PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report 2007/07

ST19NA18C secure microcontroller

Paris, 28th of March 2007

Courtesy Translation

SÉCURITÉ
Ti
CERTIFICATION

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. 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 evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed 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 a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

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
France

certification.dcssi@sgdn.pm.gouv.fr

Reproduction of this document without any change or cut is authorised.

Certification report reference	
2007/07	
Product name	
ST19NA18C secure microcontroller	
Product reference	
ST19NA18 revision C microcontroller (dedicated software ZSC, maskset K7L0A)	
Protection profile conformity	
PP/9806 – PP BSI-PP-002-2001	
Evaluation criteria and version	
Common Criteria version 2.3 **compliant with ISO 15408:2005**	
Evaluation level	
EAL 5 augmented **ALC_DVS.2, AVA_MSU.3, AVA_VLA.4**	
Developer	
STMicroelectronics **Smartcard IC division, ZI de Rousset, BP2, 13106 Rousset Cedex, France**	
Sponsor	
STMicroelectronics **Smartcard IC division, ZI de Rousset, BP2, 13106 Rousset Cedex, France**	
Evaluation facility	
Serma Technologies **30 avenue Gustave Eiffel, 33608 Pessac, France** **Phone: +33 (0)5 57 26 08 64, email : m.dus@serma.com**	
Recognition arrangements	
CCRA	**SOG-IS**
The product is recognised at EAL4 level.	

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 fulfil 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 are available on the Internet site www.ssi.gouv.fr.

Content

1.   The product

1.1.   Presentation of the product

The evaluated product is the ST19NA18 (revision C) microcontroller developed by STMicroelectronics. This product includes a software test ("Autotest") and a software library (system management, crypto library), stored in ROM memory.

The microcontroller aims to host one or several software applications and can be embedded in a plastic support to create a Smartcard with multiple possible usages (secure identity documents, 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.

1.2.   Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.

This security target is compliant to both [PP9806] and [PP0002] protection profiles.

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.
The certified version of the product can be identified by the following elements that can be checked with a microscope:
-   Die identification (maskset): K7L0A;
-   Dedicated software identification: ZSC;
-   Embedded software identification: this reference depends on the application embedded in ROM memory;
-   Manufacturing site identification: STMicroelectronics_4 (Rousset).

1.2.2. Security services

The product provides mainly the following security services:
-   Hardware initialisation & TOE attribute initialisation;
-   TOE configuration switching and control;
-   TOE logical integrity (including memory integrity);
-   Test of the TOE;
-   Administrators authentication;
-   Storage and Function Access Firewall;
-   Physical tampering security function (including attack & fault detection mechanisms);
-   Reaction to security events;
-   Unobservability;
-   Symmetric Key Cryptography Support;
-   Asymmetric Key Cryptography Support;
-   Random Number Generator.

1.2.3. Architecture

The ST19NA18C microcontroller is made up of:

- A Hardware part:
    - An 8-bit processing unit;
    - Memories: EEPROM (18KB with integrity control, for program and data storage), ROM (128KB for user, 32KB for dedicated software : autotest and cryptographic libraries) and RAM (4KB) ;
    - Security Modules: Memory Access Control Logic (MACL), clock generator, security administrator, power management, memories integrity control, fault detection mechanisms;
    - Functional Modules: 8-bits timers, I/O management in contact mode (IART ISO 7816-3), 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
    - Cryptographic libraries: DES (E-DES implementation), AES (E-AES implementation) and RSA which are included in the product security target.

