PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2004/18 bis

Micro-circuit ST19WL66B

Paris, le 20 août 2004

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.
Toutefois, 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.

Table des matières

1. LE PRODUIT EVALUE 6

1.1. REMARQUES PRELIMINAIRE 6
1.2. CONTEXTE 6
1.3. IDENTIFICATION DU PRODUIT 6
1.4. LE DEVELOPPEUR 6
1.5. DESCRIPTION DU PRODUIT EVALUE 7
1.5.1. Architecture 7
1.5.2. Cycle de vie 8
1.5.3. Périmètre et limites du produit évalué 8
1.6. UTILISATION ET ADMINISTRATION 8
1.6.1. Utilisation 8
1.6.2. Administration 9

2. L'EVALUATION 10

2.1. CENTRE D'EVALUATION 10
2.2. COMMANDITAIRE 10
2.3. REFERENTIELS D'EVALUATION 10
2.4. EVALUATION DE LA CIBLE DE SECURITE 10
2.5. EVALUATION DU PRODUIT 10
2.5.1. Développement du produit 10
2.5.2. Documentation 11
2.5.3. Livraison et installation 11
2.5.4. L'environnement de développement 11
2.5.5. Tests fonctionnels 12
2.5.6. Estimation des vulnérabilités 12

3. CONCLUSIONS DE L'EVALUATION 13

3.1. RAPPORT TECHNIQUE D'EVALUATION 13
3.2. NIVEAU D'EVALUATION 13
3.3. EXIGENCES FONCTIONNELLES 14
3.4. RESISTANCE DES FONCTIONS 15
3.5. ANALYSE DES MECANISMES CRYPTOGRAPHIQUES 15
3.6. CONFORMITE A UN PROFIL DE PROTECTION 15
3.7. RECONNAISSANCE EUROPEENNE (SOG-IS) 15
3.8. RECONNAISSANCE INTERNATIONALE (CC RA) 15
3.9. RESTRICTIONS D'USAGE 16
3.10. OBJECTIFS DE SECURITE SUR L'ENVIRONNEMENT 16
3.11. SYNTHESE DES RESULTATS 16

ANNEXE 1. RAPPORT DE VISITE DE SITE 17

ANNEXE 2. ANALYSE DES MECANISMES CRYPTOGRAPHIQUES 18

ANNEXE 3. EXIGENCES FONCTIONNELLES DE SECURITE DU PRODUIT EVALUE .. 19

ANNEXE 4. NIVEAUX D'ASSURANCE PREDEFINIS IS 15408 OU CC 22

ANNEXE 5. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 23

ANNEXE 6. REFERENCES LIEES A LA CERTIFICATION 25

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

[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.

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. Le produit évalué

1.1. Remarques préliminaires

Ce rapport de certification « 2004/18 bis » est similaire au rapport « 2004/18 ». Il intègre cependant la référence de la cible de sécurité qui permet la reconnaissance internationale (cf. [CC RA]). La préface a également été mise à jour en conséquence et les paragraphes §3.7, §3.8 ont été ajoutés.

1.2. Contexte

Les micro-circuits de la plate-forme ST19W sont dérivés directement des micro-circuits déjà certifiés de la plate-forme ST19X : ils présentent les mêmes fonctions de sécurité et politiques de sécurité que les circuits de la plate forme ST19X ; ils sont néanmoins fabriqués avec une nouvelle technologie.
De plus, le micro-circuit ST19WK08 représentatif de la plate-forme ST19W a déjà été évalué et certifié (cf. [2003/18]). Les résultats de cette évaluation ont donc été ré-utilisés dans le cadre de l'évaluation du micro-circuit ST19WL66.

1.3. Identification du produit

Le produit évalué est le micro-circuit ST19WL66 en version B. Le micro-circuit inclut une partie logicielle en ROM intégrant des logiciels de tests du micro-circuit («autotest») et des librairies (gestion du système, services cryptographiques). La version du micro-circuit intégrant ce logiciel évalué est le ST19WL66B (logiciel dédié XWB, maskset K730BCA).

1.4. Le développeur

Plusieurs acteurs interviennent dans la conception et fabrication du micro-circuit (cf. description du cycle de vie §1.5.2) :

Le produit est développé en partie, intégré (préparation de la base de données du masque), fabriqué 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 micro-circuit sont fabriqués par :

DAI NIPPON PRINTING CO., LTD

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

1.5. Description du produit évalué

Le produit évalué est le micro-circuit ST19WL66B de la famille ST19W développé et fabriqué 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 pour constituer une carte à puce. Les usages possibles de cette carte 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.

1.5.1. Architecture

Le micro-circuit ST19WL66B est constitué des éléments suivants :

- une partie matérielle :
  - un processeur 8-bit ;
  - des mémoires : 32KB de mémoire ROM pour le stockage des logiciels dédiés (logiciel de test et librairie cryptographique), 224KB de ROM pour le stockage des programmes utilisateurs, 66KB de mémoire EEPROM (high density) pour le stockage des programmes et des données et 6KB de mémoire SRAM ;
  - des modules de sécurité : contrôle logique d'accès aux mémoires (MACL), générateur d'horloge, contrôle de la sécurité, gestion de l'alimentation, contrôle d'intégrité des mémoires, gestion des entrées/sorties en mode contact (ISO 7816), deux générateurs d'aléas, co-processeur DES (implémentation E-DES) et RSA.
- une partie logicielle en ROM intégrant des logiciels de tests du micro-circuit («autotest»), des librairies (gestion du système, services cryptographiques). La version du micro-circuit intégrant ce logiciel évalué est identifiée au §1.3.

Une description détaillée de l'architecture du produit se trouve dans le document [HLD].

1.5.2. Cycle de vie

Le cycle de vie du produit inspiré du cycle de vie décrit dans le PP/9806 [PP9806] est le suivant :

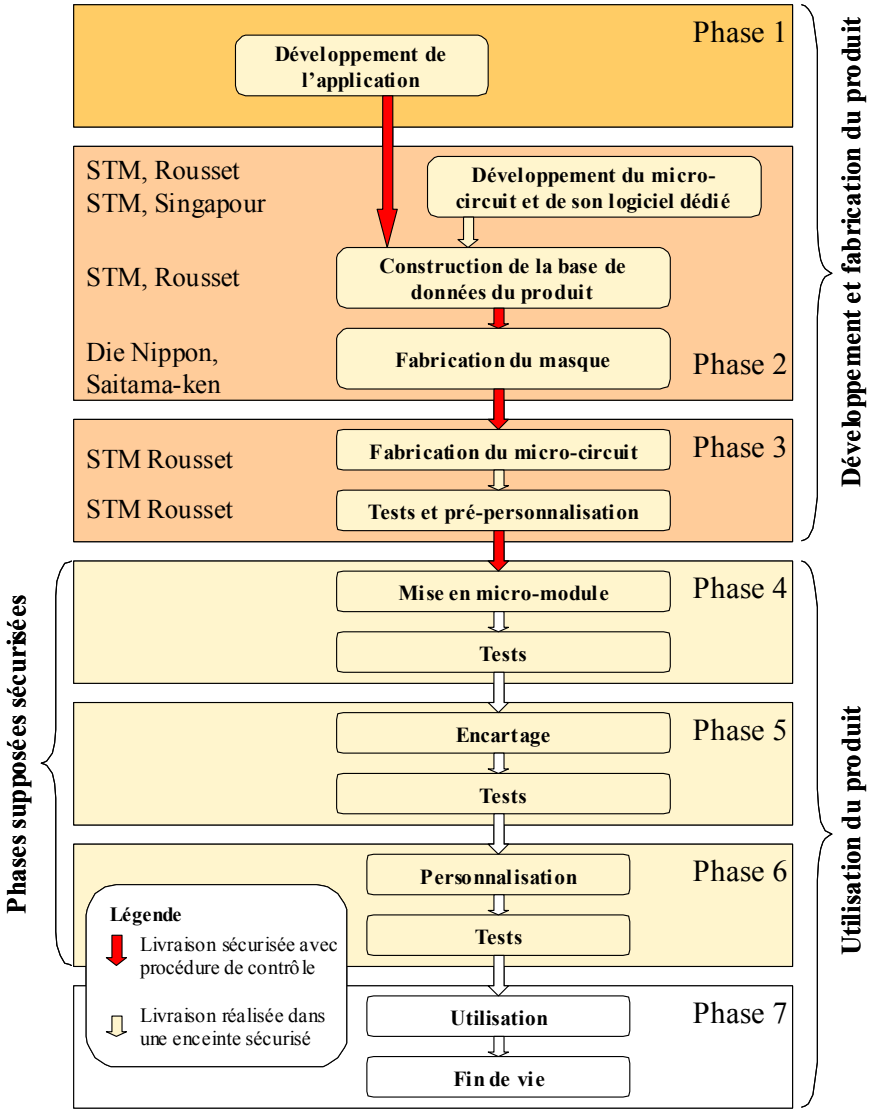

Figure 1 - Cycle de vie standard d'une carte à puce

1.5.3. 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 §1.3 et décrit au §1.5.1. Toute autre application éventuellement embarquée notamment les applications 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).

1.6. Utilisation et administration

1.6.1. Utilisation

Le produit évalué n'est pas un produit mettant 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 (phase 4 à 6) qui interviendront notamment dans la configuration et la personnalisation des applications embarquées.

Dans le cadre de l'évaluation du ST19WL66B, 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.

Les objectifs de sécurité sur l'environnement de développement et d'exploitation relatifs aux utilisateurs sont listés dans la cible de sécurité [ST] et repris dans le présent rapport au paragraphe 3.10.

1.6.2. 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 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 ST19WL66B, les rôles sont définis légèrement 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 (cf. §1.5.2) ;
- ISSUER administrators : 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 objectifs de sécurité sur l'environnement de développement et d'exploitation relatifs aux administrateurs sont listés dans la cible de sécurité [ST] et repris dans le présent rapport au paragraphe 3.10.

2. L'évaluation

2.1. 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

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

2.2. Commanditaire

STMicroelectronics

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

2.3. 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 à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation respectent les exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].

2.5.1. Développement du produit

Le micro-circuit ST19WL66B étant très similaire au ST19WK08C déjà évalué et certifié (cf. [2003/18]), les résultats d'évaluations du ST19WK08C ont été ré-utilisés en partie. Seul le niveau de la représentation de l'implémentation a été de nouveau intégralement évalué.

Les documents fournis pour la classe ADV – développement – répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.2. Documentation

Du point de vue de l'évaluation, les administrateurs sont les responsables de la réalisation des tests du produit lorsqu'il est en mode « test » et les responsables des tests et personnalisation du produit lorsqu'il est en mode « issuer » (cf. §1.6.2).
Du point de vue de l'évaluation, les utilisateurs sont les personnes pouvant mettre en œuvre les fonctionnalités « utilisateurs » du produit (notamment le développeur du logiciel embarqué, cf. §1.6.1).
Le micro-circuit ST19WL66B étant très similaire au ST19WK08C déjà évalué et certifié (cf. [2003/18]), les résultats de l'évaluation précédente ont été ré-utilisés en partie.
Les guides utilisateur et administrateur [USR] répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.3. Livraison et 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).

Les différents sites impliqués sont identifiés au §1.4 du présent rapport. Tous les flux relatifs à l'ensemble des sites sont évalués et audités régulièrement dans le cadre des différentes évaluations et ré-évaluation des produits de STMicroelectronics (voir notamment le rapport de certification [2003/18]). Les conclusions des travaux associés sont satisfaisantes. Ces flux n'ont donc pas fait l'objet d'une évaluation pour ce projet.
Les procédures [DEL] de livraison sont donc suffisantes pour répondre aux exigences : elles permettent de connaître l'origine de la livraison et de détecter une modification des informations échangées pendant leur livraison.
Le produit évalué ne comportant pas d'application embarquée spécifique, il ne nécessite pas de phase d'installation, génération et démarrage spécifique.
Les documents fournis pour la classe ADO – livraison et opération – répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.4. L'environnement de développement

Le développement du micro-circuit implique l'ensemble des sites identifiés au §1.4.
Les environnements de développement des sites impliqués sont évalués et audités dans le cadre des différentes évaluations et ré-évaluation des produits de STMicroelectronics (voir notamment le rapport de certification [2003/18]). Les conclusions des travaux associés sont satisfaisantes. Les environnements de développement liés à ces sites n'ont donc pas fait l'objet d'une évaluation particulière au sein de ce projet.
Les tâches relatives à la classe ACM ont été partiellement réalisées, notamment pour vérifier la mise à jour de la liste de configuration [LGC].

Les documents fournis pour la classe ACM – gestion de la configuration – et ALC – support au cycle de vie – répondent aux exigences de la partie 3 des critères communs [CC] en termes de contenu et de présentation des éléments de preuve.

2.5.5. Tests fonctionnels

Le micro-circuit ST19WL66B étant très similaire au ST19WK08C déjà évalué et certifié (cf. [2003/18]), les résultats de l'évaluation précédente ont été ré-utilisés en partie, pour la partie documentaire. Les tests indépendants ont néanmoins été menés à nouveau sur la plate-forme ST19WL66B identifiée au §1.3 du présent rapport.

2.5.6. Estimation des vulnérabilités

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement prises en compte dans la conception du produit.
L'évaluateur a également réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré.
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élevé**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du micro-circuit ST19WL66B. Une grande partie des résultats de l'évaluation du micro-circuit ST19WK08C ont été ré-utilisés. Ils sont décrits dans le rapport technique d'évaluation associé [RTE_WK08].

3.2. Niveau d'évaluation

Le micro-circuit ST19WL66B a été évalué selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL4**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
ADV_FSP.3	Semiformal functional specification
ALC_DVS.2	Sufficiency of security measures
ALC_FLR.1	Basic Flaw Remediation
AVA_VLA.4	Highly resistant
AVA_CCA.1	Covert Channel Analysis
AVA_MSU.3	Analysis and testing for insecure states

Tableau 1 - Augmentations

Pour tous les composants, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
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
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	[2003/18]
ACM_CAP.4	Generation support and acceptance	Réussite

[1] Annexe 4 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

	procedures	
ACM_SCP.2	Problem tracking CM coverage	[2003/18]
Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	[2003/18]
ADO_IGS.1	Installation, generation, and start-up procedures	[2003/18]
Class ADV	**Development**	
ADV_FSP.3	Semiformal functional specification	[2003/18]
ADV_HLD.2	Security enforcing high-level design	[2003/18]
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
ADV_SPM.1	Informal TOE security policy model	[2003/18]
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
Class ALC	**Life cycle support**	
ALC_DVS.2	Sufficiency of security measures	[2003/18]
ALC_FLR.1	Basic Flaw Remediation	[2003/18]
ALC_LCD.1	Developer defined life-cycle model	[2003/18]
ALC_TAT.1	Well-defined development tools	[2003/18]
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_CCA.1	Covert Channel Analysis	[2003/18]
AVA_MSU.3	Analysis and testing for insecure states	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	[2003/18]
AVA_VLA.4	Highly resistant	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** suivantes[1]. Les opérations sur ces exigences sont décrites dans la cible de sécurité [ST chapitre 5].

- Potential violation analysis (FAU_SAA.1)
- Cryptographic Key Generation (FCS_CKM.1)
- Cryptographic operation (FCS_COP.1)

[1] Annexe 3 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- 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)

3.4. Résistance des fonctions

Les fonctions suivantes ont fait l'objet d'une estimation du niveau de résistance :

- authentification de l'administrateur en mode « test » et « issuer »,
- génération de nombres aléatoires (avec une métrique spécifique).

Le niveau de résistance des fonctions de sécurité est jugé **élevé** (**SOF-High**).

3.5. Analyse des mécanismes cryptographiques

Aucun mécanisme cryptographique n'a été coté dans le cadre de l'évaluation (cf Annexe 2).

3.6. Conformité à un profil de protection

Le produit répond aux exigences de sécurité du profil de protection PP/9806 [PP/9806].

3.7. Reconnaissance européenne (SOG-IS)

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

3.8. Reconnaissance internationale (CC RA)

Ce certificat a été 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, ADV_FSP.3, ALC_DVS.2, AVA_VLA.4, AVA_CCA.1 et AVA_MSU.3 (Tableau 1).

3.9. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.10) ainsi que les recommandations se trouvant dans les guides utilisateur [USR].
Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

3.10. Objectifs de sécurité sur l'environnement

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'autre produit doit être sécurisée (en terme 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.

3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que le micro-circuit ST19WL66B identifié au paragraphe 1.3 et décrit au paragraphe 1.5 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Rapport de visite de site

Aucune visite de site spécifique n'a été réalisée dans le cadre de l'évaluation de ce produit.

Annexe 2. Analyse des mécanismes cryptographiques

Aucun mécanisme cryptographique spécifique n'a été coté dans le cadre de l'évaluation de ce produit.

Annexe 3. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont données à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles du produit.

Class FAU	**Security audit**
Security audit analysis	
FAU_SAA.1	*Potential violation analysis* Le produit doit implémenter un seuil de détection élémentaire, défini selon une règle fixée (spécifiée dans la cible de sécurité [ST]).
Class FCS	**Cryptographic support**
Cryptographic key management	
FCS_CKM.1	*Cryptographic key generation* Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiées qui peuvent être basées sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Information flow control policy	
FDP_IFC.1	*Subset information flow control* Le produit doit appliquer les politiques de sécurité de contrôle de flux d'information, lesquelles sont spécifiées dans la cible de sécurité [ST] pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'informations.
Information flow control functions	
FDP_IFF.1	*Simple security attributes* Ce composant impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la

	fonction et décrit comment les attributs de sécurité sont choisis par la fonction.
FDP_IFF.4	*Partial elimination of illicit information flows* Le produit doit couvrir l'élimination de certains flux d'information illicites (mais pas nécessairement de tous).
Internal TOE transfer	
FDP_ITT.1	*Basic internal transfer protection* Les données de l'utilisateur doivent être protégées lorsqu'elles sont transmises entre différentes parties du produit.
Residual information protection	
FDP_RIP.1	*Subset residual information protection* Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets lors de l'allocation ou de la désallocation de la ressource.
Stored data integrity	
FDP_SDI.1	*Stored data integrity monitoring* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées.
FDP_SDI.2	*Stored data integrity monitoring and action* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées et entreprendre des actions (spécifiées dans la cible de sécurité [ST]) suite à une détection d'erreur.
Class FIA	**Identification and authentication**
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
Specification of secrets	
FIA_SOS.2	*TSF Generation of secrets* Le produit doit être capable de générer des secrets qui répondent à des métriques de qualité définies.
User authentication	
FIA_UAU.2	*User authentication before any action* Les utilisateurs doivent s'authentifier avant que toute action ne soit autorisée.
User identification	
FIA_UID.2	*User identification before any action* Les utilisateurs doivent s'identifier avant que toute action ne soit autorisée.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiés dans la cible de sécurité [ST]).

Class FPR	**Privacy**
Unobservability	
FPR_UNO.1	*Unobservability* Le produit n'autorise pas certains utilisateurs (spécifiés dans la cible de sécurité [ST]) à déterminer si certaines opérations (spécifiées dans la cible de sécurité [ST]) sont en cours d'exécution.
Class FPT	**Protection of the TSF**
TSF physical protection	
FPT_PHP.2	*Notification of physical attack* Le produit doit notifier automatiquement l'intrusion physique sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
FPT_PHP.3	*Resistance to physical attack* Le produit doit empêcher ou résister à certaines intrusions physiques (spécifiées dans la cible de sécurité [ST]) sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.

Annexe 4. Niveaux d'assurance prédéfinis IS 15408 ou CC

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 5. Références documentaires du produit évalué

[2003/18]	Rapport de certification 2003/18 - Micro-circuit ST19WK08C, Décembre 2003 SGDN/DCSSI
[DEL]	LIVRAISON DE PRODUITS SMARTCARD A UN CLIENT ET RECEPTION DES RETOURS CLIENTS Référence : 7147367, revision B STMicroelectronics
[HLD]	▪ ST19W Generic High Level Design Référence : PDE_YQUEM_TS_03_001 v1.2 STMicroelectronics ▪ ST19W Generic High Level Design – Annexe B Référence : PDE_YQUEM_TS_03_004, v1.1 STMicroelectronics
[LGC]	Liste de configuration du produit : ▪ Configuration list for ST19WL66 product - K730BCA Mask Set Référence : PEN_YQUEM_CFGL_04_001 v1.1 STMicroelectronics Liste des fournitures STMicroelectronics : ▪ YQUEM evaluation – Documentation report (ST19WL66 and ST19WS04) Référence : SMD_YQUEM_DR_04_001 v1.1 ST Microelectronics
[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 - ST19WL66B (EAL4+ evaluation) Référence : YQM_WL66B_ETR v1.1 Pour le besoin des évaluations en composition, une version diffusable du document a été validée : ETR-lite for composition - ST19WL66B (EAL4+ evaluation) Référence : YQM_WL66B_ETR_lite v1.0
[RTE_WK08]	ST19WK08 Evaluation Technical Report (EAL4+ evaluation) Référence : YQM_WK08_ETR v1.2 Serma Technologies

[ST]	▪ ST19W Generic Security Target Référence : SCP_YQUEM_ST_03_001_V01.01 STMicroelectronics ▪ ST19WL66 Security Target Lite Référence : SMD_YQUEM_ST_04_002_V01.02 STMicroelectronics Pour les besoins de la reconnaissance internationale, le cible suivante a été fournie et validée dans le cadre de cette évaluation : ▪ ST19WL66 - Security Target, Référence : SMD_ST19WL66_ST_04_001 v1.00 STMicroelectronics
[USR]	Les guides d'utilisation du produit sont constitués des documents suivants : ▪ ST19WLxx - Datasheet Référence : DS_19WLxx/0301VP1 STMicroelectronics ▪ Manuals of security recommendations v1.7 Référence : APM_19X-19W_SECU/0312V1.7 STMicroelectronics ▪ ST19W - System ROM –Issuer configuration - user manual Référence : UM_19W_SR_I/0306VP2 STMicroelectronics ▪ Addendum au ST19W - System ROM –Issuer configuration - user manual Référence : AD_UM_19W_SR_I/0308V1.1 STMicroelectronics ▪ ST19X – 19W – System library User Manual Référence : UM_19X_19W_SYSLIB/0304V2 STMicroelectronics ▪ ST19X – Enhanced DES Library User Manual Référence : UM_19XV2_EDESLIB/0203V1.1 STMicroelectronics ▪ ST19X – User Manual – Cryptographic library lib4 v2.0 Référence : UM_19X_LIB4V2/0301V1.1 STMicroelectronics ▪ Card Manager Manuel Référence : UM_19X_19W_MG/0401 v3 STMicroelectronics

Annexe 6. 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.	
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ 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.
[CC_AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002
[CC_IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, Version 1.2, July 2000
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[IS 15408]	Norme Internationale ISO/IEC 15408:1999, comportant 3 documents : ▪ 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 ;
[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