Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/15

Micro-circuit ST22L128-A rev. L

Paris, le 29 juin 2005

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

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

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

Synthèse

Rapport de certification 2005/15

Produit : Micro-circuit ST22L128-A rev. L

Développeur(s) : STMicroelectronics

Critères Communs version 2.2

EAL5 Augmenté
(ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

conforme au profil de protection BSI-0002-2001

Commanditaire : STMicroelectronics

Centre d'évaluation : CEACI

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics. (article 7)
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (article 8)

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

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le micro-circuit ST22L128-A en révision L (maskset K640LMA). Le micro-circuit inclut une partie logicielle en ROM intégrant le logiciel dédié OST référence V5.0 XLG, l'interface logicielle « hardware/software » (HSI) référence SmartJ_HSI V3.00 patch V00.01, et une bibliothèque cryptographique logicielle référence LIB_CHIP V02.21.

1.2. Développeur

Deux acteurs interviennent dans la conception et la fabrication du micro-circuit :

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

STMicroelectronics

Smartcard IC division
ZI de Rousset, BP2
13106 ROUSSET CEDEX
FRANCE

Les réticules du produit sont fabriqués par :

DAI NIPPON PRINTING CO., LTD

2-2-1, Fukuoka, kamifukuoka-shi,
SAITAMA-KEN, 356-8507
JAPON

1.3. Description du produit évalué

Le produit évalué est le micro-circuit ST22L128-A rev. L de la plate-forme ST22 développée et fabriquée par STMicroelectronics.
Le produit a trois modes d'utilisation :

- mode «Test» : à la fin de sa fabrication, le micro-circuit est testé à l'aide du logiciel de test présent en ROM. Les données de pré-personnalisation peuvent être chargées en EEPROM. Ce mode est ensuite bloqué de manière irréversible lors du passage en mode «Issuer» ;
- mode «Issuer» : mode utilisé lors des phases d'encartage et de personnalisation du micro-circuit. Certains tests internes du micro-circuit sont encore disponibles. Les données de personnalisation peuvent être chargées en EEPROM. Ce mode est ensuite bloqué de manière irréversible lors du passage en mode «User» ;
- mode «User» : mode final d'utilisation du micro-circuit 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 micro-circuit que dans ce mode.

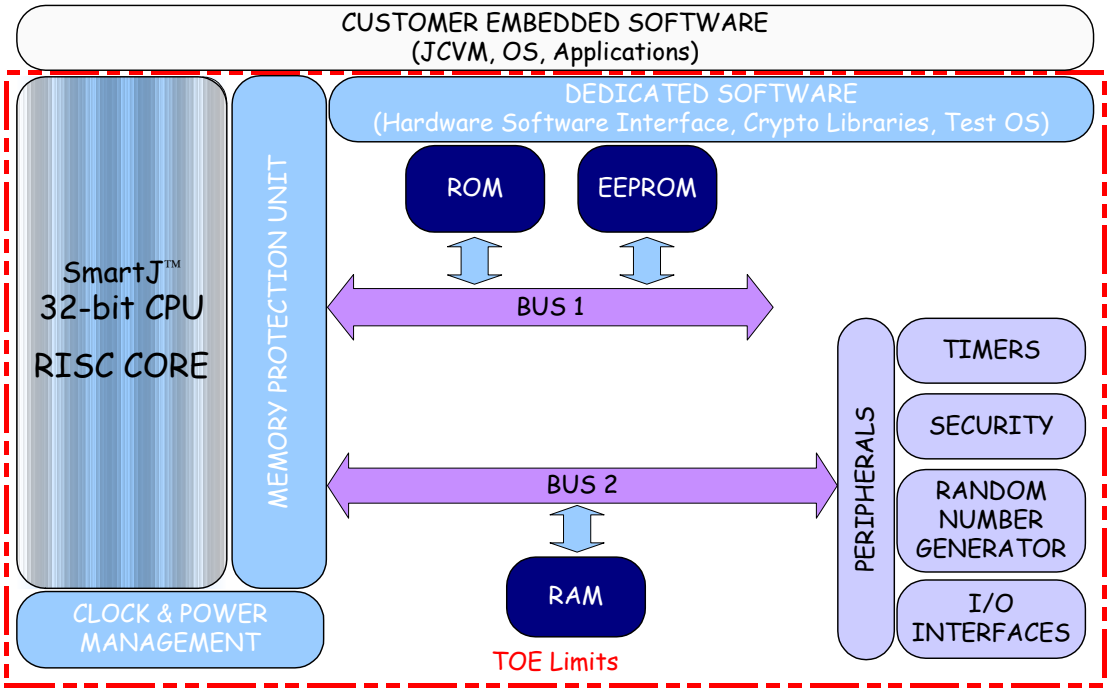
Le micro-circuit seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou des applications et à être inséré dans un support plastique compatible avec une

utilisation finale. Il pourra s'agir d'une carte à puce dont les usages possibles sont multiples (applications bancaires, télévision à péage, transport, santé,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels n'ont pas fait partie de l'évaluation.

1.3.1. Architecture

Le micro-circuit ST22L128-A rev. L est constitué des éléments suivants :

- une partie matérielle composée :
  - d'un processeur RISC 32-bit, incluant une exécution matérielle des instructions Javacard™, des modes User et Superviseur ainsi qu'un jeu d'instructions privilégiées dont certaines dédiées à la cryptographie ;
  - de mémoires : 128KB de mémoire EEPROM (avec contrôle d'intégrité) pour le stockage des programmes et des données , 240KB de ROM pour le stockage des programmes utilisateurs, 8KB de mémoire RAM et 80KB de mémoire ROM pour le stockage des logiciels dédiés (logiciel de test, HSI et librairie cryptographique) ;
  - de modules de sécurité : contrôle logique d'accès aux ressources matérielles, protection dynamique des mémoires, par domaine applicatif, générateur interne d'horloge et d'aléas, contrôleur centralisé de sécurité, gestion de l'alimentation, contrôle d'intégrité des mémoires, accélérateur matériel de communication carte à puce en mode contact (ISO 7816), implémentation de mécanismes matériels de protection contre les fuites et les intrusions physiques du produit.
- une partie logicielle en ROM intégrant :
  - des logiciels de tests du micro-circuit («autotest»),
  - des utilitaires pour la gestion du système et de l'interface hardware/software,
  - des services cryptographiques optionnels parmi lesquels les fonctions de génération de nombres aléatoires, SHA-1, DES, Triple DES et AES sont inclus dans la cible de sécurité du produit.



1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

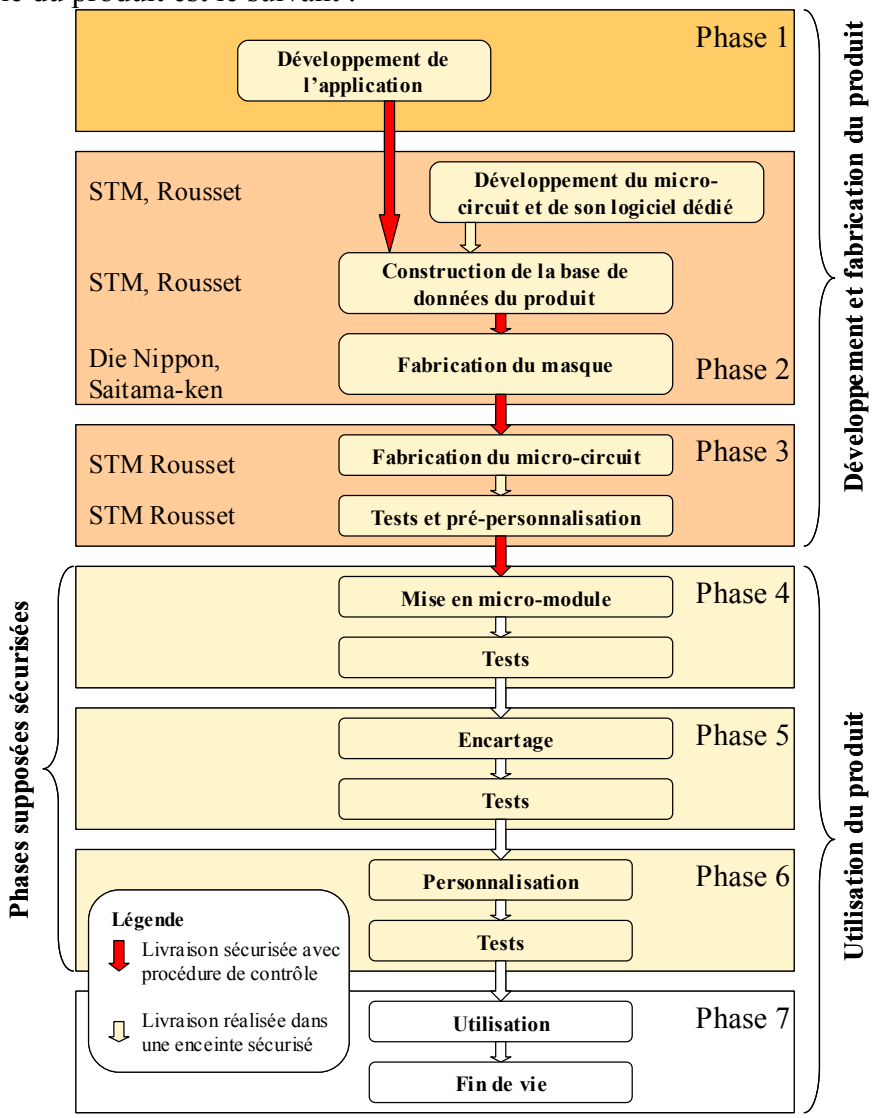


Figure 1 - Cycle de vie standard d'une carte à puce

1.3.3. Périmètre et limites du produit évalué

Ce rapport de certification présente les travaux d'évaluation relatifs au micro-circuit et à la librairie logicielle identifiés au §1.1, conformément à la description et aux limites indiquées au §1.3.1. Toutes autres applications éventuellement embarquées, notamment les routines embarquées pour les besoins de l'évaluation, ne font donc pas partie du périmètre d'évaluation.

En regard du cycle de vie, le produit évalué est le produit qui sort de la phase de fabrication, tests et pré-personnalisation (phase 3).

2. L'évaluation

2.1. Référentiels d'évaluation

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

2.2. Commanditaire

STMicroelectronics

Smartcard IC division
ZI de Rousset, BP2
13106 ROUSSET CEDEX
FRANCE

2.3. Centre d'évaluation

L'évaluation du produit a été réalisée par le centre d'évaluation :

CEACI

18 avenue Edouard Belin
31401 Toulouse Cedex 4

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : ceaci@cnes.fr

Cependant, les tâches environnementales ont été réalisées par le centre d'évaluation :

SERMA Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Téléphone : +33 (0)5 57 26 08 64

Adresse électronique : m.dus@serma.com

2.4. Rapport technique d'évaluation

L'évaluation s'est déroulée de mars 2004 à mai 2005.

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

2.5. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Cette cible de sécurité est conforme au profil de protection BSI-0002-2001 (cf. [PP_BSI]).

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

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite

2.6. Evaluation du produit

2.6.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL5[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL5	Methodically designed, tested, and reviewed
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_MSU.3	Analysis and testing for insecure state
+ AVA_VLA.4	Highly resistant

2.6.2. L'évaluation de l'environnement de développement

Le produit est développé sur les sites identifiés au §1.2 (Rousset en France et Saitama-Ken au Japon).

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

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

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

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

L'évaluateur a vérifié que le cycle de développement du produit correspondait à un cycle de vie standard, appliqué dans le domaine de la carte à puce[1]. L'évaluateur a également vérifié que les méthodes et outils de développement étaient documentés et correspondent à des standards d'implémentation.

La vérification de l'application des procédures analysées a été effectuée lors d'une visite du site de Rousset (cf Annexe 1). Le site de Saitama-Ken n'a pas fait l'objet de visite, ayant déjà été audité dans le cadre d'un autre projet (cf. [2003/18]).

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

Classe ACM: Gestion de configuration		**Verdicts**
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.3	Development tools CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.2	Standardised life-cycle model	Réussite
ALC_TAT.2	Compliance with development standards	Réussite

2.6.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles semi-formelles (FSP), conception de haut-niveau semi-formelle (HLD), conception de bas-niveau (LLD), implémentation (IMP). La conception modulaire est réalisée de fait, de par les techniques de développement hardware, et n'a pas fait l'objet d'une analyse particulière.

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

- Exigences extraites des [CC] :
  - Cryptographic Key Generation (FCS_CKM.1)
  - Cryptographic operation (FCS_COP.1)
  - Complete access control (FDP_ACC.2)
  - Security attributes based access control (FDP_ACF.1)
  - Subset information flow control (FDP_IFC.1)
  - Basic internal transfer protection (FDP_ITT.1)
  - Management of security attributes (FMT_MSA.1)
  - Static attribute initialisation (FMT_MSA.3)

[1] Il ne s'agit pas d'un modèle de cycle de vie normalisé par une instance de normalisation, mais formalisé rigoureusement et correspondant au modèle reconnu et utilisé dans le domaine de la carte à puce (cf. [CC] partie 3, §386).

  - Specification of management functions (FMT_SMF.1)
  - Failure with preservation of secure state (FPT_FLS.1)
  - Resistance to physical attack (FPT_PHP.3)
  - Complete reference monitor (FPT_SEP.3)
  - Limited fault tolerance (FRU_FLT.2)
- Exigences de sécurité explicitement énoncées :
  - Audit storage (FAU_SAS.1)
  - Quality metrics for random numbers (FCS_RDN.1)
  - Limited capabilities (FMT_LIM.1)
  - Limited availability (FMT_LIM.2)

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

Classe ADV: Développement		**Verdicts**
ADV_SPM.3	Formal security policy model	Réussite
ADV_FSP.3	Semiformal functional specification	Réussite
ADV_HLD.3	Semiformal high-level design	Réussite
ADV_INT.1	Modularity	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_RCR.2	Semiformal correspondence demonstration	Réussite

2.6.4. L'évaluation des procédures de livraison et d'installation

Conformément au guide pour l'évaluation « The application of CC to IC » (cf. [CC_IC]), les livraisons considérées sont :

- la livraison du code des applications embarquées au fabricant du micro-circuit,
- la livraison des informations nécessaires au fabricant du masque,
- la livraison du masque au fabricant du micro-circuit,
- la livraison des micro-circuits au responsable de l'étape suivante (mise en micro-module, encartage).

Les différents sites impliqués sont identifiés au §1.2 du présent rapport.

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

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

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

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

2.6.5. L'évaluation de la documentation d'exploitation

Utilisation

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

Dans le cadre de cette évaluation, ces rôles sont rappelés dans la cible de sécurité [ST §5.3.1] : les utilisateurs sont définis comme étant les personnes pouvant mettre en œuvre les fonctionnalités du micro-circuit, de sa bibliothèque logicielle et de son logiciel applicatif. Cette définition comprend tous les utilisateurs utilisant le produit en mode « user » : l'émetteur de la carte mais également le développeur du logiciel embarqué, le responsable de l'encartage et la personne en charge d'intégrer la carte dans son système d'utilisation finale.

Administration

Le guide « The application of CC to Integrated Circuits » [CC IC] spécifie les administrateurs du produit comme étant les différents intervenants des phases 4 à 7 du cycle de vie et qui configurent (personnalisation) le produit final. Ces opérations sont en grande partie liées au type d'applications embarquées. Dans le cadre d'un micro-circuit, seules les interfaces d'administration propres au micro-circuit sont évaluées. Par ailleurs, les phases 4 à 6 dites « d'administration » sont couvertes par une hypothèse dans le profil de protection, qui suppose que les opérations associées à ces phases sont réalisées dans des conditions ne remettant pas en cause la sécurité du produit. Ces conditions n'ont pas été évaluées.

