PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Certification report 2004/18 bis

ST19WL66B microcontroller

Paris, 20th August 2004

Courtesy Translation

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.

Contents

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated 18 April, 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 ITSEC and Common Criteria certification 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)

[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.

Thus, the Common Criteria Recognition Arrangement allow the recognition, by all signatory countries[1], 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 :

The international site concerning Common Criteria certification can be accessed at the following Internet address:

www.commoncriteria.org

[1] In November 2003, 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 and Turkey.

1. Evaluated product

1.1. Preamble

This certification report « 2004/18 bis » is similar to certification report « 2004/18 ». However, it includes the Security Target reference which enables the international recognition (cf. [CC RA]). The introduction has been updated accordingly. Paragraphs §3.7 and §3.8 have also been added.

1.2. Context

The ST19W platform micro-circuits are directly derived from the already certified ST19X platform: they feature the same security functions and security policies than those of the ST19X platform. However, they are manufactured by STMicroelectronics in a new CMOS technology.
The ST19WK08 microcontroller, representative of the ST19W platform, has already been evaluated and certified (cf. [2003/18]). Results from this evaluation were re-used for the ST19WL66B microcontroller evaluation.

1.3. Product identification

The evaluated product is the ST19WL66 (revision B) microcontroller (dedicated software XWB, maskset K730BCA) developed by STMicroelectronics. This product includes a test software (“autotest”) and a software library (system management, crypto library), stored in ROM memory

1.4. The developer

Several actors are in charge of the product development and manufacturing:
The ST19XL34P 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 photomask of the product and the product itself are manufactured by:

DAI NIPPON PRINTING CO., LTD

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

1.5. Evaluated product description

The evaluated product is ST19WL66B microcontroller 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. However, only the microcontroller is evaluated. The software applications are not in the scope of this evaluation.

1.5.1. Architecture

The ST19WL66B microcontroller is made up of:

- A Hardware part:
  - An 8-bit processing unit;
  - Memories : ROM (32KB for dedicated software : autotest and cryptographic librairies, 224KB de ROM for user), EEPROM (high density 66KB for program and data storage) and SRAM (6KB);
  - Security Modules : memory access control logic (MACL), clock generator, security administrator, power management, memories integrity control, I/O management (contact mode ISO 7816), unpredictable number generator, DES (E-DES implementation) et RSA co-processing units.
- A dedicated software is embedded in ROM which comprises test capabilities (« autotest ») and librairies (system library, cryptographic libraries). The evaluated microcontroller version is identified in §1.3.

A more detailed description of the application architecture is provided in documentation [HLD].

1.5.2. Life-cycle

Inspired from the PP/9806 [PP9806], the life-cycle of the product is the following:

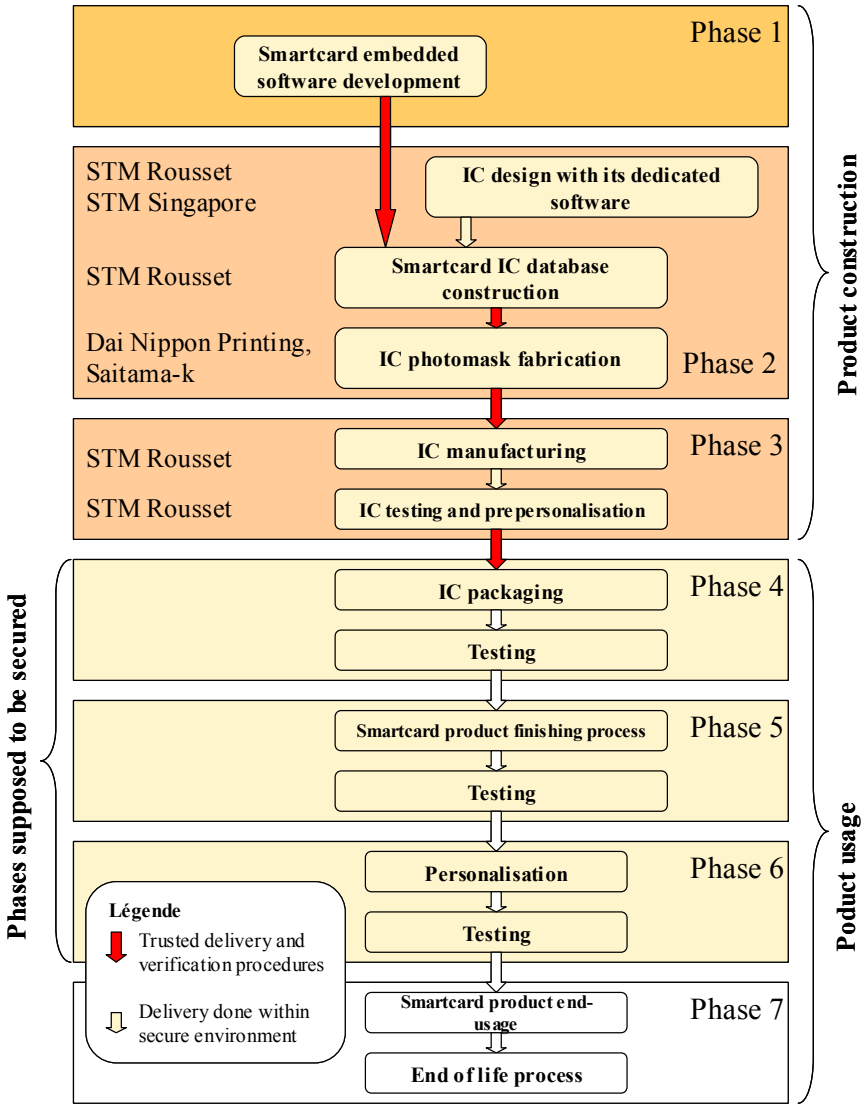

Figure 1 –Life-cycle

1.5.3. Evaluated product scope

This certification report presents the evaluation work related to the product and the dedicated software library identified in §1.3 and described in §1.5. Any other embedded application such as embedded applications intended specifically for the sake of the evaluation is not a 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).

1.6. Usage and administration

1.6.1. Usage

The evaluated product is not a product embedding a specific 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 (cf. document [CC_IC]) as well as all any other actor who intervene during the administration phases of the micro-module and of the card (Phase 4 to 6), including configuration and personalization of embedded applications.

In the ST19WL66B evaluation frame, these roles are defined in the security target [ST §5.3.1]: The users are defined as the people able to use the functionalities of the microcontroller, its software library and its application software. This definition includes any user using the product in "user" mode: The card issuer as well as the embedded software developer, the entity in charge of embedding and the entity in charge of inserting the card in its final system.

The security objectives on development and usage environment related to users are listed in the security target [ST] and reproduced in this document at §3.10.

1.6.2. Administration

The guide "The application of CC to integrated Circuits" [CC_IC] specifies the product administrators as the entities having an action on the product between phases 4 to 7 of the life cycle, which set-up (personalization) the final product. These operations are linked to the type of embedded application.

In the frame of the microcontroller, only the administration interfaces specific to the microcontroller are evaluated. Phases 4 to 6 called administrative, are covered by a hypothesis in the protection profile, which assumes that the operations linked to those phases are done in specific conditions that are not threatening the product security. Those conditions have not been evaluated.

In the ST19WL66B evaluation framework, the roles are defined with a slight difference. In the security target [ST, §5.3.1], the administrators are defined as:

- TEST administrator : Test administrator: he is in charge of testing the product in its development environment and of changing the product configuration from "test" mode to "issuer" mode (et in "user" mode if needed). This role is related to phase 3 of the life cycle (cf. §1.5.2) ;
- ISSUER administrators : in charge of carrying out a limited number of product tests, of personalizing, if needed, and of changing the product configuration from "issuer" to "user" mode. This role may intervene at several phases of the life cycle and can be plaid by the developer himself, the embedded software developer, the embedder or any entity taking action in one of the following phases of the product life cycle. This role is related to phases 3 to 6 of the life cycle.

Security objectives on development and operating environment related to administrators are listed in the Security Target [ST] and reproduced in this document at §3.10.

