PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2005/10

Micro-circuit ST19XL18P

Paris, le 5 avril 2005

Le Directeur central de la sécurité des systèmes d'information

Henri Serres
[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 le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2005/10

Produit : Micro-circuit ST19XL18P

Développeur(s) : STMicroelectronics

Critères Communs version 2.1
(norme internationale ISO/IEC 15408:1999)

EAL4 Augmenté
(ADV_FSP.3, ADV_IMP.2, ALC_DVS.2, AVA_CCA.1, AVA_VLA.4)

conforme au profil de protection PP/9806

Commanditaire : STMicroelectronics

Centre d'évaluation : Serma Technologies

Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA :
ADV_IMP.2, ALC_DVS.2, AVA_VLA.4

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

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)
Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle 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] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.
[2] En novembre 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède et la Turquie.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est le micro-circuit ST19XL18 en version P (logiciel dédié XJD, maskset K5F0A). Le micro-circuit inclut une partie logicielle en ROM intégrant des logiciels de test du micro-circuit («autotest») et des bibliothèques (gestion du système, services cryptographiques).

1.2. Développeur

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

Le produit est développé en partie, intégré (préparation de la base de donnée du masque), et testé par :

STMicroelectronics

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

Une partie du développement du produit est réalisée par :

STMicroelectronics

28 Ang Mo Kio - Industrial park 2
SINGAPORE 569508
SINGAPOUR.

Les réticules du produit et le produit lui-même sont fabriqués par :

SMIC

18 Zhangjiang Road, PuDong New Area,
Shanghai Zip : 201203
China

1.3. Description du produit évalué

En termes de description technique, les fonctionnalités de sécurité du produit sont identiques à celles des versions précédemment certifiées (version N, certificat [2003/25] et version J, certificat [2002/22]). Seule une étape du développement a changé dans le cycle de vie puisque la fabrication des réticules et la fabrication du produit lui-même sont sous-traitées à la société SMIC en Chine.
Le périmètre d'évaluation est également identique à celui des versions précédentes (cf. [2002/22]).

2. L'évaluation

2.1. Contexte

Le produit évalué est une évolution du micro-circuit ST19XL18 en version N, certifié en 2003 sous la référence 2003/25 (cf. [2003/25]), lui-même étant une évolution du micro-circuit en version J, initialement évalué et certifié en 2002, sous la référence 2002/22 (cf. [2002/22]).
Dans le cadre d'une ré-évaluation, les travaux consistent à analyser l'impact des évolutions du produit, décrit dans un document du développeur (cf. [SIA]). A l'issue de cette analyse d'impact, le centre d'évaluation peut réaliser à nouveau certaines tâches d'évaluation relatives aux composants d'assurance pour lesquels les changements ont un impact majeur sur la sécurité.
Une partie des verdicts de la présente évaluation s'appuie donc sur les résultats des travaux menés lors des précédentes évaluations.

2.2. Référentiels d'évaluation

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

- RI008,
- RI032,
- RI043,
- RI049,
- RI084.

2.3. Commanditaire

STMicroelectronics

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

2.4. 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

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée de décembre 2004 à mars 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.

2.6. 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 PP/9806 (cf. [PP/9806]).

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	[2002/22]
ASE_ENV.1	Security environment	[2002/22]
ASE_INT.1	ST introduction	[2002/22]
ASE_OBJ.1	Security objectives	[2002/22]
ASE_PPC.1	PP claims	[2002/22]
ASE_REQ.1	IT security requirements	[2002/22]
ASE_SRE.1	Explicitly stated IT security requirements	[2002/22]
ASE_TSS.1	Security Target, TOE summary specification	[2002/22]

2.7. Evaluation du produit

2.7.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL4[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ ADV_FSP.3	Semiformal functional specification
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_CCA.1	Covert Channel Analysis
+ AVA_VLA.4	Highly resistant

2.7.2. L'évaluation de l'environnement de développement

Concernant la classe ALC, une étape du développement a changé dans le cycle de vie : les réticules et le produit lui-même sont désormais fabriqués par la société SMIC en Chine. De même, la liste de configuration du produit [LGC] a changé. En conséquence, la

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

documentation sécuritaire du fabriquant « SMIC » en Chine a fait l'objet d'une évaluation, et une visite sur site a été réalisée afin de vérifier l'application des procédures (cf. Annexe 1). Les tâches relatives à la classe ACM ont été partiellement réalisées pour vérifier la mise à jour de la liste de configuration [LGC].

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	[2002/22]
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	[2002/22]
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	[2002/22]
ALC_TAT.1	Well-defined development tools	[2002/22]

2.7.3. L'évaluation de la conception du produit

L'analyse de l'impact des évolutions sur la sécurité du micro-circuit ST19XL18P (cf. [RTE]) a permis de conclure qu'il n'y avait pas nécessité de réaliser de travaux pour la classe d'assurance ADV.

