Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Certification Report 2005/41

ST19WP18E microcontroller

Courtesy Translation

Paris, November, 18th 2005

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 2005/41

ST19WP18E 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

The following augmentations are not recognized within the framework of the 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

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 ST19WP18 in revision E microcontroller (dedicated software YAC, maskset K780EEA) 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 ST19WP18E microcontroller from the ST19W 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.

a) «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 only is not a product usable as such. It is intended to host software applications such as TPM (Trusted Platform Module). The TPM software applications are not in the scope of this evaluation.

1.3.1. Architecture

The ST19WL66B microcontroller is made up of:

- A Hardware part:
  - An 8-bit processing unit;
  - Memories: EEPROM (high density 18KB with integrity control, for program and data storage), ROM (112KB 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 (contact mode ISO 7816-3, LPC, GPI/O), random number generators (TRNG), DES and RSA co-processing units.
- A dedicated software is embedded in ROM which comprises :
  - Microcontroller test capabilities («Autotest ») ;
  - System management capabilities
  - Cryptographic libraries: DES (E-DES implementation), RSA and SHA-1 which are included in the product security target.

1.3.2. Life-cycle

The product life-cycle is the following:

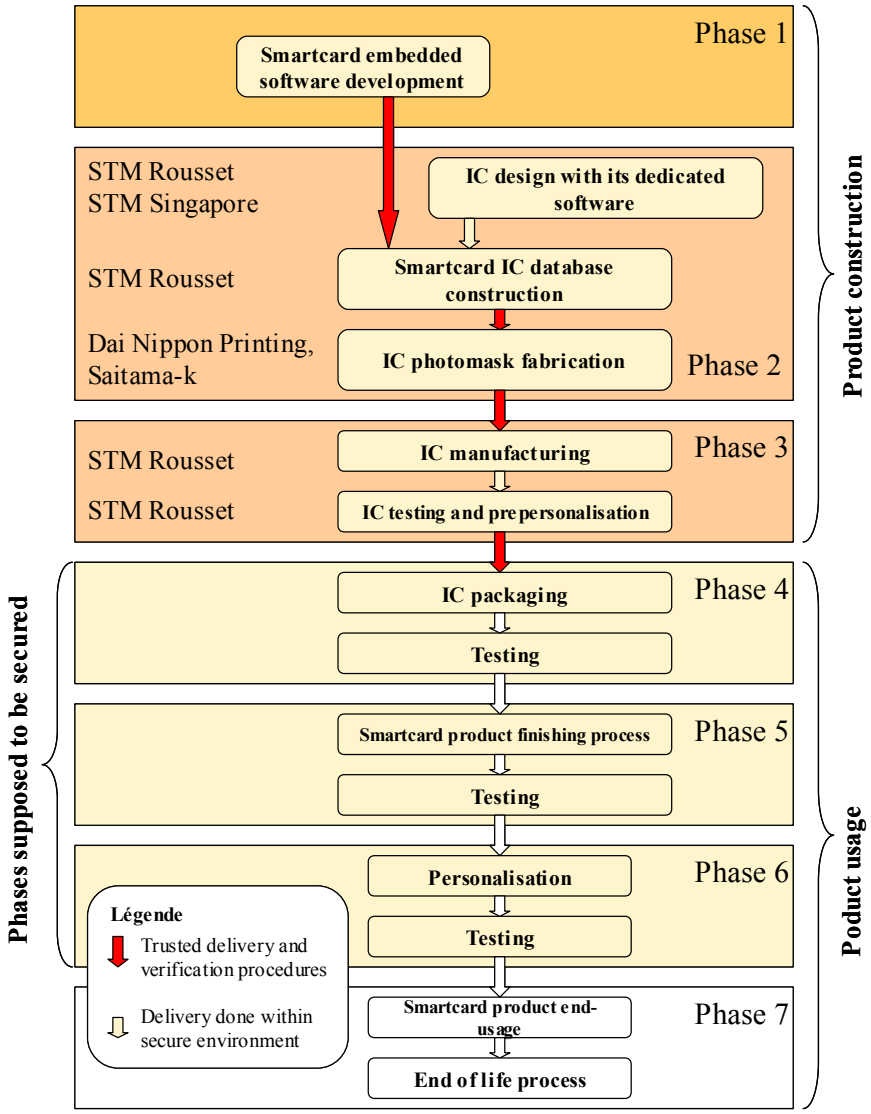

Figure 1 – Life cycle

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. The evaluation tasks related to the I/O interfaces included in the evaluation perimeter but dedicated to the TPM applications (LPC and GPIO) were limited to the documentary aspects.

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 evaluated product is similar to the ST19WR66D (certified in 2005 - [2005/39] reference). Thus, some of the current evaluation verdicts are based on the results of the related evaluation works but also on the surveillance works performed for the certificates released on other product of the same family.

2.2. Evaluation referential

The evaluation has been conducted in accordance with Common Criteria [CC], with 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 May to November 2005.

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 analysis of the procedures related to the product development and the environmental protection of the development sites has been performed in the frame of the ST1WR66 evaluation. The associated results are satisfactory (see [2005/39]).

The verification of the procedure application was performed during the Rousset and Singapore visits (see Appendix 1 and Appendix 2). The Saitama-Ken site was not visited since it has already been audited in the frame of another project (see [2003/18]).

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

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	[2005/39]
ACM_CAP.4	Generation support and acceptance procedures	Pass
ACM_SCP.3	Development tools CM coverage	[2005/39]
ALC class: Life-cycle support		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Pass
ALC_LCD.2	Standardised life-cycle model	[2005/39]
ALC_TAT.2	Compliance with development standards	[2005/39]

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). For the generic parts, work had already been completed within the framework of the ST19WR66 evaluation. The associated results thus were re-used mainly or completely (see [2005/39]).

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)
- 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	[2005/39]
ADV_FSP.3	Semiformal functional specification	[2005/39]
ADV_HLD.3	Semiformal high-level design	[2005/39]
ADV_INT.1	Modularity	[2005/39]
ADV_LLD.1	Descriptive low-level design	Pass
ADV_IMP.2	Implementation of the TSF	Pass
ADV_RCR.2	Semiformal correspondence demonstration	[2005/39]

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.

All flows related to the whole of the sites are evaluated and audited regularly within the framework of the various evaluations and re-evaluations of the STMicroelectronics products. It was done in particular during the ST19WR66 evaluation (see [2005/39]). The conclusions of associated work are satisfactory. Those flows were not the subject of evaluation for this project.

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	[2005/39]
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 administration and user guidance [GUIDES] are included in the ST19WR66 guidance which are already evaluated and certified (see [2005/39]). No re-evaluation was done.

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

AGD class: Guidances		**Verdicts**
AGD_ADM.1	Administrator guidance	[2005/39]
AGD_USR.1	User guidance	[2005/39]

2.7.6. Functional test evaluation

The ST19WP18 test plans are included in the ST19WR66 test plans which are already evaluated and certified (see [2005/39]).

Only the checking of the functional test results as well as the independent functional tests were carried out again for the microcontroller ST19WP18 (tests performed on the microcontroller ST19WP18 in revision E 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	[2005/39]
ATE_DPT.2	Testing: low level design	[2005/39]
ATE_FUN.1	Functional testing	Pass
ATE_IND.2	Independent testing – sample	Pass

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

2.7.7. Vulnerability assessment

Provided that the guidance documentation and the vulnerability assessment delivered by the developer have already been analysed within the framework of the ST19WR66 (see [2005/39]), some of results have been re-used.

Regarding the intrinsic resistance of the mechanisms, only the «test» and «issuer» configuration authentication and the random number generator functions (with metrics inspired from 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;
- « Level 3[1] » according to [FIPS 140-2] for the true random number generators.

The evaluator has performed its own independent analysis jointly to the ST19WR66 one (see [2005/39]). This analysis was completed by additional tests performed on the ST19WL34 product revision A, identified at §1.1 and provided to the ITSEF in a mode known as « open[2] ». Regarding the specific interfaces LPC and GPIO, the documentary analysis showed that they did not introduce any specific vulnerability. The security guidance must nevertheless be applied, as well as for the ISO7816-3 interface.

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	[2005/39]
AVA_MSU.3	Analysis and testing for insecure state	[2005/39]
AVA_SOF.1	Strength of TOE security function evaluation	[2005/39]
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] 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] mode that enables to load and execute a native code in EEPROM and also to disable the configurable security mechanisms

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 ST19WP18E 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.

3.3. European Recognition (SOG-IS)

This certificate is released in accordance with the provisions of the SOG-IS agreement [SOG-IS].

3.4. International Recognition (CC RA)

This certificate is released in accordance with the provisions of the CC RA [CC RA]. However, the following augmentations are not mutually recognized in accordance with provisions of the CC RA [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.

Appendix 1. Visit of the development site of the company STMicroelectronics in Rousset

The development and manufacturing site of the company STMicroelectronics located at Z.I. de Peynier-Rousset, 13106 Rousset Cedex, France, has been visited by the evaluator on February, 3rd and 4th 2005 in order to verify the application of the procedures related to the configuration management, life-cycle support and delivery, for the ST19WP18 product.

The procedures have been provided and analyzed in the following evaluation framework:
- ACM_AUT.1 and ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

A visit report [Visit] has been released by the evaluator.

Appendix 2. Visit of the development site of the company STMicroelectronics in Singapore

The development site of the company STMicroelectronics located at 28, Ang Mo Kio - Industrial park 2, SINGAPORE 569508, in SINGAPORE, has been visited by the evaluator on March, 10th 2005 in order to verify the application of the procedures related to the configuration management, life-cycle support and delivery, for the ST19WP18 product.

The procedures have been provided and analyzed in the following evaluation framework:
- ACM_AUT.1 and ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

A visit report [Visit] has been released by the evaluator.

Appendix 3. 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 4. References about the evaluated product

[2003/18]	Rapport de certification 2003/18 - Micro-circuit ST19WK08C, December 2003 SGDN/DCSSI
[2005/39]	Rapport de certification 2005/39 - Micro-circuit ST19WR66D, November 2005 SGDN/DCSSI
[CONF]	Product configuration list : • Configuration List ST19WP18E PRODUCT – K784A MASK SET Reference: CIT_CFGL_05_003_V1.0 STMicroelectronics List of the delivered materials by STMicroelectronics : • Documentation report (ST19WR66D, ST19WL34A and ST19WP18E), Reference : SMD_YQUEM_DR_05_002 V01.01 STMicroelectronics
[GUIDES]	The product user guidance documentation is the following : • ST19WP18 - Data Sheet, Reference : DS_19WP18/0505V1 STMicroelectronics • ST19X-19W - Security Application Manual, Reference : APM_19X-19W_SECU/0312 v1.7 STMicroelectronics • ST19X-ST19W - Security Application Manual - Addendum-3 to V1.7, Reference : AD3_APM_19x-19W_SECU1.7_0411 V1.0 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 Family Product - Autotest User Manual – TEST Configuration, Reference : AUM_0214_02 V1.5 STMicroelectronics • ST19X-19W - Manager - User Manual, Reference: UM_19X-19W_MG/0504V5 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 - ST19WP18E, Reference : YQM_ETR_WP18E_v2.0 Serma Technologies For the composite evaluation need, an exportable version of the report has been validated : • ETR-lite for composition - ST19WP18E, Reference : ETR lite ST19WP18E v1 Serma Technologies
[ST]	Referenced target for the evaluation : • ST19W generic security target, Reference : SCP_YQUEM_ST_03_001_V02.01 STMicroelectronics For the international recognition purpose, the following security target has been provided and validated in the evaluation frame : • ST19WP18 Security Target, Reference : SMD_ST19WP18_ST_05_001_V01.02 STMicroelectronics
[Visit]	Rousset site visit report • Annex E.5 of [ETR]. Singapore site visit report • Annex E.6 of [ETR].

Appendix 5. 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.
[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.
[AIS31]	Functionality classes and evaluation methodology for physical random number generator, Reference: AIS31 version 1, 25/09/2001, BSI.
[AIS34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004
[FIPS 140-2]	Security Requirements for Cryptographic Modules Reference: FIPS PUB-140-2:1999 NIST.

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