



*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 2006/18**

### **Microcontrôleur sécurisé ST19WR66I**

*Paris, le 7 novembre 2006*

*Le Directeur central de la sécurité des  
systèmes d'information*

Patrick Pailloux  
[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 présumées 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 2006/18**

## Microcontrôleur sécurisé ST19WR66I

Développeur : STMicroelectronics

**Critères Communs version 2.2**

**EAL5 Augmenté**  
(ALC\_DVS.2, AVA\_MSU.3, AVA\_VLA.4)

conforme aux profils de protection PP/9806 et BSI-PP-002-2001

Commanditaire : STMicroelectronics

Centre d'évaluation : Serma Technologies



Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA :  
ACM\_SCP.3, ADV\_FSP.3, ADV\_HLD.3, ADV\_IMP.2, ADV\_INT.1, ADV\_RCR.2, ADV\_SPM.3, ALC\_DVS.2, ALC\_LCD.2,  
ALC\_TAT.2, ATE\_DPT.2, AVA\_CCA.1, AVA\_MSU.3, 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](http://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<sup>1</sup>, 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<sup>2</sup>, 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 :



---

<sup>1</sup> 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.

<sup>2</sup> En septembre 2006, 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, le Japon, la Norvège, les Pays-Bas, la Corée du Sud et l'Espagne ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Suède, la Turquie, la République Tchèque, Singapour, l'Inde et le Danemark.

# Table des matières

<b>1. LE PRODUIT EVALUE.....</b>	<b>6</b>
1.1. IDENTIFICATION DU PRODUIT.....	6
1.2. DEVELOPPEUR.....	6
1.3. DESCRIPTION DU PRODUIT EVALUE .....	6
1.3.1. <i>Architecture</i> .....	7
1.3.2. <i>Cycle de vie</i> .....	7
1.3.3. <i>Périmètre et limites du produit évalué</i> .....	8
<b>2. L'EVALUATION.....</b>	<b>9</b>
2.1. CONTEXTE.....	9
2.2. REFERENTIELS D'EVALUATION.....	9
2.3. COMMANDITAIRE.....	9
2.4. CENTRE D'EVALUATION.....	9
2.5. RAPPORT TECHNIQUE D'EVALUATION.....	9
2.6. EVALUATION DE LA CIBLE DE SECURITE.....	10
2.7. EVALUATION DU PRODUIT .....	10
2.7.1. <i>Les tâches d'évaluation</i> .....	10
2.7.2. <i>L'évaluation de l'environnement de développement</i> .....	10
2.7.3. <i>L'évaluation de la conception du produit</i> .....	11
2.7.4. <i>L'évaluation des procédures de livraison et d'installation</i> .....	12
2.7.5. <i>L'évaluation de la documentation d'exploitation</i> .....	13
2.7.6. <i>L'évaluation des tests fonctionnels</i> .....	14
2.7.7. <i>L'évaluation des vulnérabilités</i> .....	14
2.7.8. <i>L'analyse de la résistance des mécanismes cryptographiques</i> .....	15
2.7.9. <i>L'analyse du générateur d'aléas</i> .....	15
<b>3. LA CERTIFICATION.....</b>	<b>16</b>
3.1. CONCLUSIONS.....	16
3.2. RESTRICTIONS D'USAGE.....	16
3.3. RECONNAISSANCE EUROPEENNE (SOG-IS).....	16
3.4. RECONNAISSANCE INTERNATIONALE (CC RA).....	16
<b>ANNEXE 1. NIVEAUX D'ASSURANCE PREDEFINIS EAL.....</b>	<b>18</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE.....</b>	<b>19</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION.....</b>	<b>22</b>

# 1. Le produit évalué

## 1.1. Identification du produit

Le produit évalué est le microcontrôleur sécurisé ST19WR66 en révision I. Le microcontrôleur inclut une partie logicielle en ROM intégrant des logiciels de tests du microcontrôleur («autotest») et des bibliothèques (gestion du système, services cryptographiques). La version du microcontrôleur intégrant ce logiciel évalué est le ST19WR66I (logiciel dédié ZIC, maskset K7E0IIA).

