PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/08

ATMEL Secure Microcontroller AT90SC9604RU rev. E

Paris, 14th of March 2008

Courtesy Translation

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.gouv.fr

Certification report reference

DCSSI-2008/08

Product name

ATMEL Secure Microcontroller AT90SC9604RU rev. E

Product reference

AT90SC9604RU, reference AT58U08 revision E

Protection profile conformity

PP/9806

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4 augmented

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

Developer

Atmel Secure Microcontroller Solutions

Maxwell Building - Scottish Enterprise technology Park

East Kilbride, G75 0QR – Scotland, United Kingdom

Sponsor

Atmel Secure Microcontroller Solutions

Maxwell Building - Scottish Enterprise technology Park

East Kilbride, G75 0QR – Scotland, United Kingdom

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

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 AT90SC9604RU, reference AT58U08 revision E developed by Atmel Secure Microcontroller Solutions.

This product belongs to the AVR ASL4 family developed by Atmel Secure Microcontroller Solutions**.**

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 [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: AT90SC9604RU, and product identification number: AT58U08. This information can be checked using Serial number register SN_0, which content should be hexadecimal 0x2F (Cf. [GUIDES], "AT90SC9604RU Datasheet" section 21.1.1).
- Silicon revision: E. This information can be checked using Serial number register SN_1, which content should be hexadecimal 0x04 **(**Cf. [GUIDES], "AT90SC9604RU Datasheet" section 21.1.2).
- The TOE can be physically identified by the mask numbers visible on the metal layer, and listed in the "Twister Pattern Mask List" 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 AT90SC9604RU microcontroller is made up of:

- AVR Risk processing unit,
- 96Kb of program ROM memory,
- 4Kb of EEPROM program/data memory including 64 bytes of One Time Programmable (OTP) memory and a 192-byte of bit-addressable area,
- 2Kb of static RAM memory,
- a Checksum Accelerator,
- a CRC-16 peripheral,
- a Random Number Generator,
- a fast hardware DES/3DES peripheral,
- detectors which monitor voltage, frequency and temperature,
- a firewall that protects all memories, peripheral and IO register accesses,
- a power management system (the microcontroller works under a voltage range from 2.7V to 5.5V),
- 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's life cycle is organised as follow:

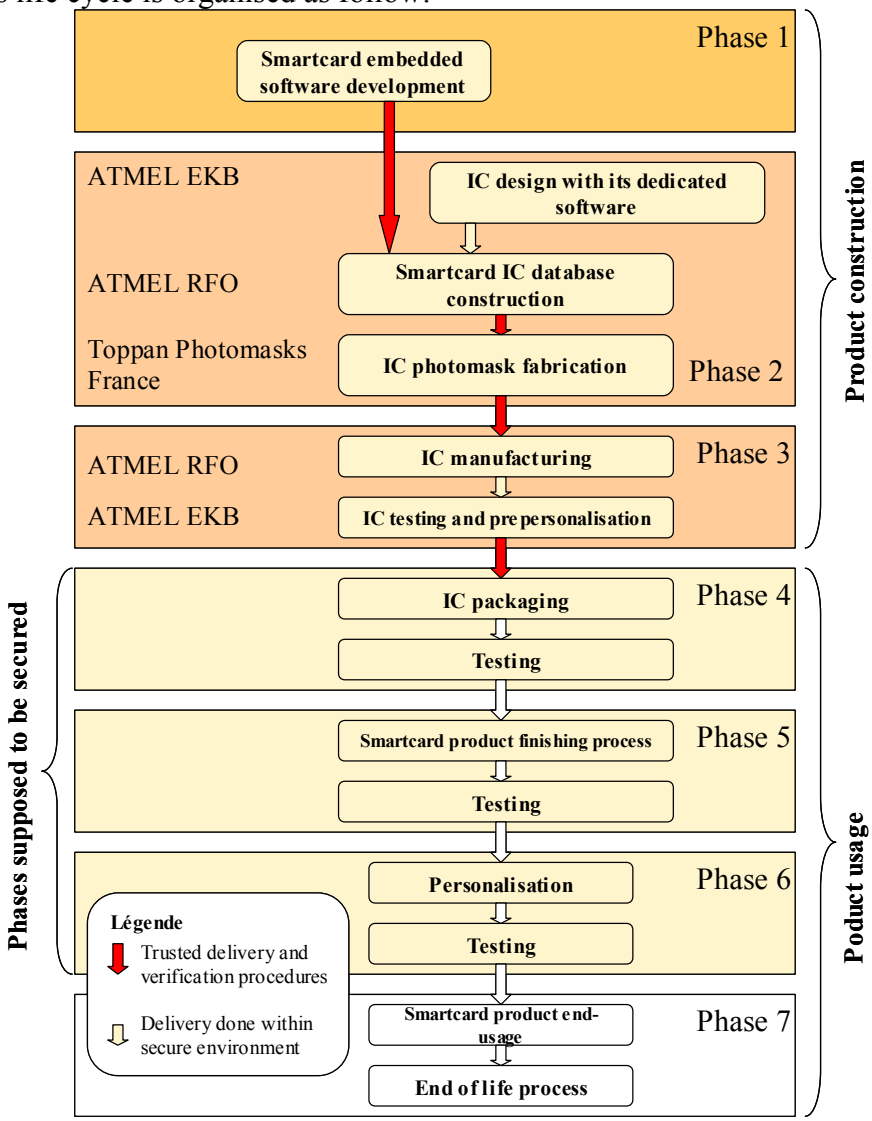

Figure 1 – standard IC life-cycle

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 and the manufacturing of the product are performed 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 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. After the testing activity, the tests interface is definitely deactivated by sawing the wafer and cannot be accessed any more.
- "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 microcontroller 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 only. 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 (Cf. [CC AP]).

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 [AIS 34], validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] guides have been applied.

2.2. Evaluation work

The evaluation relies on the evaluation results of the AT90SC25672RCT-USB rev. D product certified the 19th of December under the reference 2006/30 (Cf. [2006/30]).

The evaluation technical report [ETR], delivered to DCSSI the 21st of February 2008, 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.

3. Certification

3.1. Conclusion

The evaluation 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 "AT90SC9604RU, reference AT58U08 revision E" 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 AT90SC9604RU 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 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 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

[2006/30]	Certification report 2006/30 - ATMEL secure microcontroller AT90SC25672RCT-USB rev. D, 19th December 2006, SGDN/DCSSI
[ST]	Reference security target for the evaluation: - Targa Security Target, Reference: Targa_ST_V1.3 Atmel Secure Microcontroller Solutions For the needs of publication, the following security target has been provided and validated in the evaluation: - AT90SC9604RU Security Target Lite, Reference: TPG0142A_13Feb07 Atmel Secure Microcontroller Solutions
[ETR]	Evaluation technical report : - Targa Evaluation Technical Report, Reference: LETI.CESTI.TAR.RTE.001-v1.2-11/02/08 CESTI LETI For the needs of composite evaluation with this microcontroller a technical report for composition has been validated: - TARGA Project - Evaluation Technical Report – Lite, Référence : LETI.CESTI.TAR.ETR_LITE.001 Version 1.3, CESTI LETI
[CONF]	The configuration list is: - TARGA Design Configuration List, Reference: Targa_DCL_V1.2_03Sep07 Atmel Secure Microcontroller Solutions - TARGA Manufacturing Configuration List, Reference: TARGA_MCL_V1.1 Atmel Secure Microcontroller Solutions - AT90SC9604RU (Targa) Mask List Plan, Reference: Targa_PML_V2.0_11Apr07 Atmel Secure Microcontroller Solutions - Targa Deliverables list, Reference: Targa EDL_V1.15 Atmel Secure Microcontroller Solutions
[GUIDES]	Guidance of the product: - AT90SC CC AGD Interface, Reference: AT90SC_GUID_V1.4_05Jul05 Atmel Secure Microcontroller Solutions - AT90SC9604RU Technical Datasheet, Reference: TPR0241CX_14Aug07 Atmel Secure Microcontroller Solutions - AT90SC Addressing Modes and Instruction Set, Reference: 1323C-03May04 Atmel Secure Microcontroller Solutions

	- Security Recommendations for AT90SC ASL4 Products, Reference: TPR0066H_31Jan08 Atmel Secure Microcontroller Solutions - Secured Hardware DES/TDES on AT90SC ASL4 Products, Reference: TPR0063IX_05Dec07 Atmel Secure Microcontroller Solutions - Generating unpredictable random numbers on the AT90SC family devices, Reference: 1573CX_SMIC_21mar03 Atmel Secure Microcontroller Solutions - Using the Supervisor and User Modes on the AT90SC ASL4, Reference: TPR0095A-11Mar03 Atmel Secure Microcontroller Solutions - Using the Checksum Accelerator on AT90SC ASL4 products, Reference: TPR0065A-02Jul02 Atmel Secure Microcontroller Solutions - Wafer Saw Recommendations, Reference: TPG0079A_13Jun05 Atmel Secure Microcontroller Solutions
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certified by DCSSI 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, 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.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, 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 BSI (Bundesamt für Sicherheit in der Informationstechnik)