



PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

## **Certification Report 2007/03**

### **ATMEL Secure Microcontroller AT90SC6404RT rev. B**

*Paris, 9<sup>th</sup> of February 2007*

**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.pm.gouv.fr](mailto:certification.dcssi@sgdn.pm.gouv.fr)

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



Certification report reference

**2007/03**

Product name

**ATMEL Secure Microcontroller AT90SC6404RT rev. B**

Product reference

**AT90SC6404RT, reference AT58884 revision B**

Protection profile conformity

**PP/9806**

Evaluation criteria and version

**Common Criteria version 2.3**

Evaluation level

**EAL 5 augmented**  
**ALC\_DVS.2, AVA\_MSU.3, AVA\_VLA.4**

Developer(s)

**ATMEL Smart Card ICs**  
**Maxwell Building - Scottish Enterprise technology Park, East Kilbride,**  
**Glasgow G75 0QR, Scotland**

Sponsor

**ATMEL Smart Card ICs**  
**Maxwell Building - Scottish Enterprise technology Park, East Kilbride,**  
**Glasgow G75 0QR, Scotland**

Evaluation facility

**CEACI (Thales Security Systems – CNES)**  
**18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France**  
**Phone: +33 (0)5 62 88 28 01, email : ceaci@cnes.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](http://www.ssi.gouv.fr).



# Content

<b>1. THE PRODUCT .....</b>	<b>6</b>
1.1. PRESENTATION OF THE PRODUCT.....	6
1.2. EVALUATED PRODUCT DESCRIPTION .....	6
1.2.1. <i>Product identification</i> .....	6
1.2.2. <i>Security services</i> .....	6
1.2.3. <i>Architecture</i> .....	7
1.2.4. <i>Life cycle</i> .....	8
1.2.5. <i>Evaluated configuration</i> .....	9
<b>2. THE EVALUATION.....</b>	<b>10</b>
2.1. EVALUATION REFERENTIAL .....	10
2.2. EVALUATION WORK .....	10
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	10
<b>3. CERTIFICATION.....</b>	<b>11</b>
3.1. CONCLUSION .....	11
3.2. RESTRICTIONS.....	11
3.3. RECOGNITION OF THE CERTIFICATE.....	11
3.3.1. <i>European recognition (SOG-IS)</i> .....	11
3.3.2. <i>International common criteria recognition (CCRA)</i> .....	12
<b>ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....</b>	<b>13</b>
<b>ANNEX 2. EVALUATED PRODUCT REFERENCES .....</b>	<b>14</b>
<b>ANNEX 3. CERTIFICATION REFERENCES .....</b>	<b>16</b>

# 1. The product

## 1.1. Presentation of the product

The evaluated product is the secure microcontroller AT90SC6404RT, reference AT58884 revision B.

This product belongs to the AVR ASL4 family developed by Atmel Smart Card Ics.

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: AT90SC6404RT, and product identification number: AT58884. This information can be checked using Serial number register SN\_0, which content should be hexadecimal 0x1D (see [GUIDES], "AT90SC6404RT Technical Data Sheet" section 20.1.1.),
- Silicon revision: B. 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).
- The TOE can be physically identified by the mask numbers visible on the metal layer, and listed in the "Pattern and 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 AT90SC6404RT secure microcontroller is made up of:

- AVR Risk processing unit,
- 64Kb of program ROM memory,
- 4Kb of EEPROM program/data memory including 64 bytes of One Time Programmable (OTP) memory and a 192 bytes of bit-addressable area,
- 2Kb of static RAM memory,
- a 32bit Checksum Accelerator,
- a CRC-16/32 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 and an ISO7816 interface,
- 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:

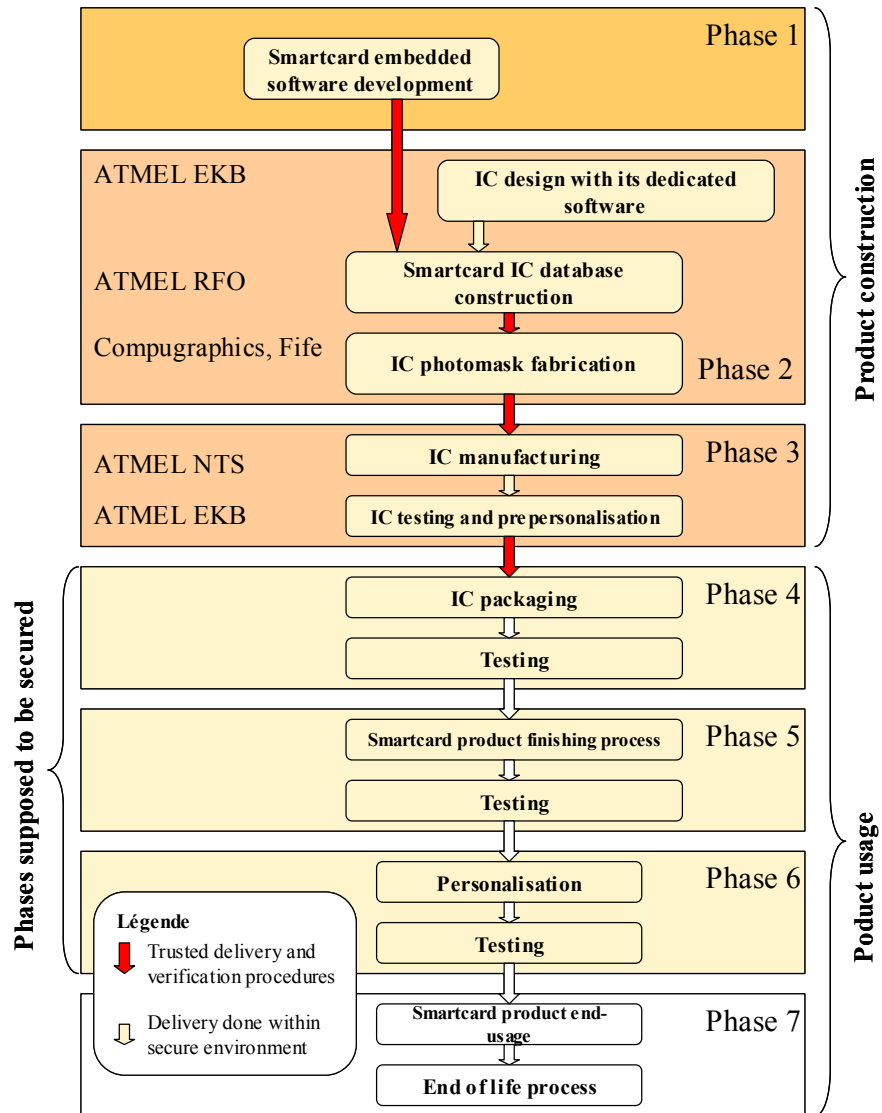


Figure 1 – standard IC life-cycle

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 is performed by:

**Atmel Rousset**

Z.I. Rousset Peynier  
13106 Rousset Cedex  
France.

The photo masks of the product are manufactured by:

**Compugraphics International Ltd**

Newark Road North  
Eastfield industrial Estate  
Glenrothes  
Fife, KY7 4NT,  
Scotland.

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 two 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.
- “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.

### ***1.2.5. Evaluated configuration***

This certification report applies only to the microcontroller with or without its cryptographic software library. Any other software used for the evaluation is 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<sup>1</sup>”.

---

<sup>1</sup> 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 2.3** [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 ATMEL Secure Microcontroller AT90SC6404RT rev. I, certified the 8 September 2006 under the reference 2006/14 (cf. [2006/14]).

The evaluation technical report [ETR], delivered to DCSSI the 7<sup>th</sup> of February 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.



## 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 “ATMEL Secure Microcontroller AT90SC6404RT rev. B” 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 AT90SC6404RT 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<sup>1</sup>, of ITSEC and Common Criteria certificates. The

---

<sup>1</sup> The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, 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:



### ***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<sup>1</sup>, 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:



---

<sup>1</sup> 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

[2006/14]	Certification report 2006/14 - ATMEL Secure Microcontroller AT90SC6404RT rev. I, 8 September 2006, SGDN/DCSSI
[ST]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> <li>- Pollux Security target, Reference: Pollux_ST_V2.5_13Nov06 ATMEL Smart Card ICs</li> </ul> <p>For the needs of publication, the following security target has been provided and validated in the evaluation:</p> <ul style="list-style-type: none"> <li>- AT90SC6404RT Security Target Lite – EAL5+, Reference: TPG0130B_10Jan07 ATMEL Smart Card ICs</li> </ul>
[ETR]	<p>Evaluation technical report :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report - Project: Pollux5 rev B, Reference: POB_ETR_V1.0 CEACI</li> </ul> <p>For the needs of composite evaluation with this microcontroller a technical report for composition has been validated:</p> <ul style="list-style-type: none"> <li>- ETR LITE for composition - ATMEL AT90SC6404RT MCU Device (AT58884) Rev: B, Référence : POB_ETR_Lite_V1.0 CEACI</li> </ul>
[CONF]	<p>The configuration list is:</p> <ul style="list-style-type: none"> <li>- Pollux Design Configuration List, Reference: Pollux_DCL_V3.1_17Jul06, ATMEL Smart Card ICs</li> <li>- Pollux Manufacturing Configuration List, Reference: Pollux_MCL_V3.1_17Jul06, ATMEL Smart Card ICs</li> <li>- Pollux Pattern &amp; Mask List, Reference: Pollux_PML_RevB_14Nov06, ATMEL Smart Card ICs</li> <li>- AT90SC Development Tools Configuration List, Reference: AT90SC_DTCL_V1.1_13Dec05 ATMEL Smart Card ICs</li> <li>- Pollux Deliverables List, Reference: Pollux EAL5 EDL_05Feb07, ATMEL Smart Card ICs</li> </ul>
[GUIDES]	<p>Guidance of the product:</p> <ul style="list-style-type: none"> <li>- AT90SC AGD Interface Document, Reference: AT90SC_AGD_V2.0_22Sep05, ATMEL Smart Card Ics</li> </ul>



	<ul style="list-style-type: none"> <li>- AT90SC6404RT Technical Data Sheet, Reference: TPR0125A-26Feb04 ATMEL Smart Card Ics</li> <li>- Errata Sheet AT90SC6404RT Rev I - Full NVM Erase, Reference: TPR0191 AX-SMIC, ATMEL Smart Card Ics</li> <li>- Atmel AT90SC Addressing Modes and Instruction Set, Reference: 1323C-03May04 ATMEL Smart Card Ics</li> <li>- Security Recommendations for AT90SC ASL4 Products, Reference: TPR0066G-05Jul05 ATMEL Smart Card ICs</li> <li>- Generating unpredictable random numbers on the AT90SC family devices, Reference: 1573CX_SMIC_21mar03 ATMEL Smart Card ICs</li> <li>- Using the supervisor and user modes on the AT90SC ASL4 products, Reference: TPR0095A-11Mar03 ATMEL Smart Card Ics</li> <li>- Secured Hardware DES/TDES on AT90SC ASL4 Products, Reference: TPR0063E-05Aug04 ATMEL Smart Card Ics</li> <li>- Checksum Accelerator use on the AT90SC ASL4 products, Reference: TPR0065A-02Jul02 ATMEL Smart Card Ics</li> <li>- POLLUX Wafer Saw Recommendation, Reference: Pollux_WSR_V1.0, 14Jun04 ATMEL Smart Card Ics</li> </ul>
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. <i>Certified under the reference PP/9806.</i>

### Annex 3. Certification references

Decree number 2002-535 dated 18 <sup>th</sup> 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