## 1.2. Développeur

Plusieurs acteurs interviennent dans la conception et la fabrication du microcontrôleur. 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

Une partie du développement du produit est réalisée par :

### **STMicroelectronics**

28 Ang Mo Kio - Industrial park 2  
Singapore 569508  
Singapour

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 microcontrôleur ST19WR66I de la famille ST19W développé et fabriqué par STMicroelectronics.

Le produit a trois configurations d'utilisation :

- configuration «Test» : à la fin de sa fabrication, le microcontrôleur 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 configuration «Issuer» ;

- configuration «Issuer» : mode utilisé lors des phases d'encartage et de personnalisation du microcontrôleur. Certains tests internes du microcontrôleur sont encore disponibles. Les données de personnalisation peuvent être chargées en EEPROM. Ce mode est ensuite bloqué de manière irréversible lors du passage en configuration «User» ;
- configuration «User» : mode final d'utilisation du microcontrôleur qui fonctionne alors sous le contrôle du logiciel embarqué de la carte à puce. Le logiciel de test n'est plus accessible. Les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans cette configuration.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé,...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

### ***1.3.1. Architecture***

Le microcontrôleur ST19WR66I est constitué des éléments suivants :

- une partie matérielle composée :
  - o d'un processeur 8-bits ;
  - o de mémoires : 66KB de mémoire EEPROM (avec contrôle d'intégrité) pour le stockage des programmes et des données, 224KB de mémoire ROM pour le stockage des programmes utilisateurs, 6KB de mémoire RAM et 32KB de mémoire ROM pour le stockage des logiciels dédiés (logiciel de test et bibliothèque cryptographique) ;
  - o de 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 ;
  - o de modules fonctionnels : compteurs 8-bits, gestion des entrées/sorties en mode contact (IART ISO 7816-3) et sans contact (RFUART ISO 14443-B), générateurs de nombres aléatoires (TRNG), co-processeurs DES et RSA.
- une partie logiciels dédiés en ROM intégrant :
  - o des logiciels de tests du microcontrôleur («autotest») ;
  - o des utilitaires pour la gestion du système et de l'interface hardware/software, et la gestion de l'interface ISO 14443-B ;
  - o des services cryptographiques DES (implémentation E-DES), AES et RSA inclus dans la cible de sécurité du produit.

### ***1.3.2. Cycle de vie***

Le cycle de vie du produit est le suivant :