2. The evaluation

2.1. Evaluation facility

SERMA Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

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

Adresse électronique : m.dus@serma.com

The evaluation took place from March to May 2004.

2.2. Evaluation sponsor

STMicroelectronics

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

2.3. Evaluation referential

The evaluation has been conducted in accordance with Common Criteria [CC], with the evaluation methodology defined within the CEM manual [CEM], and with the whole finalised interpretations listed within evaluation reports.

2.4. Security target evaluation

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

All security functional requirements and security assurance requirements from the security target are taken from part 2 and part 3 of Common Criteria [CC].

The security target meets ASE class requirements.

2.5. Product evaluation

The evaluation consists in checking that the product and its documentation is compliant to security functional and assurance requirements defined in the security target [ST] of the product.

2.5.1. Product development

Considering the ST19WL66B being very similar to the ST19WK08C which has already been evaluated and certified (cf [2003/18]), the results of evaluation of the ST19WK08C have been partially reused. Only the implementation representation level has been fully re-evaluated.

ADV assurance class – development – defines requirements for the stepwise refinement of the product's security functions from its summary specification in the security target [ST] down to the actual implementation. Each of the resulting product's security function representations provide information to help the evaluator determine whether the functional requirements of the product have been met.

Documents associated to ADV class analysis shows that security functional requirements are correctly and completely refined into the different levels of the product representation (functional specifications (FSP), subsystems (HLD), modules (LLD) and implementation (IMP)), down to the implementation of its security functions.

Documents provided for ADV – development – class evaluation meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.2. Documentation

From the point of view of the evaluation, the administrators are in charge of the product testing when it is in "test" mode, and of the product personalization and testing when the product is in "issuer" mode (cf. §1.6.2).

From the point of view of evaluation, users are the people able to operate "user" functionalities of the product (including embedded software, cf. §1.6.1).

The ST19WL66B being very similar to the ST19WK08C which has already been evaluated and certified (cf [2003/18]), the results of previous evaluations have been partially reused.

User and administrator guides [USR] meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.3. Delivery and installation

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 reticule manufacturer.
- The delivery of the reticle 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 sites involved are identified at §1.4. All the flows related to the sites are evaluated and audited on regular basis in the frame of different evaluation and re-evaluation of STMicroelectronics products (see certification report [2003/18]). The conclusions of these works are satisfactory. Those flows have thus not been re-evaluated for this specific project.

The delivery procedures [DEL] are thus satisfying the requirements. They allow to identify the origin of delivery and to detect any modification of the information which would have been exchanged during the delivery.

The evaluated product is not embedding any specific application; it does not need any installation, generation or start-up specific phase.

Documents provided for ADO – Delivery and operation – class evaluation meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.4. Development environment

The microcontroller development involves all the sites identified at §1.4. The environment development of the involved sites are evaluated and audited on regular basis in the frame of different evaluation and re-evaluation of STMicroelectronics products (see certification report [2003/18]). The conclusions of these works are satisfactory. Those fluxes have then not been re-evaluated for this specific project.

The tasks related to Class ACM have been partially done, including the verification of the update of the configuration list [LGC].

The documents provided for the class ACM – configuration management – and ALC – life cycle support- fulfill the requirements of part 3 of common criteria [CC] in term of contents and presentation of content of evidence.

2.5.5. Functional testing

The ST19WL66B being very similar to the ST19WK08C which has already been evaluated and certified (cf [2003/18]), the results of previous evaluations have been partially reused. Independent tests have been carried out on the ST19WL66B platform identified at §1.3.

2.5.6. Vulnerability assessment

Vulnerabilities identified by the developer have been checked through an analysis and through penetration testing. The evaluator concludes that vulnerabilities identified by the developer are correctly covered.

The evaluator performed an independent vulnerability analysis that results do not point out any additional vulnerability.

The product within its operational environment is resistant to an attacker possessing **a high level attack potential**.

3. Conclusions of the evaluation

3.1. Evaluation technical report

The Evaluation Technical Report [RTE] describes results from the evaluation of the ST19WL66B microcontroller. Many results from the ST19WK08C microcontroller evaluation have been re-used. They are described in the ST19WK08C Evaluation Technical Report [RTE_WK08].

