Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification
Certification report
2006/26

ATMEL Secure Microcontroller AT90SC9618RCT rev. D

Paris, 14 December 2006

Courtesy Translation

SÉCURITÉ CERTIFICATION TI

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

Référence du rapport de certification — *Certification report reference*

2006/26

Nom du produit — *Product name*

ATMEL Secure Microcontroller AT90SC9618RCT rev. D

Référence/version du produit — *Product reference*

AT90SC9618RCT, reference AT58823 revision D, with Cryptographic software library Toolbox 3.x revision: 00.03.01.04.

Conformité à un profil de protection — *Protection profile conformity*

PP/9806

Critères d'évaluation et version — *Evaluation criteria and version*

Common Criteria version 2.2

Niveau d'évaluation — *Evaluation level*

EAL 4 augmented
ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeur — *Developer*

Atmel SmartCard ICs
Maxwell Building - Scottish Enterprise technology Park, East Kilbride,
Glasgow G75 0QR, Scotland

Commanditaire — *Sponsor*

Atmel SmartCard ICs
Maxwell Building - Scottish Enterprise technology Park, East Kilbride,
Glasgow G75 0QR, Scotland

Centre d'évaluation — *Evaluation facility*

CEA - LETI
17 rue des martyrs, 38054 Grenoble Cedex 9, France
Phone: +33 (0)4 38 78 40 87, email : cesti.leti@cea.fr

Recognition arrangements

CCRA — **SOG-IS**

IT Security Certified

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 secure microcontroller AT90SC9618RCT, reference AT58823 revision D, with Cryptographic software library Toolbox 3.x revision: 00.03.01.04, developed by Atmel SmartCard ICs.

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 (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. Technical references used in this report are identified in the security target.
This security target is compliant to [PP9806] protection profile.

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:

- Product name: AT90SC9618RCT, and product identification number: AT58823. This information can be checked using Serial number register SN_0, which content should be hexadecimal 0x22 (see [GUIDES], "AT90SC9618RCT Technical Data Sheet" section 21.1.1.),
- Silicon revision: D. Contrary to the specifications described in the technical datasheet, This information cannot be checked using Serial number register SN_1, which was not properly updated. So ATMEL proposed the following process:
  Customers will contact ATMEL with batch number information (Registers SN_2 to SN_8),
  ATMEL reply with required identification information (silicon revision).
- Toolbox revision: 00.03.01.04. This information can be checked using Tool-box 3.x "Selftest" command, which answer should be hexadecimal 0x00030104 (see [TBX], section 4.1).

The TOE can be physically identified by the mask numbers visible on the metal layer, and listed in the PML document (cf. [CONF]).

1.2.2. Security services

The product provides mainly the following security services:

- Test Mode Entry,
- Protected Test Memory Access,
- Test Mode Disable,

- TOE Testing,
- Data Error Detection,
- FireWall,
- Event Audit,
- Event Action,
- Unobservability,
- Cryptography,
- Package mode entry,
- Test Memory Access in Package Mode.

1.2.3. Architecture

The AT90SC9618RCT microcontroller is made up of:

- AVR Risk processing unit,
- 96Kb of program ROM memory, and 32Kb ROM memory dedicated to Atmel's Crypto Library,
- 18K bytes of EEPROM program/data memory including 128 bytes of One Time Programmable (OTP) memory and a 384-byte of bit-addressable area.
- 4K bytes of static RAM memory,
- a 32bit Checksum Accelerator,
- a CRC-16/32 peripheral,
- a Random Number Generator,
- a fast hardware DES/3DES peripheral,
- a 32bit crypto accelerator (AdvX) with its 32K-byte Crypto ROM that can be loaded with either the ATMEL Toolbox library (ATMEL ROM or ATMEL crypto ROM), or it can be loaded with the Customer Proprietary crypto library. The Atmel Toolbox software library allows fast cryptographic algorithm implementations (RSA, SHA-1, Prime Generation,...) on the AdvX.
- detectors which monitor voltage, frequency and temperature,
- a firewall that protects all memories, peripheral and IO register accesses,
- a power management system,
- logic peripherals including 2 timers, 1 serial port, an ISO7816 interface and an ISO7816 controller,
- a dedicated test structure that can be used only in test mode for production testing, and sawn before IC packaging.