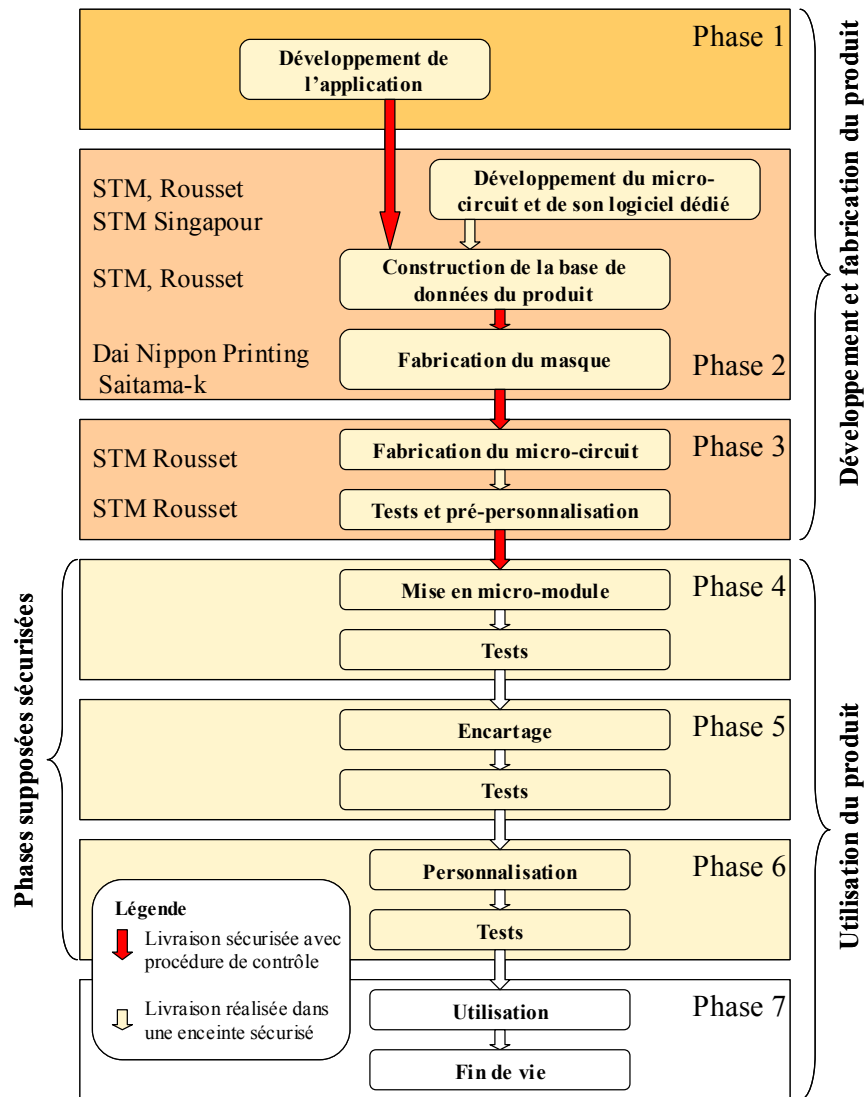


Figure 1 - Cycle de vie standard d'une carte à puce

### 1.3.3. Périmètre et limites du produit évalué

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur et aux logiciels dédiés identifiés au §1.1 et décrits au §1.3. Toute autre application éventuellement embarquée, 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. Contexte

Le produit ST19WR66I a déjà certifié en 2006 sous la référence 2006/12 (cf. [2006/12]). Quelques travaux complémentaires ont été menés sur le générateur de nombres aléatoires afin de vérifier sa conformité aux critères de la méthodologie d'évaluation allemande AIS31 (cf. [AIS31]). Les verdicts associés à l'ensemble des autres travaux ont été réutilisés.

### 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].

Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au CESTI, validées par la DCSSI et compatibles avec le document [AIS34] ont été utilisées.

### 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](mailto:m.dus@serma.com)

### 2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée d'avril à septembre 2006.

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 aux profils de protection [PP9806] et [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

## 2.7. Evaluation du produit

### 2.7.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL5<sup>1</sup> augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
<b>EAL5</b>	Semiformally designed and tested
+ <b>ALC_DVS.2</b>	Sufficiency of security measures
+ <b>AVA_MSU.3</b>	Analysis and testing for insecure state
+ <b>AVA_VLA.4</b>	Highly resistant

### 2.7.2. L'évaluation de l'environnement de développement

Le produit est développé sur les sites identifiés au §1.2 (Rousset en France, Singapour, 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.

<sup>1</sup> Annexe 1 : 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<sup>1</sup>. 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 est effectuée régulièrement dans le cadre des différentes évaluations et réévaluations de produit STMicroelectronics. Aucun audit particulier n'a été planifié dans le cadre de cette réévaluation.

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

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

### 2.7.3. 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 :

- 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)
- Basic internal transfer protection (FDP\_ITT.1)
- Subset residual information protection (FDP\_RIP.1)

<sup>1</sup> 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).

- Stored data integrity monitoring and action (FDP\_SDI.1)
- Stored data integrity monitoring and action (FDP\_SDI.2)
- User attribute definition (FIA\_ATD.1)
- 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)
- Specification of management functions (FMT\_SMF.1)
- Security management roles (FMT\_SMR.1)
- Unobservability (FPR\_UNO.1)
- Failure with preservation of secure state (FPT\_FLS.1)
- Basic TSF data internal protection (FPT\_ITT.1)
- Notification of physical attack (FPT\_PHP.2)
- Resistance to physical attack (FPT\_PHP.3)
- TSF domain separation (FPT\_SEP.1)
- TSF testing (FPT\_TST.1)
- 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

#### 2.7.4. L'évaluation des procédures de livraison et d'installation

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

- la livraison du code des applications embarquées au fabricant du microcontrôleur ;
- la livraison des informations nécessaires au fabricant du masque ;
- la livraison du masque au fabricant du microcontrôleur ;
- la livraison des microcontrôleurs 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 microcontrôleur 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

### 2.7.5. 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 microcontrôleur 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] : les utilisateurs sont définis comme étant les personnes pouvant mettre en œuvre les fonctionnalités du microcontrôleur, sa bibliothèque logicielle et 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 chargée 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 microcontrôleur, seules les interfaces d'administration propres au microcontrôleur 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

### 2.7.6. 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 ST19WR66 en révision I identifiée au §1.1 et fournie au CESTI dans un mode dit « ouvert<sup>1</sup> ».

