Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Certification Report 2006/18

ST19WR66I microcontroller

Courtesy Translation

Paris, november, 7th 2006

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux

SÉCURITÉ CERTIFICATION

Warning

This report is designed to provide principals with a document enabling them to certify the level of security offered by a product under the conditions of use or operation laid down in this report for the version evaluated. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the user and administration guides evaluated, as well as with the product security target, which presents threats, environmental scenarios and presupposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.

Certification does not, however, constitute in and of itself a product recommendation from the certifying organization, and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Synthesis

Certification Report 2006/18

ST19WR66I secure microcontroller

Developer: STMicroelectronics

Common Criteria version 2.2

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

conformant to both PP/9806 and BSI-PP-002-2001 protection profiles

Evaluation sponsor: STMicroelectronics

Evaluation facility: Serma Technologies

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfill the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures have been published and are available in French on the following Internet site:

www.ssi.gouv.fr

Recognition Agreement of the certificates

The European Recognition Agreement made by SOG-IS in 1999 allows recognition, between Signatory States of the agreement[1], of the certificates delivered by the respective certification bodies. The mutual European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

The Direction Centrale de la Sécurité des Systèmes d'Information has also signed recognition agreements with other certification bodies from countries that are not members of the European Union. Those agreements can feature that the certificates delivered by France are recognized by the Signatory States. They also can feature that the certificated delivered by each Party are recognized by all signatory parties. (Article 9 of decree number 2002-535).
Thus, the Common Criteria Recognition Arrangement allows the recognition, by all signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

1 In April 999, the signatory countries of the SOG-IS agreement are: United Kingdom, Germany, France, Spain, Italy, Switzerland, Netherlands, Finland, Norway, Sweden and Portugal.
2 In May 2005, the countries releasing certificates that have signed the agreement are : France, Germany, United Kingdom, United States, Canada, Australia-New Zealand and Japan ; the countries not releasing certificates that have signed the agreement are: Austria, Spain, Finland, Greece, Hungary, Israel, Italy, Norway, Netherlands, Sweden,Turkey, Tcheque Republic, Singapore and India.

Table of contents

1. The evaluated product

1.1. Product identification

The evaluated product is the ST19WR66 (revision I) microcontroller (dedicated software ZIC, maskset K7E0IIA) developed by STMicroelectronics. This product includes a software test ("Autotest") and a software library (system management, crypto library), stored in ROM memory.

1.2. The developer

Several actors are in charge of the product development and manufacturing:

The product is designed, prepared and tested by:

STMicroelectronics

Smartcard IC division
ZI de Rousset, BP2
13106 Rousset Cedex
France

A part of the design is realised by:

STMicroelectronics

28 Ang Mo Kio - Industrial park 2
Singapore 569508
Singapore.

The photo masks of the product are manufactured by:

DAI NIPPON PRINTING CO., LTD

2-2-1, Fukuoka, kamifukuoka-shi,
Saitama-Ken, 356-8507
Japan

1.3. Evaluated product description

The evaluated product is the ST19WR66I microcontroller from the ST19W platform family developed and manufactured by STMicroelectronics.
The product can be in one of its three possible configurations:

- «Test» configuration: TOE configuration at the end of developer IC manufacturing. The TOE is tested with a part of the Dedicated Software (called "Autotest") within the secure developer premises. Pre-personalization data can be loaded in the EEPROM. The TOE configuration is changed to "Issuer" before delivery to the next user, and the part cannot be reversed to the «test» configuration.

- «Issuer» configuration: TOE configuration when delivered to users involved in IC packaging and personalization. Limited tests are still possible with the Dedicated Software (System Rom operating system). Personalization data can be loaded in the EEPROM.
  The TOE configuration is changed to its final "User" configuration when delivered to the end user (the part cannot be reversed to the «Issuer» configuration).
- «User» configuration: Final TOE configuration. The developer test functionalities are unavailable. The Dedicated Software only provides the power-on reset sequence and routine libraries (mainly cryptographic services). After the power-on reset sequence, the TOE functionality is driven exclusively by the Embedded Software.

The microcontroller aims to host one or several software applications and to be embedded in a plastic support to create a Smartcard with multiple possible usages (banking, health card, pay-TV or transport applications …) depending on the Embedded Software applications. However, only the microcontroller is evaluated. The software applications are not in the scope of this evaluation.

1.3.1. Architecture

The ST19WR66I microcontroller is made up of:

- A Hardware part:
  - An 8-bit processing unit;
  - Memories: EEPROM (high density 66KB with integrity control, for program and data storage), ROM (224KB for user, 32KB for dedicated software : autotest and cryptographic libraries) and SRAM (6KB) ;
  - Security Modules: Memory Access Control Logic (MACL), clock generator, security administrator, power management, memories integrity control ;
  - Functional Modules: 8-bits timers, I/O management in contact mode (IART ISO 7816-3) and contactless mode (RFUART ISO 14443-B), True Random Number Generators, DES and RSA co-processing units.
- A dedicated software is embedded in ROM which comprises :
  - Microcontroller test capabilities («Autotest ») ;
  - System and Hardware/Software interface management capabilities
  - ISO 14443-B interface management capabilities;
  - Cryptographic libraries: DES (E-DES implementation), AES and RSA which are included in the product security target.

1.3.2. Life-cycle

The product life-cycle is the following:

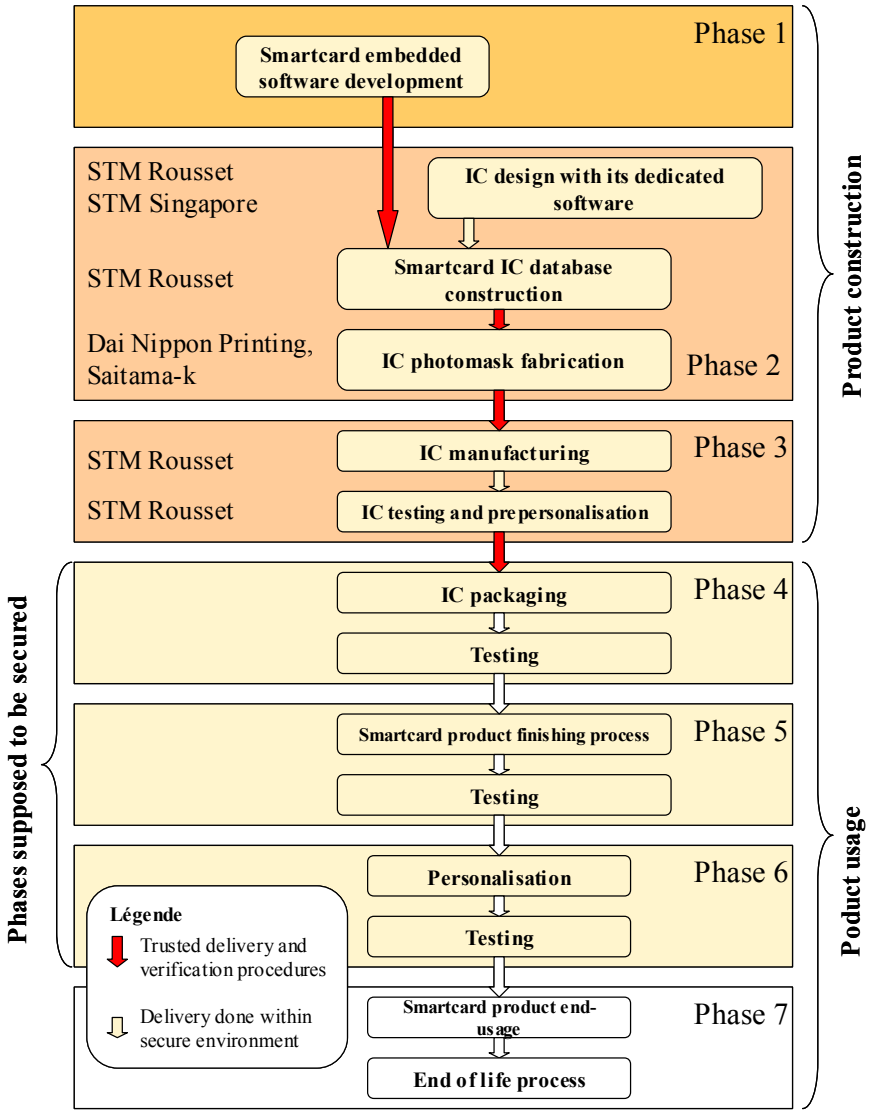

Figure 1 – Life cycle

1.3.3. Evaluated product scope

This certification report presents the evaluation work related to the product and the dedicated software library identified in §1.1 and described in §1.3. Any other embedded application, such as embedded applications intended specifically for the sake of the evaluation is not part of the evaluation perimeter.

Referring to the life-cycle, the evaluated product is the product that comes out the manufacturing, test and pre-personalization phase (phase 3).

2. The evaluation

2.1. Context

The ST19WR66I product has already certified in 2006 with [2006/12] reference. Some complementary works have been performed on the random number generator in order to assess the conformance to the AIS31 method criteria (see [AIS31]). Thus, the verdicts related to all the other evaluation works are re-used.

2.2. Evaluation referential

The evaluation has been conducted in accordance with the Common Criteria standard [CC] and the evaluation methodology defined within the CEM [CEM]. For the assurance components higher than EAL4 level, the ITSEF have used proprietary methods that are compliant to the [AIS34] documentation. These methods have been validated by the DCSSI.

2.3. Evaluation sponsor

STMicroelectronics

Smartcard IC division
ZI de Rousset, BP2
13106 Rousset Cedex
France

2.4. Evaluation facility

Serma Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Phone: +33 (0)5 57 26 08 64

Email: m.dus@serma.com

2.5. Technical evaluation report

The evaluation took place from April to July 2006.

The Evaluation Technical Report [ETR] describes the evaluator activities and presents the obtained results. The following paragraphs summarize the main evaluation results.

2.6. Security target evaluation

The security target [ST] defines the evaluated product and its operational environment.

This security target is compliant to both [PP9806] and [PP BSI] protection profiles.

For the security target evaluation tasks, the evaluator has issued the following verdicts:

ASE class: Security target evaluation		**Verdicts**
ASE_DES.1	TOE description	Pass
ASE_ENV.1	Security environment	Pass
ASE_INT.1	ST introduction	Pass
ASE_OBJ.1	Security objectives	Pass
ASE_PPC.1	PP claims	Pass
ASE_REQ.1	IT security requirements	Pass
ASE_SRE.1	Explicitly stated IT security requirements	Pass
ASE_TSS.1	Security Target, TOE summary specification	Pass

2.7. Product evaluation

2.7.1. Evaluation tasks

The evaluation tasks have been performed in compliance to Common Criteria [CC] and its methodology [CEM] at level EAL5[1] augmented. The following table details the selected EAL5 augmentations:

Assurance component	
EAL5	Semi-formally designed and tested
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_MSU.3	Analysis and testing for insecure state
+ AVA_VLA.4	Highly resistant

2.7.2. Development environment evaluation

The product is developed on the sites identified at §1.2 (Rousset in France, Singapore and Saitama-Ken in Japan).

The security measures assessed by the evaluator provide guaranty to maintain the confidentiality and the integrity of the evaluated product and its related documentation during the development phase.

The evaluator has analyzed the configuration management plan provided by the developer that describes the use of the configuration management system. This system can generate in particular the configuration list [CONF] that identifies all the product components managed by the system.

[1] 0 : Table of the different evaluation assurance levels (EAL – Evaluation Assurance Level) predefined in the Common Criteria [CC].

The generation procedures also provide assurance that the appropriate components are used to generate the evaluated product.

The evaluator has verified that the product development cycle was corresponding to a standard life-cycle applied to the Smartcard domain[1]. The evaluator has also verified that the methods and the development tools were documented and corresponding to implementation standards.

The verification of the procedure application is regularly performed during other STMicroelectronics product evaluations or re-evaluations. No specific audit has been planned in the frame of the current re-evaluation.

For the development environment related evaluation tasks, the evaluator has issued the following verdicts:

ACM class: Configuration management		**Verdicts**
ACM_AUT.1	Partial CM automation	Pass
ACM_CAP.4	Generation support and acceptance procedures	Pass
ACM_SCP.3	Development tools CM coverage	Pass
ALC class: Life-cycle support		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Pass
ALC_LCD.2	Standardised life-cycle model	Pass
ALC_TAT.2	Compliance with development standards	Pass

2.7.3. Product development evaluation

The development documentation analysis has provided the evaluator assurance that the functional requirements which are identified in the security target and listed here below, are correctly and completely refined in the following product representation levels: semi-formal functional specification (FSP), semi-formal high level design (HLD), low level design (LLD), implementation (IMP).

The modular design is demonstrated by construction, due to the hardware development, and was not subject to any specific analysis.

The functional requirements which are identified in the security target are the following:

- 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)
- Stored data integrity monitoring and action (FDP_SDI.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- User attribute definition (FIA_ATD.1)

[1] It is not a standardized life-cycle model issued by a standardization body but a strictly formalized model that fits to a recognized Smartcard related model (see [CC] part 3, §386).

  - 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)
- Explicit security requirements :
  - Audit storage (FAU_SAS.1)
  - Quality metrics for random numbers (FCS_RDN.1)
  - Limited capabilities (FMT_LIM.1)
  - Limited availability (FMT_LIM.2)

For the product development evaluation tasks, the evaluator has issued the following verdicts:

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

2.7.4. Delivery and installation procedure evaluation

As per the evaluation guide « The application of CC to IC » (cf. [CC_IC]), the deliveries under consideration are:
- The delivery of the embedded application code to the microcontroller manufacturer,
- The delivery of information required by the mask manufacturer,
- The delivery of the mask to the microcontroller manufacturer,
- The delivery of the microcontroller to the entity in charge of the next step (embedding into micro-module, card manufacturing).

The involved sites are identified at §1.2.

The evaluator has analysed the product delivery procedures between all related sites. Those procedures allow to identify the origin of the delivery and to detect any product modification during the delivery.

The product is a generic microcontroller without specific embedded application. As a consequence, it does not need any installation, generation or start-up phase. The ADO_IGS.1 assurance component requirements are thus not applicable.

For the delivery and installation procedure evaluation tasks, the evaluator has issued the following verdicts:

ADO class: Delivery and installation		Verdicts
ADO_DEL.2	Detection of modification	Pass
ADO_IGS.1	Installation, generation, and start-up procedures	Pass

2.7.5. Guidance documentation evaluation

Utilisation

The evaluated product has no specific embedded application. It is a hardware and software platform offering several services to the user embedded software targeting a usage as smartcard. The users of the microcontroller can be seen as application developers (see document [CC IC]) as well as any related people involved during the administration phases of the micro-module and of the card (phases 4 to 6), including configuration and personalization of the embedded applications.

In this evaluation frame, those roles are reminded in the security target [ST]: the users are defined as the people able to use the functionalities of the microcontroller, its software libraries and its application software. This definition includes any user using the product when configured in the « user » mode: the card issuer, the embedded software developer, the entity in charge of the embedding and the entity in charge of integrating the card in the final system.

Administration

The guide « The application of CC to Integrated Circuits » [CC IC] defines the product administrators as the entities having an action on the product between phases 4 to 7 of the life-cycle, who set-up (personalization) the final product. Those operations are mainly depending on the embedded applications. In the frame of the microcontroller, only the administration interfaces related to this microcontroller are evaluated. Phases 4 to 6 called « administrative » are covered by a hypothesis in the protection profile, which assumes that the operations related to those phases are done in specific conditions that are not threatening the product security. Those conditions have not been evaluated.

The evaluator has analysed the administration and user guidance [GUIDES] to provide assurance that the evaluated product could be used in a secured manner.

For the guidance documentation evaluation tasks, the evaluator has issued the following verdicts:

AGD class: Guidances		Verdicts
AGD_ADM.1	Administrator guidance	Pass
AGD_USR.1	User guidance	Pass

2.7.6. Functional test evaluation

The evaluator has analysed the documentation of the tests performed by the developer in order to provide assurance that all the product functionalities listed in the security target have been properly tested.

The evaluator has also carried out independent functional tests to provide assurance of the correct operation of the evaluated product.

The evaluator has performed his independent functional tests on platform ST19WR66 in revision I identified at §1.1 and provided to the ITSEF in a mode known as « open[1] ».

For the functional test evaluation tasks, the evaluator has issued the following verdicts:

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

2.7.7. Vulnerability assessment

The evaluator has checked that the documentation delivered with the product [GUIDES] is clear enough to avoid any misuse or operational mistake that could lead to a non secured state of the product.

Only the test configuration authentication functions and the random number generator function (with metrics inspired from the [AIS31] and the [FIPS 140-2]) have been subject to an intrinsic resistance level assessment. Strength of those functions meets the high level:

- SOF-high for the authentication function in «test» and «issuer» configuration;
- Class « P2 - High » according to the [AIS31] and « Level 3[2] » according to [FIPS 140-2] for the true random number generators.

Relying on the developer vulnerability analysis and all the information provided in the evaluation frame, the evaluator has performed its own independent analysis to assess the potential vulnerabilities of the product. This analysis was completed by tests performed on the ST19WR66 product revision I, identified at §1.1 and provided to the ITSEF in a mode known as « open[1] ».

The analysis conducted by the evaluator does not point the existence of exploitable vulnerabilities for the targeted security level. The product is thus resistant to attacker possessing **a high level attack potential**.

For the vulnerability assessment tasks, the evaluator has issued the following verdicts:

AVA class: Vulnerability assessment		Verdicts
AVA_CCA.1	Covert Channel Analysis	Pass
AVA_MSU.3	Analysis and testing for insecure state	Pass
AVA_SOF.1	Strength of TOE security function evaluation	Pass
AVA_VLA.4	Highly resistant	Pass

2.7.8. Cryptographic mechanism analysis

No analysis of the cryptographic mechanism resistance has been performed by the DCSSI.

[1] mode that enables to load and execute a native code in EEPROM and also to disable the configurable security mechanisms

[2] Only the [FIPS 140-2] subset related to random number generators has been evaluated and only regarding the statistical tests specified in the standard.

2.7.9. Cryptographic mechanism analysis

The evaluated product is featuring two random generators available for the user's embedded software. These generators have been analyzed by the DCSSI.
The analysis did not evidence any blocking statistical bias for a direct usage of both random generator outputs. However, this analysis cannot prove that the generated data are really random but provide the assurance that the generators have no major design default. As mentioned in [CRYPTO], it is reminded that, for a cryptographic use, the TRNG output must imperatively undergo an algorithmic reprocessing, even if the analysis of the physical random generator has revealed no weakness.

3. The certification

3.1. Conclusions

The whole tasks performed by the ITSEF and described in the evaluation technical report [ETR] enable the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the copies of the products or systems submitted for evaluation fulfill the security features specified in its security target [ST]. It also certifies that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (Art. 8 of decree 202-535).

3.2. Usage restrictions

The evaluation conclusions are valid only for the product identified in chapter 1 of the current certification report.

This certificate provides a resistance assessment of the ST19WR66I product to a set of attacks which remains generic due to the missing of any specific embedded application. Therefore, the security of a final product based on the evaluated microcontroller would only be assessed through the final product evaluation which could be performed on the basis of the current evaluation results.

The user of the certified product shall respect the operational environmental security objectives summarized here-after and the recommendations within the user guidance [GUIDES]:

- Security procedures must be applied during the product delivery to the users in order to maintain the confidentiality and integrity of the product and the related manufacturing and test data (prevent any copy, modification, theft, unauthorized manipulation or usage) ;
- The communication between a product developed based on the secured microcontroller and other products must be secured (in terms of protocols and procedures) ;
- The system (work station, terminal, communication,…) must guaranty the confidentiality and the integrity of the sensitive data which are stored or processed.

Appendix 1. Predefined Evaluation Assurance Level

Class	Family	Components by Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ACM class Configuration Management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
ADO class Delivery & operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
ADV class Development	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
AGD class Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
ALC class Life-cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
ATE class 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**
AVA class Vulnerability assessment	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

Appendix 2. References about the evaluated product

[2006/12]	Rapport de certification 2006/12 - Micro-circuit ST19WR66I, 19 juillet 2006 SGDN/DCSSI
[CONF]	Product configuration list : • Configuration List ST19WR66I PRODUCT K7E4A MASK SET Reference: SCP_K7E0_YQUEM_CFGL_06_001_V01.01 STMicroelectronics List of the delivered materials by STMicroelectronics : • Documentation report (ST19WR66I), Reference : SMD_YQUEM_DR_05_002 V02.01 STMicroelectronics
[GUIDES]	The product user guidance documentation is the following : • ST19WR66 - Data Sheet, Reference : DS_19WR66/0605 V3 STMicroelectronics • ST19X-19W - Security Application Manual, Reference : APM_19X-19W_SECU/0312 v1.7 STMicroelectronics • ST19X-ST19W - Security Application Manual - Addendum-2 to V1.7, Reference : AD2_APM_19X-19W_SECU1.7/0407V1.0 STMicroelectronics • ST19X-ST19W - Security Application Manual - Addendum-3 to V1.7, Reference : AD3_APM_19x-19W_SECU1.7_0411 V1.0 STMicroelectronics • ST19X-ST19W - Security Application Manual - Addendum-4 to V1.7, Reference : AD4_APM_19x-19W_SECU/0606 rev 1 STMicroelectronics • ST19W - System ROM –Issuer configuration - user manual Reference : UM_19W_SR_I/0306VP2 STMicroelectronics • ST19W - System ROM –Issuer configuration - user manual addendum Reference : AD_UM_19W_SR_I/0308V1.1 STMicroelectronics • System Library - User Manual, Reference : UM_19X-19W_SYSLIB/0404V2.1 STMicroelectronics • ST19X – Enhanced DES Library User Manual Reference : UM_19XV2_EDESLIB/0203V1.1 STMicroelectronics

	• ST19X - Cryptographic Library LIB4 V2.0 - User Manual, Reference : UM_19X_LIB4V2/0503V3 STMicroelectronics • ST19W AES library – User manual, Reference : UM_19W_AES/0304VP1 STMicroelectronics • ST19W - AIS31 Compliant Random Numbers - User Manual, Reference : UM_19W_AIS31_CRN/0503V3 STMicroelectronics • ST19X-19W - RF Products - Communication Library - User Manual, Reference : UM_19X-19W_RFComLib/0409 V2 STMicroelectronics • ST19WR66 - Using RFUART with Contactless Communication Library – Addendum, Reference : AD_19WR66_RFComLib_UART/0410V1 STMicroelectronics • ST19WR66 - Recommendations for Contactless Operation - Application Note, Reference : AN_19WR66_Recom/0604 Rev3 STMicroelectronics • ST19X-19W RF products – Dual Interface Manager - User Manual, Reference : UM_19X-19W _DI_MG/0504V2 STMicroelectronics
[PP/9806]	Common Criteria for Information Technology Security Evaluation - Protection Profile: Smart Card Integrated Circuit Version 2.0, Issue September 1998. Certified by the French Certification Body under the reference PP/9806. *Documentation released on the website : www.ssi.gouv.fr*
[PP BSI]	Smartcard IC Platform Protection Profile, Reference : BSI-0002-2001, version 1.0, July 2002 Bundesamt für Sicherheit in der Informationstechnik (BSI)
[ETR]	Complete Evaluation Technical Report : • Evaluation Technical Report - ST19WR66I (EAL5+ evaluation), Reference : YQM_ETR_WR66I_v2.0 Serma Technologies For composite evaluation purpose, a deliverable version has been validated: • ETR-lite for composition – ST19WR66D ST19WR66I, Reference : ETR_lite_ST19WR66D-I v1.0 Serma Technologies

[ST]	Referenced security target for the evaluation : • ST19W generic security target, Reference : SCP_YQUEM_ST_03_001_V02.02 STMicroelectronics Public security target • ST19WR66 Security Target, Reference : SMD_ST19WR66_ST_05_001_V01.02 STMicroelectronics

Appendix 3. References related to the certification

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure 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 Reference : AIS31 version 1, 25 September 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 140-2]	Security Requirements for Cryptographic Modules Reference: FIPS PUB-140-2:1999 NIST
[CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard – version1.02 du 19/11/04, SGDN/DCSSI Documentation available on the site : www.ssi.gouv.fr

Any correspondence about this report has to be addressed to:

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