR02, ST23ZC08/ST23ZC04/ST23ZC02

Référence/version du produit

Révision externe A, révision interne M (logiciel de test dédié OST YBC version 61, maskset K340A)

Conformité à un profil de protection

[BSI-PP-0035-2007]

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(s)

STMicroelectronics

ZI de Rousset BP 2, 13106 Rousset Cedex, France

Commanditaire

STMicroelectronics

ZI de Rousset BP 2, 13106 Rousset Cedex, France

Centre d'évaluation

SERMA Technologies

14 rue Galilée, CS – 10055, 33615 PESSAC Cedex, 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 famille de « Microcontrôleurs sécurisés ST23ZR08/ST23ZR04/ST23ZR02, ST23ZC08/ST23ZC04/ST23ZC02 », en révision externe A, en révision interne M, avec le logiciel de test dédié OST (« *Operating system for Test* ») YBC en version 61 et en maskset K340A, développé par STMicroelectronics.

Pour des raisons commerciales, ce produit est vendu sous d'autres références détaillées au chapitre « 2.1 TOE Overview » de la [ST] », la différence réside uniquement dans la taille de la mémoire non volatile et le type d'interface (dual ou « sans contact » uniquement) proposés comme le résume le tableau suivant :

Nom du produit	Quantité de mémoire EEPROM	Modes I/O
ST23ZR08	8 Ko	Dual
ST23ZR04	4 Ko	Dual
ST23ZR02	2 Ko	Dual
ST23ZC08	8 Ko	Sans-contact
ST23ZC04	4 Ko	Sans-contact
ST23ZC02	2 Ko	Sans-contact

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 [BSI-PP-0035-2007].

1.2.1 Identification du produit

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

La version certifiée du produit est identifiable par les éléments suivants (voir [ST] au chapitre « 2.1 TOE overview » et [GUIDES] pour plus de détails) :

- informations écrites sur le microcontrôleur :
  - K340A : nom interne STMicroelectronics du produit (Maskset), la lettre A correspond à la révision externe, elle identifie la lettre de la révision majeure du silicium ;
  - YBC : trigramme identifiant le logiciel de test dédié OST ;
  - UZI[1] : trigramme identifiant le logiciel utilisateur embarqué en ROM *User* ; dans le cas présent de l'évaluation, il identifie le système d'exploitation de démonstration STMicroelectronics appelé « *Card Manager* » (ou encore « *Reference Implementation* »). Le *Card Manager* n'entre pas dans le périmètre d'évaluation ;
  - ST 4 : Identification du site de fabrication (ici, 4 correspond au site de STMicroelectronics/Rousset) ;
- informations présentes dans la zone OTP (« *One Time Programmable* ») de la mémoire EEPROM accessibles par l'utilisateur (voir [GUIDES] pour plus de détails):
  - « 0015h » : ces 2 octets identifient chaque variante du produit, ici cela correspond à ST23ZR08 ; pour les autres variantes ST23ZR04, ST23ZR02, ST23ZC08, ST23ZC04, ST23ZC02 du produit, cette valeur est « 0020h », « 0021h », « 0022h », « 0023h », « 0024h » respectivement ;
  - « 61h » : cet octet identifie la version du logiciel de test dédié OST, la valeur est écrite en hexadécimal ;
  - « 4Dh » : cet octet identifie la lettre de la révision interne du produit (M), cette valeur est écrite en caractère ASCII codé en format hexadécimal.

Le produit est une évolution de celui précédemment certifié sous la référence [ANSSI-CC-2012/42].

1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit, détaillés au chapitre « 2.1 TOE overview » de la [ST], sont :

- l'initialisation de la plate-forme matérielle et des attributs ;
- la gestion sécurisée du cycle de vie ;
- l'intégrité logique du produit ;
- le test du produit ;
- la gestion mémoire (*firewall*) ;
- la protection physique ;
- la gestion des violations sécuritaires ;
- la non-observabilité ;
- le support au chiffrement cryptographique à clés symétriques ;

[1]Ce trigramme identifie le logiciel embarqué et est propre à chaque utilisateur car le logiciel embarqué est fourni par le client au commanditaire pour être mis en ROM. Le trigramme présent sur les puces fournies à un client sera donc forcément différent de celui apparaissant sur les microcontrôleurs évalués.

- le support à la génération de nombres non prédictibles.

1.2.3 Architecture

L'architecture de la TOE est illustrée dans la figure suivante :

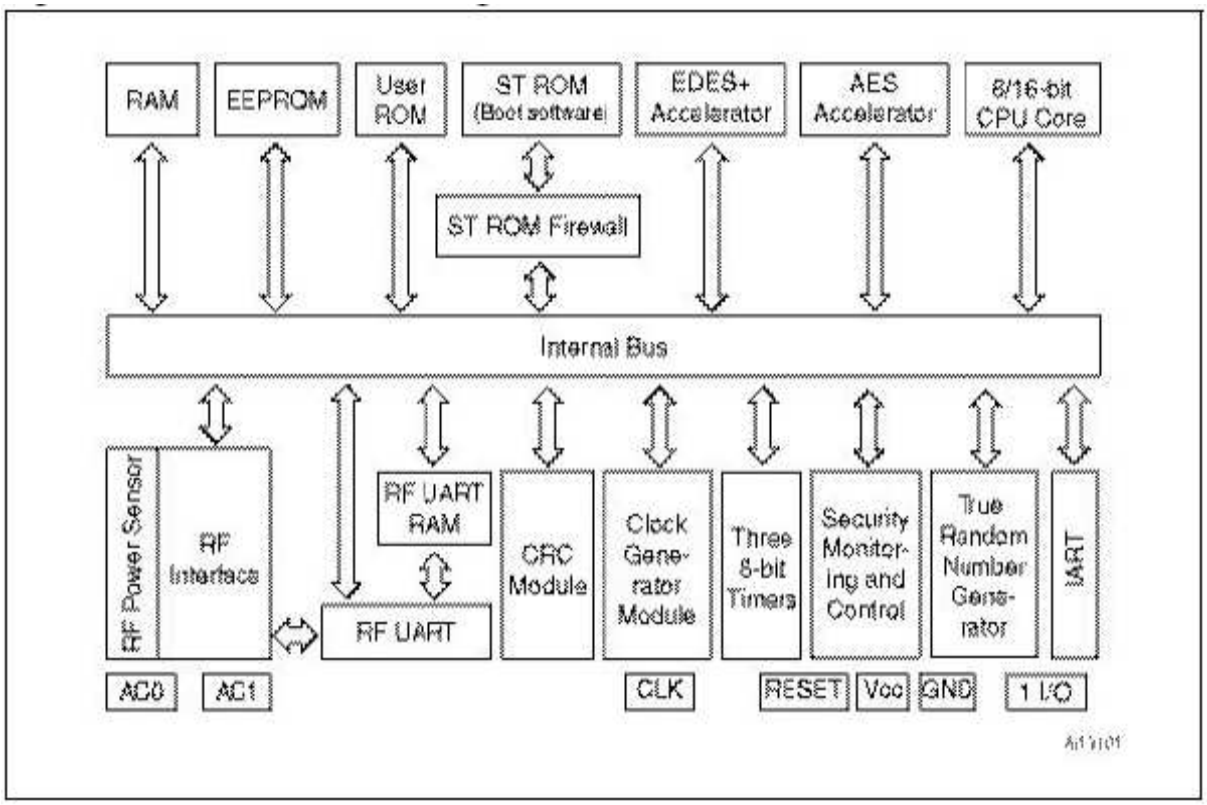

Figure 1 : architecture du microcontrôleur

En plus de ces composants matériels, la TOE embarque également, dans la ROM, un composant logiciel OST qui :

- assure le démarrage du produit (« *Boot* ») ;
- offre des commandes pour les tests et la maintenance de la TOE ;
- assure également un contrôle d'accès à ces fonctionnalités lorsque la TOE est en configuration « Test » ou en configuration « *User* ».

Ce logiciel n'est plus accessible une fois que la TOE est configurée en mode « *end user* » (voir chapitre suivant « 1.2.4 Cycle de vie).

1.2.4 Cycle de vie

Le cycle de vie du produit est conforme à celui décrit dans [BSI-PP-0035-2007]. Il est détaillé aux chapitres « 2.3 TOE life cycle » et « 2.4 TOE environment » de la [ST]. Les différentes étapes sont récapitulées dans le tableau suivant :

Phase	***Nom***	***Description***	***Entité responsable***
1	Développement de l'application embarquée	Développement de l'application utilisateur	Développeur de l'application utilisateur
2	Développement du composant	- Conception du composant - Développement du logiciel dédié OST	Concepteur et développeur du composant : STM (Rousset, Valbonne, Grenoble/France et Ang Mo Kio/Singapour), George Charpak (Gardanne/France)
3	Fabrication du composant	- Fabrication et intégration du *photomask* - Production du composant - Test du composant - Préparation - Pré-personnalisation	- Fabrication du *photomask :* DNP/Japon et DPE/Italie - Fabricant du composant : STM (Rousset/France) - Testeur : STM (Rousset/France et Toa Payoh/Singapour)
4	*Packaging* du composant	- *Packaging* du composant (et test)	Chargé du *packaging* du composant : STM (Bouskoura/Maroc), STS (Shenzen/Chine), STM (Calamba/Philippines), SMARTFLEX (Singapour) et NEDCARD (Pays-bas) qui utilise DISCO (Allemagne) pour le sciage des wafers
5	Intégration du produit composite	- Process de finalisation du produit composite - Préparation du produit composite - Expédition du produit composite	Intégrateur du produit composite
6	Personnalisation	- Personnalisation du produit composite - Test du produit composite	Personnalisateur
7	Utilisation	Utilisation du produit composite par ses émetteurs et utilisateurs finaux	Utilisateurs finaux

Les autres entités pouvant intervenir durant la production de la TOE sont :
- STM (Loyang et Ang Mo Kio/Singapour) pour la logistique ;
- STM (Shenzen/Chine) et DISCO (Allemagne) pour l'amincissement des *wafers*.

La présente évaluation a couvert les phases 2, 3 et 4 du cycle de vie décrit plus haut. L'évaluation a également couvert les procédures de livraison et de vérification de l'application développée en phase 1, ainsi que les procédures de livraison de la TOE à l'entité chargée du packaging du composant intervenant en phase 4. Les procédures correspondant aux autres phases sont en dehors du périmètre de cette évaluation.

La TOE est toujours livrée en mode « *End User* » :
- soit sous forme de *wafer*, éventuellement scié, en fin de phase 3 ;
- soit sous une forme packagée en fin de phase 4.

Le produit est conçu, développé, intégré (préparation de la base de données du produit), fabriqué et testé par :

STMicroelectronics SAS (Rousset/France),
SMD division, 190 Avenue Célestin Coq, ZI de Rousset, BP2,
13106 Rousset Cedex,
France.

Une partie du développement du produit est réalisée par :

STMicroelectronics Pte ltd (Ang Mo Kio/Singapour),
5A Serangoon North Avenue 5,
554574, Singapore,
Singapour.

STMicroelectronics (Valbonne/France)
635 route des lucioles,
06560 Valbonne,
France.

STMicroelectronics (Grenoble/France)
12 rue Jules Horowitz, BP 217
38019 Grenoble Cedex,
France.

CMP George Charpak (Gardanne/France)
880 Avenue de Mimet
13542 Gardanne
France.

Le produit peut également être testé par :

STMicrolectronics (Toa Payoh/Singapour),
629 Lorong 4/6 Toa Payoh
319521
Singapour.

Les réticules du produit sont fabriqués par :

DAI NIPPON PRINTING CO., LTD (DNP/Japon),
2-2-1, Fukuoka, kamifukuoka-shi,
Saitama-Ken, 356-8507,
Japon.

DAI NIPPON PRINTING EUROPE (DPE/Italie),
Via C. Olivetti, 2/A,
I-20041 Agrate Brianza,
Italie.

Le produit peut transiter par un site de logistique :

STMicroelectronics (Loyang/Singapour)
7 loyang Drive
508938
Singapour.

STMicroelectronics (Ang Mo Kio/Singapour)
18 Ang Mo Kio Industrial park 2
56950
Singapour.

Le produit peut être mis en module ou en boitier par :

STMicroelectronics SA (Bouskoura/Maroc),
101, boulevard des Muriers BP 97,
20180, Bouskoura – Casablanca,
Maroc.

STS Microelectronics (Shenzen/Chine)
16 Tao hua Rd.
Futian free trade zone
518048 Shenzen
P.R Chine.

STMicroelectronics (Calamba/Philippines)
9 Mountain Drive
LISP II, Brgy La mesa
Calamba,
Philippines 4027.

SMARTFLEX TECHNOLOGIES (Singapour),
N°27 UBI rd 4, MSL building #04-04
408618
Singapour.

NEDCARD BV (Pays-bas),
Bijsterhuizen 25-29,
6604 LM Wijchen,
Pays-Bas.

NEDCARD utilise **DISCO** pour le sciage des wafers :
DISCO HI-Tec Europe GmbH (Allemagne),
Liebigstasse 8,
D-85551Kirchheim bei Munchen,
Allemagne.

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit le développeur de l'application utilisateur à embarquer dans le microcontrôleur (il n'y a pas de rôle « administrateur » défini dans le produit).

Le produit comporte lui-même une gestion de son cycle de vie, prenant la forme de deux configurations d'utilisation :

- configuration « Test » : à la fin de sa fabrication en phase 3, le microcontrôleur est testé à l'aide du logiciel de test présent en ROM ; les données de pré-personnalisation peuvent être chargées en EEPROM ; cette configuration est ensuite bloquée de manière irréversible lors du passage en configuration « *User* » ;
- configuration « *User » :* ce mode, activé en fin de phase 3, comprend trois sous-modes :
  - mode « *reduced test »* permettant à STMicroelectronics d'effectuer quelques tests restreints ;
  - mode « *diagnosis » :* sous-ensemble du mode « *reduced test »*, il est réservé à STMicroelectronics ;
  - mode « *end user » :* mode final d'utilisation du microcontrôleur qui fonctionne alors sous le contrôle du logiciel embarqué de la carte à puce ; le logiciel de test n'est plus accessible ; les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans cette configuration.

1.2.5 Configuration évaluée

Le certificat porte sur la TOE définie plus haut au chapitre « 1.2.3 Architecture » et configurée en mode « *User* ». Les caractéristiques de cette TOE sont :

Nom du Produit	Quantité de mémoire EEPROM	Modes I/O	Maskset	Version du Maskset externe/interne	Nom de l'OST	Version de l'OST
ST23ZR08	8 Ko	Dual	K340A	A/M	YBC	61h
ST23ZR04	4 Ko	Dual	K340A	A/M	YBC	61h
ST23ZR02	2 Ko	Dual	K340A	A/M	YBC	61h
ST23ZC08	8 Ko	Sans-contact	K340A	A/M	YBC	61h
ST23ZC04	4 Ko	Sans-contact	K340A	A/M	YBC	61h
ST23ZC02	2 Ko	Sans-contact	K340A	A/M	YBC	61h

Tous ces produits sont identiques du point de vue matériel et en particulier présentent le même *layout*. Les résultats sont applicables à l'ensemble des configurations listées.

Pour les besoins de l'évaluation, les échantillons de la TOE livrés à l'évaluateur embarquaient dans la ROM un système d'exploitation dit « *Card Manager* » identifié par le trigramme UZI et dont l'objet était de permettre :

- l'interaction avec la TOE au travers de commandes passées par l'I/O ;
- le chargement en EEPROM, ou en RAM, d'applications de tests.

Ce « *Card Manager* » ne fait pas partie du périmètre de l'évaluation.

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 [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 [CC AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [CC 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 23 septembre 2014, 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-CRY] 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

Le générateur de nombres aléatoires, de nature physique, a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d’évaluation : il atteint le niveau « P2 – SOF High ».

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 sécurisés ST23ZR08/ST23ZR04/ST23ZR02, ST23ZC08/ST23ZC04/ST23ZC02 », en révision externe A, en révision interne M, avec le logiciel de test dédié OST YBC en version 61 et en *maskset* K340A, soumise à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa 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 du produit 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].

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 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_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	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	**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**	**2**	**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]	Cible de sécurité de référence pour l'évaluation : - ST23ZR08, ST23ZR04, ST23ZR02, ST23ZC08, ST23ZC04, ST23ZC02, Security Target, référence SMD_ST23Zxxx_ST_10_001_V02.05, STMicroelectronics. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST23ZR08, ST23ZR04, ST23ZR02, ST23ZC08, ST23ZC04, ST23ZC02, Security Target – Public Version, référence SMD_ST23ZRCxxx_ST_11_001 Rev 01.04, STMicroelectronics.
[RTE]	Rapport technique d'évaluation : - *Evaluation technical report - Project: COGNAC_R-2*, référence COGNAC-R-2_ETR_v1.1, version: 1.1, SERMA TECHNOLOGIES ITSEF. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - *Evaluation technical report lite - Project: ST23ZR08*, référence ST23ZR08_ETRLiteComp_v1.1, version: 1.1, SERMA TECHNOLOGIES ITSEF.
[CONF]	Liste de configuration du produit : - La liste de configuration est incluse dans l'analyse d'impact sécuritaire, référence SMD_ST23ZR08_revM_SIA_13_001, version 1.4, STMicroelectronics. Liste de la documentation du produit pour l'évaluation : - Cognac-R - ST23ZR08 - CC Evaluation Documentation Report, référence SMD_ST23Zxxx_DR_13_001, version 2.2, STMicroelectronics.
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : - ST23ZRxx/ST23ZCxx Secure microcontroller with enhanced security with up to 8 Kbyte EEPROM and dual or contactless-only interface - Preliminary Datasheet, référence DS_23ZR08, version 4.0, STMicroelectronics. - Programming Manual ST21/23 SmartcardMCU, référence PM_21_23, version 3.0, STMicroelectronics. - Application Note - ST23ZRxx/ST23ZCxx Recommendations for Contactless Operations, référence AN_23Zx_RF_RCMD, version 1.0, STMicroelectronics, - How to identify certified hardware devices using additional ST

	traceability information, référence AN_TRACE, version 2.0, STMicroelectronics, - ST23 AIS 31: Compliant Random Number – User Manual, référence UM_23_AIS31, v2.0, STMicroelectronics, - ST23 AIS 31: Reference Implementation - StartUp, Online and Total Failure Tests, référence AN_23_AIS31, v2.0, STMicroelectronics, - Application Note ST23ZRxx/ST23ZCxx Security guidance, référence AN_SECU_23ZR08 Rev 5, STMicroelectronics.
[ANSSI-CC-2012/42]	Certificat ANSSI délivré le 19 Juillet 2012 pour les produits « Microcontrôleurs sécurisés ST23ZR08A / ST23ZR04A / ST23ZR02A, ST23ZC08A / ST23ZC04A / ST23ZC02A».
[BSI-PP-0035-2007]	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.*

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.
[JIWG IC]*	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP]*	Mandatory Technical Document – Application of attack potential to smart-cards, JIWG, version 2.9, January 2013.
[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.
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, 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.