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

### 2.7.7. 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 configuration test et de génération de nombres aléatoires (avec une métrique inspirée de l'[AIS31] et de la [FIPS 140-2]) ont fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé élevé :

- SOF-high pour la fonction d'authentification en configuration test ;
- Classe « P2 – high » selon l'[AIS31] et « Level 3<sup>2</sup> » selon la [FIPS 140-2] pour la génération de nombres aléatoires.

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 le microcontrôleur ST19WR66I identifiée au §1.1 et fournie au CESTI dans un mode dit « ouvert<sup>1</sup> ».

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de niveau **élevé**.

Cette cotation est réalisée conformément au guide « Application of attack potential to smart-card » (cf. [CC AP]).

<sup>1</sup> Mode permettant de charger et d'exécuter du code natif en EEPROM et de déconnecter les mécanismes sécuritaires paramétrables.

<sup>2</sup> Seul le sous-ensemble de la [FIPS 140-2] relatif aux générateurs de nombres aléatoires a été évalué et uniquement au travers des tests statistiques spécifiés dans le standard.

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

<b>Classe AVA : Estimation des vulnérabilités</b>		<b>Verdicts</b>
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

### ***2.7.8. L'analyse de la résistance des mécanismes cryptographiques***

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

### ***2.7.9. L'analyse du générateur d'aléas***

Le produit évalué offre deux générateurs d'aléas qui peut être utilisé par le logiciel embarqué. Ces générateur ont fait l'objet d'une analyse par la DCSSI.

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquant pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [CRYPTO], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléa n'a pas révélé de faiblesse.

## 3. La certification

### 3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et 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 microcontrôleur sécurisé ST19WR66I 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 microcontrôleur 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) ;
- la communication entre un produit développé sur le microcontrôleur 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 : ACM\_SCP.3, ADV\_FSP.3,



ADV\_HLD.3, ADV\_IMP.2, ADV\_INT.1, ADV\_RCR.2, ADV\_SPM.3, ALC\_DVS.2,  
ALC\_LCD.2, ALC\_TAT.2, ATE\_DPT.2, AVA\_CCA.1, AVA\_MSU.3, AVA\_VLA.4.



## Annexe 1. 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 2. Références documentaires du produit évalué

[2006/12]	Rapport de certification 2006/12 - Microcontrôleur sécurisé ST19WR66I, 19 juillet 2006 SGDN/DCSSI
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>• Configuration List ST19WR66I - PRODUCT - K7E4A MASK SET, Référence : SCP_K7E0_YQUEM_CFGL_06_001 V01.01 STMicroelectronics</li> </ul> <p>Liste de la documentation :</p> <ul style="list-style-type: none"> <li>• Yquem evaluation – Documentation report (ST19WR66I), Référence : SMD_YQUEM_DR_05_002 V02.01 STMicroelectronics</li> </ul>
[GUIDES]	<p>Les guides d'utilisation du produit sont constitués des documents suivants :</p> <ul style="list-style-type: none"> <li>• ST19WR66 - Data Sheet, Référence : DS_19WR66/0605 V3 STMicroelectronics</li> <li>• ST19X-19W - Security Application Manual, Référence : APM_19X-19W_SECU/0312 v1.7 STMicroelectronics</li> <li>• ST19X-ST19W - Security Application Manual - Addendum-2 to V1.7, Référence : AD2_APM_19X-19W_SECU1.7/0407V1.0 STMicroelectronics</li> <li>• ST19X-ST19W - Security Application Manual - Addendum-3 to V1.7, Référence : AD3_APM_19x-19W_SECU1.7_0411 V1.0 STMicroelectronics</li> <li>• ST19X-ST19W - Security Application Manual - Addendum-4 to V1.7, Référence : AD4_APM_19x-19W_SECU/0606 Rev1 STMicroelectronics</li> <li>• ST19W - System ROM –Issuer configuration - user manual Référence : UM_19W_SR_I/0306VP2 STMicroelectronics</li> <li>• ST19W - System ROM –Issuer configuration - user manual addendum Référence : AD_UM_19W_SR_I/0308V1.1 STMicroelectronics</li> <li>• System Library - User Manual, Référence : UM_19X-19W_SYSLIB/0404V2.1 STMicroelectronics</li> </ul>