1.2.4. Life cycle

1.2.5. Life cycle

The product's life cycle is organised as follow:
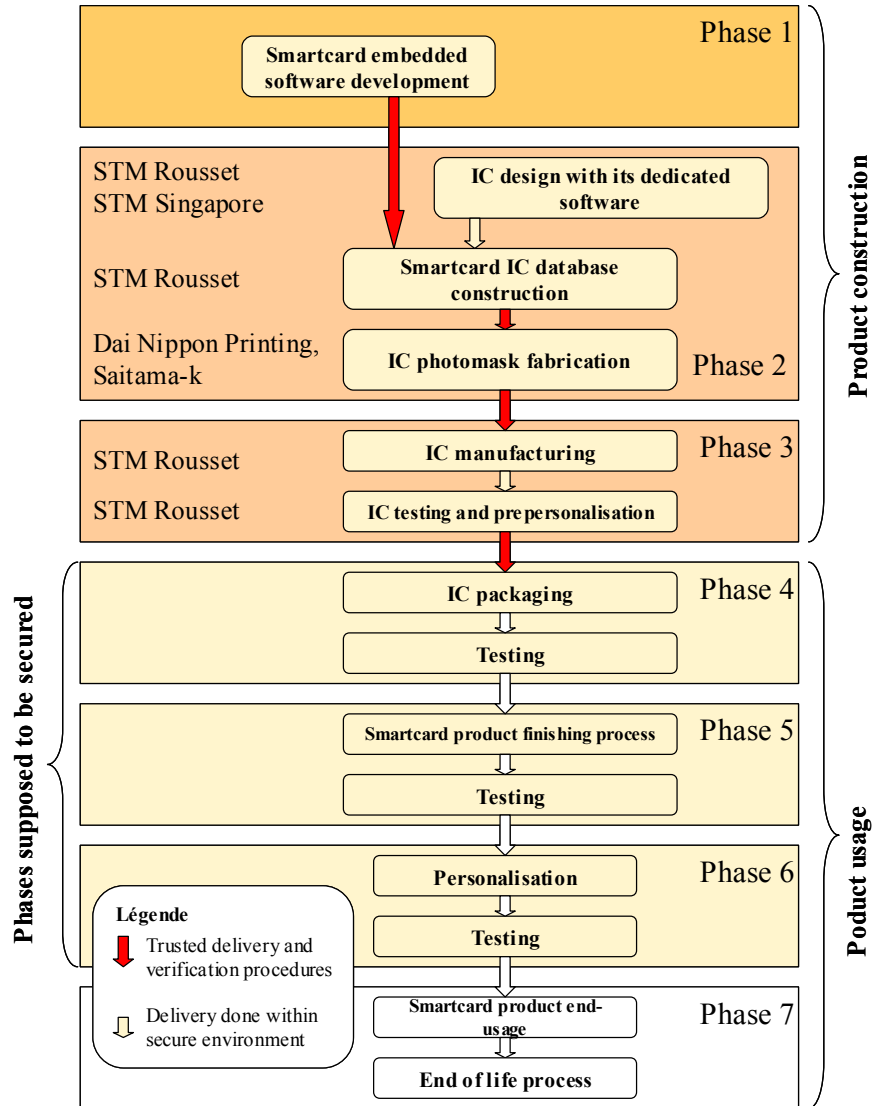

Figure 1 – Life cycle

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

5A Serangoon North Avenue 5,
Singapore 554574
Singapour

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

The product can be in one of its three possible configurations:
-   «Test» configuration: product configuration at the end of developer IC manufacturing. The product 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 product configuration is changed to "Issuer" before delivery to the next user, and the part cannot be reversed to the «test» configuration.
-   «Issuer» configuration: product 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 product 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 product 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 product functionalities are driven exclusively by the Embedded Software.

1.2.6. Evaluated configuration

This certification report presents the evaluation work related to the product and the dedicated software library identified in §1.1. 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).
For the evaluation needs, the product ST19NA18C was provided to the ITSEF with a dedicated test software (Card Manager) in a mode known as « open[1] ».

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC] and with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods consistent with [AIS34], validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CCIC] and [CCAP] guides have been applied.

2.2. Evaluation work

The evaluation relies on the evaluation results of the ST19NR66B product certified in 2006 under the reference 2006/27 (cf. [2006/27]).

The evaluation technical report [ETR], delivered to DCSSI the 19th of March 2007, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has not been analysed by DCSSI.

2.4. Random number generator analysis

The evaluation facility has evaluated the random number generator with the [AIS31] and [FIPS 140] methodology.
The generator reaches the class "P2 – *SOF-high*" according to [AIS31] and Level 3[1] according to [FIPS 140].

---

[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.

3. Certification

3.1. Conclusion

The evaluation identified in chapter 2 and described in the evaluation technical report [ETR], was carried out according to the current rules and standards, with the required competency and impartiality by a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product "ST19NA18C secure microcontroller" submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 5 augmented.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

This certificate provides a resistance assessment of the ST19NA18C 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 specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:
-   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. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

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

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The 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:

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by 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 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.
2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, The Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, United Kingdom and United States.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Name of the component
ACM Configuration management	ACM_AUT				1	1	2	2	1	Partial CM automation
	ACM_CAP	1	2	3	4	4	5	5	4	Configuration support and acceptance procedures
	ACM_SCP			1	2	3	3	3	3	Development tools CM coverage
ADO Delivery and operation	ADO_DEL		1	1	2	2	2	3	2	Detection of modification
	ADO_IGS	1	1	1	1	1	1	1	1	Installation, generation and start-up procedures
ADV Development	ADV_FSP	1	1	1	2	3	3	4	3	Semiformal functional specification
	ADV_HLD		1	2	2	3	4	5	3	Semiformal high-level design
	ADV_IMP				1	2	3	3	2	Implementation of the TSF
	ADV_INT					1	2	3	1	Modularity
	ADV_LLD				1	1	2	2	1	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	2	Semiformal correspondence demonstration
	ADV_SPM				1	3	3	3	3	Formal TOE security policy model
AGD Guidance	AGD_ADM	1	1	1	1	1	1	1	1	Administrator guidance
	AGD_USR	1	1	1	1	1	1	1	1	User guidance
ALC Life-cycle support	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	2	Standardised life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	2	Testing: low-level design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing – sample
AVA Vulnerability assessment	AVA_CCA					1	2	2	1	Covert channel analysis
	AVA_MSU			1	2	2	3	3	3	Analysis and testing of insecure states
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	4	Highly resistant

Annex 2. Evaluated product references

[2006/27]	Certification report 2006/27 – ST19NR66B secure microcontroller, 8 December 2006, SGDN/DCSSI

[ST]	Reference security target for the evaluation:
	- ST19NA18 Security Target,
	  Reference: SMD_ST19NA18_ST_06_001 V01.00
	  STMicroelectronics
	For the needs of publication, the following security target has been provided and validated in the evaluation:
	- ST19NA18 Security Target – Public version,
	  Reference: SMD_ST19NA18_ST_07_001 V01.01
	  STMicroelectronics

[ETR]	Evaluation technical report :
	- Evaluation Technical Report – ST19NA18C – (EAL5+ evaluation),
	  Reference: YQM_ETR_NA18C_v1.2
	  Serma Technologies
	For the needs of composite evaluation with this microcontroller a technical report for composition has been validated:
	- ETR Lite for Composition, ST19NA18C (EAL5+ evaluation)
	  Reference: YQUEM_ETR lite ST19NA18C_v1.1
	  Serma Technologies

[CONF]	Product configuration list:
	- Configuration List ST19NA18C PRODUCT,
	  Reference: SCP_ST19NA18C_CFGL_06_001 V01.03
	  STMicroelectronics
	List of the delivered materials by STMicroelectronics:
	- Yquem evaluation –Documentation report (ST19NA18C),
	  Reference: SMD_NA18_DR_06_001 V01.04
	  STMicroelectronics

[GUIDES]	The product user guidance documentation is the following:
	- ST19NA18 Smartcard MCU with MAP, IART, High Speed CPU Clock & 18 KBytes High Density EEPROM,
	  Reference: DS_19NA18/0702 Rev. 9
	  STMicroelectronics
	- ST19NA18 - Security Application Manual,
	  Reference: APM_19NA18_SECU/0702 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 - ST19W - System ROM –Issuer configuration - user manual addendum 2, Reference: AD2_UM_19W_SR_I/0702V1.0 STMicroelectronics - ST19N System Library V2 User Manual, Reference: Um_19N_SysLibV2/0610 Rev 3 STMicroelectronics - ST19X, ST19W and 19N EDES Library User Manual, Reference: UM_19X_EDESLIB/0605 Rev 2 STMicroelectronics - ST19N - Fast Cryptographic Library FastLIB4 – User Manual, Reference: UM_19N_FASTLIB4/0605 Rev 3 STMicroelectronics - Information Note, Reference: SE_IN_06_004 V1.01 STMicroelectronics - ST19W and ST19N AES Library - User Manual, Reference: UM_19W_19N_AES/0610 Rev 2 STMicroelectronics - AIS31 Compliant Random Numbers on ST19N Products - User Manual, Reference: UM_19N_AIS31_CRN/0702 V1 STMicroelectronics
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certified under the reference PP/9806.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified under the reference BSI-PP-0002-2001.*

Annex 3. Certification references

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 of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of CEM version 2.3 is identical to the international ISO/IEC 18045:2005.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[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.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004
[AIS31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25/09/2001, Bundesamt für Sicherheit in der Informationstechnik

[FIPS 140]	Security Requirements for Cryptographic Modules Reference: FIPS PUB-140-2:1999 NIST