Pour mémoire, les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- Potential violation analysis (FAU_SAA.1)
- 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)
- Simple security attributes (FDP_IFF.1)
- Partial elimination of illicit information flows (FDP_IFF.4)
- Basic internal transfer protection (FDP_ITT.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- User attribute definition (FIA_ATD.1)
- TSF Generation of secrets (FIA_SOS.2)
- User authentication before any action (FIA_UAU.2)
- User Identification before any action (FIA_UID.2)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)

- TOE Security Functions testing (FPT_TST.1)

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.1	Informal TOE security policy model	[2002/22]
ADV_FSP.3	Semiformal functional specification	[2002/22]
ADV_HLD.2	Security enforcing high-level design	[2002/22]
ADV_LLD.1	Descriptive low-level design	[2002/22]
ADV_IMP.2	Implementation of the TSF	[2002/22]
ADV_RCR.1	Informal correspondence demonstration	[2002/22]

2.7.4. 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 de réticules,
- la livraison des réticules au fabricant du micro-circuit,
- la livraison des micro-circuits au responsable de l'étape suivante (mise en micro-module, encartage).

Or, une étape du développement a changé dans le cycle de vie : les réticules et le produit lui-même sont désormais fabriqués par la société SMIC en Chine.
Les procédures de livraison avec ce sous-traitant ont donc fait l'objet d'une évaluation et d'une visite sur site pour vérifier l'application des procédures (cf. Annexe 1).
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	[2002/22]

2.7.5. 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 l'évaluation du ST19XL18P, 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.

Dans le cadre de l'évaluation du ST19XL18P, les rôles sont définis différemment. Dans la cible de sécurité [ST, §5.3.1], les administrateurs sont définis comme étant :

- TEST administrator : il est chargé de tester le produit dans son environnement de développement et de changer la configuration du produit du mode « test » en mode « issuer » (et éventuellement en mode « user » si besoin est). Ce rôle est relatif à la phase 3 du cycle de vie ;
- ISSUER administrator : chargé de réaliser un nombre limité de tests du produit, de le personnaliser si besoin est et de changer la configuration du produit du mode « issuer » en mode « user ». Ce rôle peut intervenir à différentes phases du cycle de vie et peut être incarné par le développeur lui-même, le développeur du logiciel embarqué, le responsable de l'encartage ou tout autre responsable intervenant dans une phase ultérieure du cycle de vie. Ce rôle est relatif aux phases 3 à 6 du cycle de vie.

Les guides d'utilisation et d'administration [GUIDES] du produit ont été, en partie, mis à jour. Les travaux d'évaluation ont donc été réalisés, avec ré-utilisation de résultats, pour les guides n'ayant pas évolué.

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

2.7.6. L'évaluation des tests fonctionnels

L'analyse de l'impact des évolutions sur la sécurité du ST19XL18P (cf. [RTE]) a permis de conclure à la nécessité de réaliser partiellement les travaux associés à la classe d'assurance ATE : le développeur a réalisé les tests fonctionnels déjà menés sur la version précédente du produit. Le centre d'évaluation a vérifié que les résultats obtenus étaient conformes aux résultats attendus.

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	[2002/22]
ATE_DPT.1	Testing: high-level design	[2002/22]
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	[2002/22]

2.7.7. L'évaluation des vulnérabilités

L'analyse de l'impact des évolutions sur la sécurité du ST19XL18P (cf. [RTE]), ainsi que des travaux de caractérisation complémentaires ont permis de conclure que les changements intervenus sur le produit n'introduisent pas de nouvelles vulnérabilités. Par ailleurs, dans le cadre de la surveillance des micro-circuits certifiés de la famille ST19X, l'évaluateur met à jour régulièrement l'analyse de vulnérabilité du produit au vu de l'évolution de son environnement opérationnel. Le produit ST19XL18P 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	[2002/22]
AVA_MSU.2	Validation of analysis	[2002/22]
AVA_SOF.1	Strength of TOE security function evaluation	[2002/22]
AVA_VLA.4	Highly resistant	Réussite

2.7.8. L'analyse de la résistance des mécanismes cryptographiques

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

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 produit ST19XL18P 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].
Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST § 4.2] :

Objectifs de sécurité sur l'environnement concernant le système en phase d'utilisation

Ces objectifs de sécurité concernent le système dans lequel sera utilisé le micro-circuit avec son application embarquée (extraits de la cible de sécurité [ST § 4.2.6]) :

- la communication entre un produit développé sur le micro-circuit sécurisé et d'autres produits doit être sécurisée (en termes de protocole et de procédure) ;
- le système (terminal, communication,…) doit garantir la confidentialité et l'intégrité des données sensibles qu'il stocke ou qu'il traite.

3.3. Reconnaissance européenne (SOG-IS)

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

3.4. Reconnaissance internationale (CC RA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, les augmentations suivantes n'entrent pas dans le cadre de l'accord : ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4.