3.2. Evaluation level

The ST19WL66B microcontroller has been evaluated in compliance to Common Criteria [CC] and its methodology [CEM] at **level EAL4[1] augmented with following assurance components**, compliant to Common Criteria part 3:

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

Table 1 - Augmentations

For all these product evaluation level components, following verdicts have been issued:

ASE class	**Security Target evaluation**	
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
ACM class	**Configuration management**	
ACM_AUT.1	Partial CM automation	[2003/18]

[1] In Appendix 3, a table gives a brief description of existing Evaluation Assurance Levels (EAL) defined in Common Criteria [CC].

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

Table 2 – Components and their corresponding verdicts

3.3. Functional requirements

The product meets the following[1] security functional requirements [ST chapter 5] :

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

[1] In 0, we can find a complete table explaining the evaluated product security functional requirements (in French).

- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Partial elimination of illicit information flows (FDP_IFF.4)
- Basic internal transfer protection (FDP_ITT.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- User attribute definition (FIA_ATD.1)
- TSF Generation of secrets (FIA_SOS.2)
- User authentication before any action (FIA_UAU.2)
- User Identification before any action (FIA_UID.2)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- TOE Security Functions testing (FPT_TST.1)

3.4. Strength of functions

Only authentication functions have been subject to an estimation of their strength.

- Administrator authentication in « test » and « issuer » modes,
- Unpredictable Number Generation (with specific metric).

Strength of security functions meets the **high level (SOF-high)**.

3.5. Cryptographic mechanisms analysis

No cryptographic mechanism has been quoted during this evaluation (see annex 2).

3.6. Protection profile claim

The product is compliant to the security requirements of the PP/9806 protection profile [PP/9806].

3.7. European recognition (SOG-IS)

European mutual recognition applies up to EAL7. This certificate is released in accordance with the provisions of the SOG-IS agreement [SOG-IS].

3.8. International recognition (CC RA)

Mutual recognition applies to EAL4 and to the ALC_FLR family and the AMA class. 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 the provisions of the CC RA [CC RA]: ADV_IMP.2, ADV_FSP.3, ALC_DVS.2, AVA_VLA.4, AVA_CCA.1 et AVA_MSU.3 (Table 1).

3.9. Usage restrictions

Operational environment have to respect security objectives for the environment (§3.10), as well as recommendations within user guidance [USR].
Results from the evaluation are valid only for the configuration specified in this certification report.

3.10. Security objectives for the environment

Security objectives for the environment are the followings [ST § 4.2]:

Security objectives for the environment related to the system during its operating phase

Those security objectives concern the system where the microcontroller with its embedded software is used (Security Target extracts [ST §4.2.6])

- The communication between a product developed from the secured microcontroller and another product must be secured (In term of protocol and procedure);
- The system (terminal, communication) must guaranty the confidentiality and the integrity of the stored or processed sensitive data.

3.11. Result summary

The whole evaluation work performed by the evaluation centre is accepted by the certification body who testify that the ST19WL66B microcontroller identified in §1.3 and described in §1.5 of this report **is compliant** with requirements specified into the security target [ST]. The whole evaluation work and theirs results are described within the evaluation technical report [RTE].

Appendix 1. Site visit report concerning the development environment

None specific site vist has been performed during the evaluation of this application.

Appendix 2. Cryptographic mechanisms analysis

None specific cryptographic mechanism has been quoted during the evaluation of this application.

Appendix 3. Predefined Evaluation Assurance Levels IS 15408 or CC

Class	Family	Assurance components by Evaluation 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 and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
ADV class Developement	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 evaluted product

[2003/18]	Rapport de certification 2003/18 - Micro-circuit ST19WK08C, Décembre 2003 SGDN/DCSSI
[DEL]	LIVRAISON DE PRODUITS SMARTCARD A UN CLIENT ET RECEPTION DES RETOURS CLIENTS Référence : 7147367, revision B STMicroelectronics
[HLD]	▪ ST19W Generic High Level Design Référence : PDE_YQUEM_TS_03_001 v1.2 STMicroelectronics ▪ ST19W Generic High Level Design – Annexe B Référence : PDE_YQUEM_TS_03_004, v1.1 STMicroelectronics
[LGC]	Product configuration list : ▪ Configuration list for ST19WL66 product - K730BCA Mask Set Référence : PEN_YQUEM_CFGL_04_001 v1.1 STMicroelectronics List of delivered materials by STMicroelectronics : ▪ YQUEM evaluation – Documentation report (ST19WL66 and ST19WS04) Référence : SMD_YQUEM_DR_04_001 v1.1 ST Microelectronics
[PP9806]	Common Criteria for Information Technology Security Evaluation - Protection Profile : Smart Card Integrated Circuit Version 2.0, Issue September 1998. Certified by the French Certification Body under the number PP/9806. *Documentation released on the web site: www.ssi.gouv.fr*
[RTE]	Evaluation Technical Report - ST19WL66B (EAL4+ evaluation) Référence : YQM_WL66B_ETR v1.1 For the composite evaluation need, a exportable version of the report has been validated : ETR-lite for composition - ST19WL66B (EAL4+ evaluation) Référence : YQM_WL66B_ETR_lite v1.0
[RTE_WK08]	ST19WK08 Evaluation Technical Report (EAL4+ evaluation) Référence : YQM_WK08_ETR v1.2 Serma Technologies

[ST]	▪ ST19W Generic Security Target Référence : SCP_YQUEM_ST_03_001_V01.01 STMicroelectronics ▪ ST19WL66 Security Target Lite Référence : SMD_YQUEM_ST_04_002_V01.02 STMicroelectronics For the international recognition purpose, the following security target has been provided and validated in the evaluation frame: ▪ ST19WL66 - Security Target, Référence : SMD_ST19WL66_ST_04_001 v1.00 STMicroelectronics
[USR]	The product User guidances are the following : ▪ ST19WLxx - Datasheet Référence : DS_19WLxx/0301VP1 STMicroelectronics ▪ Manuals of security recommendations v1.7 Référence : APM_19X-19W_SECU/0312V1.7 STMicroelectronics ▪ ST19W - System ROM –Issuer configuration - user manual Référence : UM_19W_SR_I/0306VP2 STMicroelectronics ▪ Addendum au ST19W - System ROM –Issuer configuration - user manual Référence : AD_UM_19W_SR_I/0308V1.1 STMicroelectronics ▪ ST19X – 19W – System library User Manual Référence : UM_19X_19W_SYSLIB/0304V2 STMicroelectronics ▪ ST19X – Enhanced DES Library User Manual Référence : UM_19XV2_EDESLIB/0203V1.1 STMicroelectronics ▪ ST19X – User Manual – Cryptographic library lib4 v2.0 Référence : UM_19X_LIB4V2/0301V1.1 STMicroelectronics ▪ Card Manager Manuel Référence : UM_19X_19W_MG/0401 v3 STMicroelectronics

Appendix 5. References about certification

Decree number 2002-535 dated 18th april 2002 related to the security evaluations and certifications for information technology products and systems.	
Decree 2001-272 dated 30th march 2001- Decree for the application of the Civil Code article number 1316-4 related to the electronic signature.	
[CC]	Commun Criteria for the IT security evaluation: ▪ Part 1: Introduction and general model, august 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.
[CC_AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002
[CC_IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, Version 1.2, July 2000
[CEM]	IT Security evaluation Methodology: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[IS 15408]	Standard ISO/IEC 15408 :1999, comportant 3 documents : ▪ IS 15408–1: (Part 1) Introduction and general model ; ▪ IS 15408–2: (Part 2) Security functional requirements ; ▪ IS 15408–3: (Part 3) Security assurance requirements ;
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, may 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[MQ]	Certification Body Quality Manual Référence SGDN/DCSSI/SDR/MQ.01 Version 1.0 SGDN/DCSSI
[CER/P/01]	Certification for information technology products and systems. Référence CER/P/01.1 Version 1 SGDN/DCSSI

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
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr