



PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/27

Microcontrôleur sécurisé ST19NR66B

Paris, le 8 décembre 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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.



Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense 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

La reproduction de ce document sans altération ni coupure est autorisée.



Référence du rapport de certification	2006/27
Nom du produit	Microcontrôleur sécurisé ST19NR66B
Référence/version du produit	ST19NR66 révision B (logiciel dédié ZXB, maskset K7H0A)
Conformité à un profil de protection	PP/9806 – PP BSI-PP-002-2001
Critères d'évaluation et version	Critères Communs version 2.3 conforme à la norme ISO 15408:2005
Niveau d'évaluation	EAL 5 augmenté ALC_DVS.2, AVA_MSU.3, AVA_VLA.4
Développeur(s)	STMicroelectronics Smartcard IC division, ZI de Rousset, BP2, 13106 Rousset Cedex, France
Commanditaire	STMicroelectronics Smartcard IC division, ZI de Rousset, BP2, 13106 Rousset Cedex, France
Centre d'évaluation	Serma Technologies 30 avenue Gustave Eiffel, 33608 Pessac, France Tél : +33 (0)5 57 26 08 64, mél : m.dus@serma.com
Accords de reconnaissance applicables	<div style="display: flex; justify-content: space-around;"><div style="text-align: center;">CCRA </div><div style="text-align: center;">SOG-IS </div></div> <p>Le produit est reconnu au niveau EAL4</p>

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 disponibles sur le site Internet www.ssi.gouv.fr.



Table des matières

1. LE PRODUIT	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT EVALUE	6
1.2.1. <i>Identification du produit</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Cycle de vie</i>	8
1.2.5. <i>Configuration évaluée</i>	9
2. L’EVALUATION	10
2.1. REFERENTIELS D’EVALUATION.....	10
2.2. TRAVAUX D’EVALUATION	10
2.3. L’ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES	10
2.4. L’ANALYSE DU GENERATEUR D’ALEAS	10
3. LA CERTIFICATION	11
3.1. CONCLUSION	11
3.2. RESTRICTIONS D’USAGE.....	11
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	12
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	13
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	14
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	16

1. Le produit

1.1. Présentation du produit

Le produit évalué est le microcontrôleur sécurisé ST19NR66 en révision B. 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 ST19NR66B (logiciel dédié ZXB, maskset K7H0A).

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

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme aux profils de protection [PP9806] et [PP0002].

1.2.1. Identification du produit

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

La version certifiée du produit est identifiable par les éléments suivants, visibles au microscope sur les puces :

- identification de la puce (maskset) : K7H0A ;
- référence du logiciel dédié : ZXB ;
- référence du logiciel embarqué : dépendant de l'application masquée en ROM ;
- identification du site de fabrication : STMicroelectronics_4 (Rousset).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- initialisation de la plate-forme matérielle et des attributs ;
- gestion sécurisée du cycle de vie ;
- intégrité logique du produit ;
- tests des fonctions de sécurité ;
- authentification de l'administrateur ;
- stockage et firewall de contrôle d'accès ;
- détection des attaques ;
- gestions des violations sécuritaires ;
- non-observabilité ;
- support au chiffrement cryptographique à clés symétriques ;
- support au chiffrement cryptographique à clés asymétriques ;



- support à la génération de nombres non prédictibles.

1.2.3. Architecture

Le microcontrôleur ST19NR66B 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 (SMACL), 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.

1.2.4. Cycle de vie

Le cycle de vie du développement est résumé dans le schéma suivant :

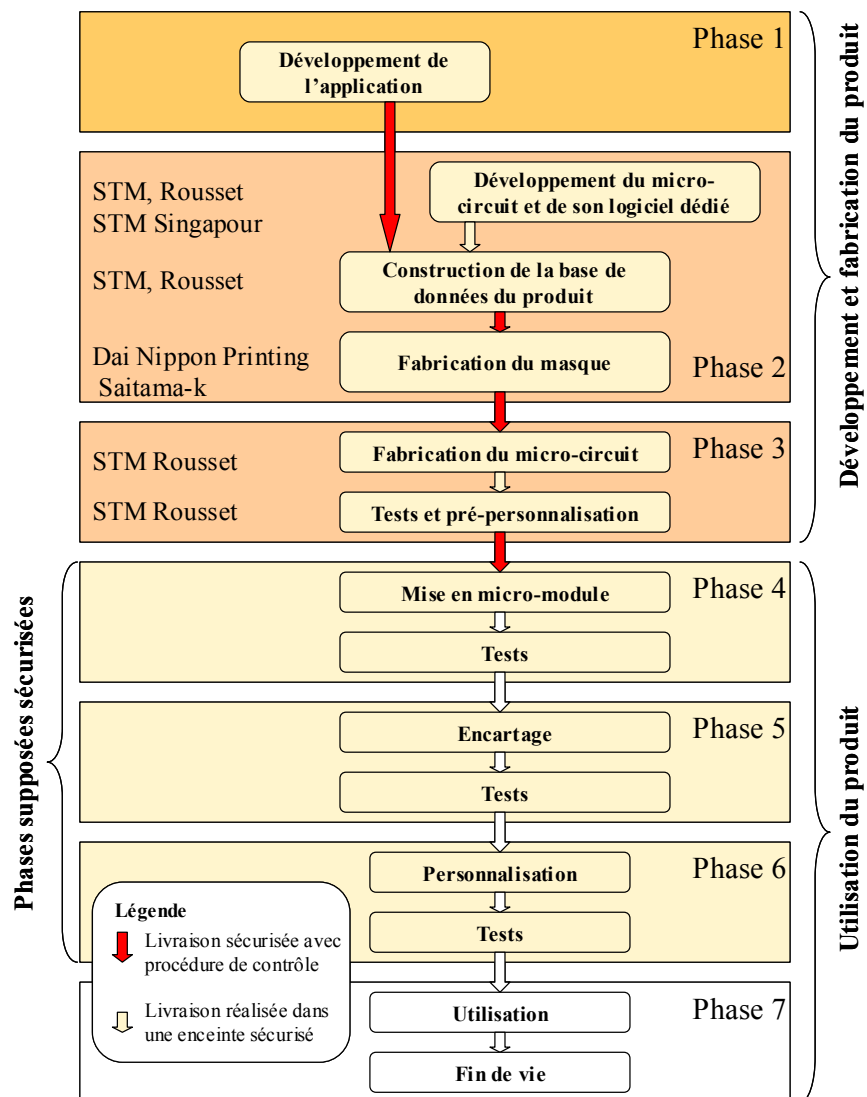


Figure 1 - Cycle de vie standard d'une carte à puce

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

Le produit comporte lui-même une gestion de son cycle de vie fonctionnel, prenant la forme de 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.

1.2.5. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur et aux logiciels dédiés identifiés au §1.1. 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).

Pour les besoins de l'évaluation, le microcontrôleur ST19NR66B a été fourni au centre d'évaluation avec un système d'exploitation logiciel dédié (Card Manager référence : TZV), dans un mode dit « ouvert¹ ».

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

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

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

Pour répondre aux spécificités des cartes à puce, les guides [CCIC] et [CCAP] ont été appliqués.

Le produit ST19NR66B a déjà été certifié en 2006 sous la référence 2006/22 (cf. [2006/22]). 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. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], délivré à la DCSSI le 1^{er} décembre 2006, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. L'analyse de la résistance des mécanismes cryptographiques

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

2.4. L'analyse du générateur d'aléas

Le produit évalué offre un générateur d'aléas qui peut être utilisé par le logiciel embarqué.

Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS31] et [FIPS 140] par le centre d'évaluation

Le générateur est de classe « P2 – *SOF-high* » selon l'[AIS31], et atteint le niveau « Level 3¹ » selon la [FIPS 140].

¹ Seul le sous-ensemble du [FIPS 140] relatif aux générateurs de nombres aléatoires a été évalué et uniquement au travers des tests statistiques spécifiés dans cette norme.



3. La certification

3.1. Conclusion

L'évaluation, identifiée au chapitre 2 et décrite dans le rapport technique d'évaluation [RTE], a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises par un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le microcontrôleur sécurisé ST19NR66B soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit ST19NR66B 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- 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 du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance 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 :



3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, il n'est reconnu qu'au niveau EAL4.

L'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires², des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

² Les pays signataires de l'accord sont : l'Allemagne, l'Australie, l'Autriche, le Canada, la Corée du Sud, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Nouvelle Zélande, la Norvège, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.



Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				1	1	2	2	1	Partial CM automation
	ACM_CAP	1	2	3	4	4	5	5	4	Configuration support and acceptance procedures
	ACM_SCP			1	2	3	3	3	3	Development tools CM coverage
ADO Livraison et opération	ADO_DEL		1	1	2	2	2	3	2	Detection of modification
	ADO_IGS	1	1	1	1	1	1	1	1	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	1	1	1	2	3	3	4	3	Semiformal functional specification
	ADV_HLD		1	2	2	3	4	5	3	Semiformal high-level design
	ADV_IMP				1	2	3	3	2	Implementation of the TSF
	ADV_INT					1	2	3	1	Modularity
	ADV_LLD				1	1	2	2	1	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	2	Semiformal correspondence demonstration
	ADV_SPM				1	3	3	3	3	Formal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	1	1	1	1	1	1	1	1	Administrator guidance
	AGD_USR	1	1	1	1	1	1	1	1	User guidance
ALC Support au cycle de vie	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	2	Standardised life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	2	Testing: low-level design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					1	2	2	1	Covert channel analysis
	AVA_MSU			1	2	2	3	3	3	Analysis and testing of insecure states
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	4	Highly resistant

Annexe 2. Références documentaires du produit évalué

[2006/22]	Rapport de certification 2006/22 - Microcontrôleur sécurisé ST19NR66B, 21 novembre 2006, SGDN/DCSSI
[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - ST19N Generic Security Target, Référence : SMD_ST19N_ST_06_001_V01.01, STMicroelectronics <p>Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - ST19NR66 Security Target, Référence : SMD_ST19NR66_ST_06_001_V01.00 STMicroelectronics
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report - ST19NR66B (EAL5+ evaluation), Référence : YQM_ETR_NR66B_v1.1 Serma Technologies <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validée :</p> <ul style="list-style-type: none"> - Evaluation Technical Report Lite - ST19NR66B, Référence : YQUEM_ETR Lite ST19NR66B_v1.0 Serma Technologies
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - Configuration List ST19NR66B - PRODUCT - K7H0A MASK SET, Référence : MKT_K7H0_CFGL_06_003_V1.1 STMicroelectronics <p>Liste de la documentation :</p> <ul style="list-style-type: none"> - Yquem Evaluation – documentation report (ST19NR66B), Référence : SMD_YQUEM_DR_06_001_V1.2 STMicroelectronics
[GUIDES]	<p>Les guides d'utilisation du produit sont constitués des documents suivants :</p> <ul style="list-style-type: none"> - ST19NR66 Dual Contactless Smartcard MCU with 66 KBytes High Density EEPROM, Enhanced RF Performances, Référence : DS_19NR66/0609 Rev 2, STMicroelectronics - Application Note: Migrating from STWR66 to ST19NR66, Référence : AN19WR66_NR66/0605 Rev 1, STMicroelectronics - Manuals of security recommendations v2.0, Référence : APM_19W-19N_SECU/0612V2.0 STMicroelectronics <p>ST19NR66 System ROM Issuer Configuration User</p>



	<p>Manual, Référence : UM_19NR66_SR_I/0611 Rev 3, STMicroelectronics</p> <ul style="list-style-type: none"> - ST19W - System ROM –Issuer configuration - user manual addendum, Référence : AD_UM_19W_SR_I/0308V1.1 STMicroelectronics - ST19N System Library V2 User Manual, Référence : Um_19N_SysLibV2/0610 Rev 3, STMicroelectronics - ST19X, ST19W and 19N EDES Library User Manual, Référence : UM_19X_EDESLIB/0605 Rev 2, STMicroelectronics - ST19N - Fast Cryptographic Library FastLIB4 – User Manual, Référence : UM_19N_FASTLIB4/0605 Rev 3, STMicroelectronics - ST19W and ST19N AES Library - User Manual, Référence : UM_19W_19N_AES/0610 Rev 2, STMicroelectronics - ST19N RF UART Communication Library User Manual, Référence : Um19N_RFUART_CommLib/0610 Rev 2, STMicroelectronics - ST19W AIS31 compliant random numbers, User Manual, Référence : UM_19W_AIS31_CRN/0503, V3 STMicroelectronics
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. <i>Certifié sous la référence PP/9806.</i>
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. <i>Certifié sous la référence BSI-PP-0002-2001.</i>

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]	<p>Common Criteria for Information Technology Security Evaluation :</p> <p>Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001;</p> <p>Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002;</p> <p>Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003.</p> <p>Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004.</p> <p>Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.</p>
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[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.
[AIS34]	<p>Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004</p> <p>Bundesamt für Sicherheit in der Informationstechnik</p>



[AIS31]	Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25/09/2001, Bundesamt für Sicherheit in der Informationstechnik
[FIPS 140]	Security Requirements for Cryptographic Modules Référence : FIPS PUB-140-2:1999 NIST.