	<ul style="list-style-type: none"> <li>• ST19X – Enhanced DES Library User Manual Référence : UM_19XV2_EDESLIB/0203V1.1 STMicroelectronics</li> <li>• ST19X - Cryptographic Library LIB4 V2.0 - User Manual, Référence : UM_19X_LIB4V2/0503V3 STMicroelectronics</li> <li>• ST19W AES library – User manuel, Référence : UM_19W_AES/0304VP1 STMicroelectronics</li> <li>• ST19W - AIS31 Compliant Random Numbers - User Manual, Référence : UM_19W_AIS31_CRN/0503V3 STMicroelectronics</li> <li>• ST19X-19W - RF Products - Communication Library - User Manual, Référence : UM_19X-19W_RFComLib/0409 V2 STMicroelectronics</li> <li>• ST19WR66 - Using RFUART with Contactless Communication Library – Addendum, Référence : AD_19WR66_RFComLib_UART/0410V1 STMicroelectronics</li> <li>• ST19WR66 - Recommendations for Contactless Operation - Application Note, Référence : AN_19WR66_Recom/0604 Rev3 STMicroelectronics</li> <li>• ST19X-19W RF products – Dual Interface Manager - User Manual, Référence : UM_19X-19W_DI_MG/0504V2 STMicroelectronics</li> </ul>
[PP/9806]	<p>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. <i>Document publié sur le site : <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a></i></p>
[PP BSI]	<p>Smartcard IC Platform Protection Profile, Référence : BSI-0002-2001, version 1.0, juillet 2002 Bundesamt für Sicherheit in der Informationstechnik (BSI)</p>
[RTE]	<p>Rapport technique d'évaluation complet :</p> <ul style="list-style-type: none"> <li>• Evaluation Technical Report - ST19WR66I (EAL5+ evaluation), Référence : YQM_ETR_WR66I_v2.0 Serma Technologies</li> </ul> <p>Pour le besoin des évaluations en composition, une version diffusable du document a été validée :</p> <ul style="list-style-type: none"> <li>• ETR-lite for composition - ST19WR66D - ST19WR66I - (EAL5+ evaluation), Référence : YQUEM_ETR lite ST19WR66D-I v1 Serma Technologies</li> </ul>

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"><li>• ST19W generic security target, Référence : SCP_YQUEM_ST_03_001_V02.02 STMicroelectronics</li></ul> <p>Pour les besoins de la reconnaissance internationale, la cible suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"><li>• ST19WR66 Security Target, Référence : SMD_ST19WR66_ST_05_001_V01.02 STMicroelectronics</li></ul>
------	---

### Annexe 3. 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.
[COMP]	Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002.
[AIS31]	Functionality classes and evaluation methodology for physical random number generator, Référence : AIS31 version 1 du 25/09/2001, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[AIS34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004 Bundesamt für Sicherheit in der Informationstechnik (BSI)
[FIPS 140]	Security Requirements for Cryptographic Modules Référence : FIPS PUB-140-2:1999 NIST.
[CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard - version 1.02 du 19/11/04, SGDN/DCSSI <i>Document publié sur le site : <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a></i>

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  
Centre de certification  
51, boulevard de la Tour Maubourg  
75700 Paris cedex 07 SP

[certification.dcssi@sgdn.pm.gouv.fr](mailto:certification.dcssi@sgdn.pm.gouv.fr)

La reproduction de ce document sans altérations ni coupures est autorisée.