1.2.4. Life cycle

The product life-cycle is the following:

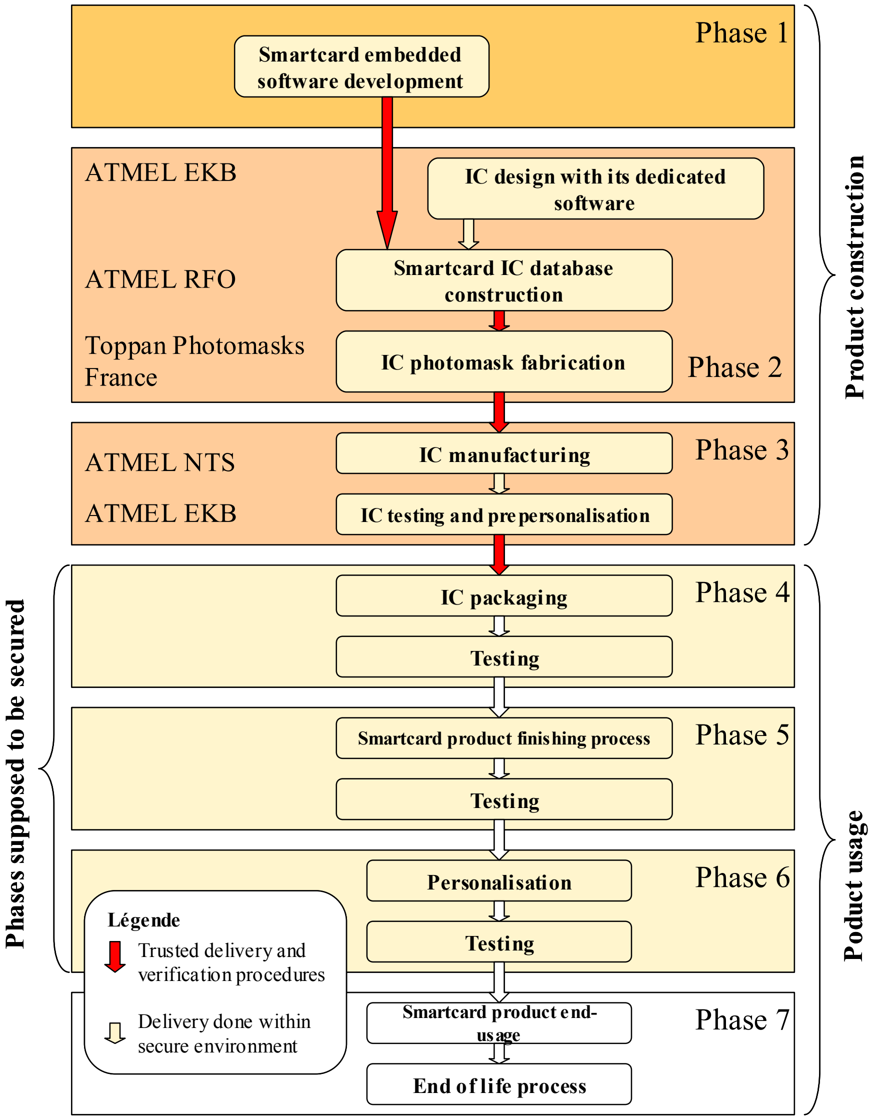
Phase 1
Smartcard embedded software development
ATMEL EKB
IC design with its dedicated software
ATMEL RFO
Smartcard IC database construction
Toppan Photomasks France
IC photomask fabrication
Phase 2
ATMEL NTS
IC manufacturing
Phase 3
ATMEL EKB
IC testing and prepersonalisation
IC packaging
Phase 4
Testing
Smartcard product finishing process
Phase 5
Testing
Personalisation
Phase 6
Testing
Smartcard product end-usage
Phase 7
End of life process
Product construction
Poduct usage
Phases supposed to be secured
Légende
Trusted delivery and verification procedures
Delivery done within secure environment

Figure 1 – standard IC life-cycle

The different sites impacted by the evaluation are listed bellow.

The product is designed and tested by:

Atmel East Kilbride

Maxwell Building
Scottish Enterprise technology Park
East Kilbride
Glasgow G75 0QR,
Scotland.

The database of the product is prepared by:

Atmel Rousset

Z.I. Rousset Peynier
13106 Rousset Cedex
France.

The photo masks of the product are manufactured by:

Toppan Photomasks France

224, bd John Kennedy
91100 Corbeil Essonnes
France.

The product is manufactured by:

Atmel North Tyneside

Middle Engine Lane
Silverlink business Park
North Tyneside, NE28 9N2
England.

The product can be in one of its three possible modes:

- "Test" mode: mode in which the microcontroller runs under the control of dedicated test software written to EEPROM via a test interface, and in conjunction with stimulus provided by an external test system. This mode is intended to be used solely by authorized development staff.
- "User" mode: mode, in which the microcontroller runs under control of the smartcard embedded software. It is intended that customers and end-users will always use the MCU in user mode.
- "Package" mode: this mode is similar to Test Mode for testing returns from Phases 4-7. Package mode runs a limited subset of test commands via a test interface, and in conjunction with stimulus provided by an external test system. This mode is intended to be used solely by authorized staff.

1.2.5. Evaluated configuration

This certification report applies to the microcontroller and software identified in §1.1 and described in §1.2.3. Any other software used for the evaluation are not part of the scope of certification.

With regard to the life-cycle, the evaluated product is the one at the end of its manufacturing phase (phase 3).

For the evaluation needs, the product was provided in to the ITSEF in a mode known as "open[1]".

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

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.2** [CC], with the Common Evaluation Methodology v2.2 [CEM].
For assurance componants above EAL4 level, the evaluation facility own evaluation methods validated by DCSSI have been used.

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

The evaluation relies on the evaluation results of the same product in revision B certified the 8 December 2005 under the reference 2005/43 (cf. [2005/43]).

2.2. Evaluation work

The evaluation technical report [RTE], delivered to DCSSI the 30 November 2006, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are “**pass**”.

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 “AT90SC9618RCT, reference AT58823 revision D, with Cryptographic software library Toolbox 3.x revision: 00.03.01.04” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level **EAL 4 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 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:

- Secure communication protocols and procedures shall be used between smartcard and terminal.
- The integrity and the confidentiality of sensitive data stored or handled by the system (terminals, communications....) shall be maintained.

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is released 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

[1] The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

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:

IT Security Certified

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA]. However, it is only recognised for EAL4 level.

The Common Criteria Recognition Arrangement allows the recognition, by 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:

[1] 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 4+	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	**2**	Problem tracking 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**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal 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**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-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		
	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

[2005/43]	Certification Report 2005/43 - ATMEL Microcontroller AT90SC9618RCT rev. B, 8 Decembre 2005, SGDN/DCSSI.
[ST]	Referenced security target for the evaluation : - Carbonear Security Target, Reference: Carbonear_ST_v1.5 ATMEL Public security target - AT90SC9618RCT Security Target Lite, Reference: TPG0097B_18Oct06 ATMEL
[RTE]	Complete Evaluation Technical Report : - Carbonear project – Evaluation technical report, Reference: LETI.CESTI.CAR.RTE.001 version 1.0 CEA/LETI - Carbonear Rev. D Project - Evaluation Technical Report (Addendum), Reference: LETI.CESTI.CAR.RTE.003 Version:1.0 CESTI LETI For composite evaluation purpose, a deliverable version has been validated: - Carbonear Evaluation technical report Lite, Reference: LETI.CESTI.CAR.RTE.002 version 1.0 CEA/LETI - Carbonear Rev. D Project - Evaluation Technical Report Lite (Addendum), Reference: LETI.CESTI.CAR.RTE.004 version 1.2 CESTI LETI
[CONF]	The configuration list is: - Carbonear Design Configuration List, Reference: Carbonear_DCL_V1.2_26Oct05 ATMEL - Carbonear Manufacturing configuration list, Reference: Carbonear_MCL_V1.3_19Jul06 ATMEL - Carbonear Pattern and Mask List, Reference: Carbonear_PML_13Nov06 ATMEL - Toolbox 3.x Crypto Toolbox Configuration List, Reference: TPR0150DX_06Sep05, ATMEL - Carbonear deliverables list, Reference: Carbonear EDL-07Dec06 ATMEL

[GUIDES]	Guidance of the product: - AT90SC CC AGD Interface, Reference: AT90SC_GUID_V1.4_05Jul05 ATMEL - AT90SC9618RCT Technical Data Sheet, Reference: TPR0145AX_22Sep04 ATMEL - AT90SC9618RCTErrata : Full NVM Erase, Ref. TPG0136AX_19Oct06 ATMEL - Toolbox 3.x on AT90SCxxxxC Family with AdvX, Reference: TPR0133CX-26Jul05 ATMEL - Efficient use of AdvX for Implementing Cryptographic Operations, Reference: TPR0142CX_14Jun05 ATMEL - Securing Cryptographic Operations on AT90SC Products with Toolbox 3.x, Reference: TPR0141CX_03Apr06, ATMEL - AdvX for AT90SC family, Reference: TPR0116BX. ATMEL - AT90SC Addressing Modes and Instruction Set, Reference: 1323C-03May04 ATMEL - Security Recommendations for AT90SC ASL4 Products, Reference: TPR0066G-05Jul05 ATMEL - Secured Hardware DES/TDES on AT90SC ASL4 Products, Reference: TPR0063FX-29Sep06 ATMEL - Generating unpredictable random numbers on the AT90SC family devices, Reference: 1573CX_SMIC_21mar03 ATMEL - Using the supervisor and user modes on the AT90SC ASL4 products, Reference: TPR0095A-11Mar03 ATMEL - Checksum Accelerator use on the AT90SC ASL4 products, Reference: TPR0065A-02Jul02 ATMEL - Wafer Saw Recommendations, Reference: TPG0079A_13Jun05 ATMEL

[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 scheme under the reference PP/9806.

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, 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 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.