Annexe 1. Visite du site de fabrication de la société SMIC à Shanghai

Le site de fabrication de la société SMIC situé à l'adresse *18 Zhangjiang Road, PuDong New Area, Shanghai 201203* en Chine, a fait l'objet d'une visite par l'évaluateur les 7 et 8 mars 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 ST19XL18P.

Ces procédures avaient déjà été fournies et analysées lors de l'évaluation du micro-circuit ST19XL34P (cf. [2004/26bis]), et ont refait ici l'objet d'une vérification dans le cadre des tâches d'évaluation suivantes :

- 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

[2002/22]	Rapport de certification 2002/22 - Plate-forme ST19X Micro-circuit ST19XL18, Août 2002 SGDN/DCSSI
[2003/25]	Rapport de certification 2003/25 - Micro-circuit ST19XL18N, 8 janvier 2004 SGDN/DCSSI
[2004/26 bis]	Rapport de certification 2004/26 bis - Micro-circuit ST19XL34P, 20 août 2004 SGDN/DCSSI
[CONF]	Liste de configuration du produit : ▪ Liste de Configuration ST19XL18P (K5F0), Référence : PEN_19XL18_CFGL_05_001_V1.1 STMicroelectronics Liste des fournitures STMicroelectronics : ▪ GRENAT - Documentation report, Référence : SSE_GRENAT_DR_UK_02_001 v5.0 STMicroelectronics
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : ▪ ST19XL18 data sheet, Référence : DS_19XL18/0209V1.1 STMicroelectronics ▪ Manual for System ROM (Issuer configuration), Référence : UM_19XV2_SR_I/0204V1 STMicroelectronics ▪ Addendum to Manual for System ROM, Référence : AD_UM_19W_SR_I/0308V1.1 STMicroelectronics ▪ ST19X – 19W – System library User Manual Référence : UM_19X_19W_SYSLIB/0304V2.0 STMicroelectronics ▪ Enhanced DES Library User Manual Référence : UM_19XV2_EDESLIB/0203 V1.1 STMicroelectronics ▪ ST19X - Cryptographic Library LIB4 V2.0 - User Manual, Référence : UM_19X_LIB4V2/0503V3 STMicroelectronics

	▪ ST19X-19W - Security Application Manual, Référence : APM_19X-19W_SECU/0312 v1.7 STMicroelectronics ▪ ST19X-ST19W - Security Application Manual - Addendum-3 to V1.7, Référence : AD3_APM_19x-19W_SECU1.7_0411 V1.0 STMicroelectronics ▪ ST19X programming manual, Référence : PM_19X-19W/0210V2 STMicroelectronics
[PP9806]	Common Criteria for Information Technology Security Evaluation - Protection Profile : Smart Card Integrated Circuit Version 2.0, Issue September 1998. Certifié par le centre de certification français sous la référence 9806. *Document publié sur le site : www.ssi.gouv.fr*
[RTE]	Evaluation Technical Report - ST19XL18P, Référence : GRENAT_ETR_XL18P v1.1 Serma Technologies Pour le besoin des évaluations en composition, une version diffusable du document a été validée : ETR-lite for composition - ST19XL18P - (EAL4+ evaluation), Référence : GRENAT_ ETRLite_XL18Pv1.0 Serma Technologies
[SIA]	Impact Analysis for ST19XL18P, Référence : SMD_ST19XL18_SIA_05_001_V1.0 STMicroelectronics
[ST]	▪ ST19X GENERIC SECURITY TARGET, Référence : STM_ST_ST19X0104_003 v1.3 STMicroelectronics ▪ ST19XL18 - Security Target Lite, Référence : FNT_GRENAT_ST_02_005_V01.10, STMicroelectronics Pour les besoins de la reconnaissance internationale, le cible suivante a été fournie et validée dans le cadre de cette évaluation : ▪ ST19XL18 Security Target, Référence : SMD_ST19XL18_ST_04_001_V1.00 STMicroelectronics
[Visite]	Annexe B du [RTE]

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, August 1999, version 2.1, ref CCIMB-99-031 ; Part 2: Security functional requirements, August 1999, version 2.1, ref CCIMB-99-032 ; Part 3: Security assurance requirements, August 1999, version 2.1, réf: CCIMB-99-033. Le contenu des Critères Communs version 2.1 est identique à celui de la Norme Internationale ISO/IEC 15408:1999, comportant les trois documents suivants: ISO/IEC 15408-1: Part 1 Introduction and general model ; ISO/IEC 15408–2: Part 2 Security functional requirements ; ISO/IEC 15408–3: Part 3 Security assurance requirements.
[CEM]	Common Methodology for Information Technology Security Evaluation : Part 2: Evaluation Methodology, August 1999, version 1.0, ref CEM- 99/045.
[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