L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

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

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

2.6.6. L'évaluation des tests fonctionnels

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

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué.

L'évaluateur a réalisé ses tests fonctionnels indépendants sur la plate-forme ST22L128-A rev L. identifiée au §1.1 et fournie au CESTI dans un mode dit « ouvert[1] ».

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

Classe ATE: Tests		**Verdicts**
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.2	Testing: low level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.6.7. L'évaluation des vulnérabilités

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

Seules les fonctions d'authentification en mode test et de génération de nombres aléatoires (avec une métrique spécifique) ont fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé élevé : élevé.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests sur la plate-forme ST22L128-A rev L. identifiée au §1.1 et fournie au CESTI dans un mode dit « ouvert[1] ».

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit utilisé avec les dernières versions des guides (cf. [GUIDES]) est donc résistant à des attaquants disposant d'un potentiel d'attaque **élevé** dans son environnement d'exploitation.

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

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_CCA.1	Covert Channel Analysis	Réussite
AVA_MSU.3	Analysis and testing for insecure state	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

2.6.8. L'analyse de la résistance des mécanismes cryptographiques

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

[1] mode permettant de charger et d'exécuter du code natif en EEPROM et de déconnecter les mécanismes sécuritaires paramétrables

3. La certification

3.1. Conclusions

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

3.2. Restrictions d'usage

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

Ce certificat donne une appréciation de la résistance du micro-circuit ST22L128-A rev. L à des attaques qui demeurent fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée qu'au travers de l'évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de cette évaluation.

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

- des procédures sécuritaires doivent être utilisées lors de la distribution du produit aux utilisateurs afin de maintenir la confidentialité et l'intégrité du produit et de ses données de fabrication et de test (pour prévenir toute copie, modification, conservation vol ou usage non autorisés).

Annexe 1. Visite du site de développement et fabrication de la société STMicroelectronics à Rousset

Le site de développement et de fabrication de la société STMicroelectronics situé dans la Z.I. de Peynier-Rousset, 13106 Rousset Cedex, France, a fait l'objet d'une visite par l'évaluateur le 3 et 4 février 2005 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le produit ST22L128-A rev L

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

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

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

Annexe 2. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 3. Références documentaires du produit évalué

[2003/18]	Rapport de certification 2003/18 - Micro-circuit ST19WK08C, Décembre 2003 SGDN/DCSSI
[CONF]	Liste de configuration du produit : • ST22L128-A - K640LMA OZV/XLG configuration list, Référence : PEN_ST22L_CFGL_04_002 v1.0 STMicroelectronics Liste des fournitures STMicroelectronics : • PHENIX – Documentation report, Référence : SMD_PHENIX_DR_04_001_V1.0 STMicroelectronics
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : • ST22L128-A - Data Sheet, Référence : DS_22L128-A/0501 v1 STMicroelectronics • ST22 - Hardware Sofware Interface - V3.0 - User Manual, Référence : UM_22_HSI_3-0/0410 VP1, STMicroelectronics • ST22 Security User Guide, Référence : SUG_22/0504V2 STMicroelectronics • ST22 - System ROM - Issuer Configuration – User Manual, Référence : UM_22_SR_I/0503 v3 STMicroelectronics • ST22 - STJ2 Core - Programming Manual, Référence ; PM_22_STJ2/0406 V2 STMicroelectronics, • ST22 Cryptographic library User manual, Référence : UM_22_CRYPTOLIB/0402 V3 STMicroelectronics,
[PP BSI]	Smartcard IC Platform Protection Profile, Référence : BSI-0002-2001, version 1.0, juillet 2002 Bundesamt für Sicherheit in der Informationstechnik (BSI)
[RTE]	Evaluation technical report of PHENIX project, Référence : PH_ETR version 1.0 CEACI
[ST]	PHENIX ST22L128-A security target, Référence : SCP_PHENIX_ST_03_001_V01.03 STMicroelectronics

[Visite]	ST22 project - Evaluation report - Classes ACM, ADO, ALC, Référence : ST22_ACM_ALC_ADO_v1.0 Serma Technologies

Annexe 4. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr