Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/03

ATMEL Cryptographic Toolbox 00.03.01.07 on the AT90SC Family of devices

Paris, 20th of February 2008

Courtesy Translation

SÉCURITÉ 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.gouv.fr

Certification report reference

DCSSI-2008/03

Product name

ATMEL Cryptographic Toolbox 00.03.01.07 on the AT90SC Family of devices

Product reference

Revision: 00.03.01.07

Protection profile conformity

None

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

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

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.

Content

1. The product

1.1. Presentation of the product

The evaluated product is the ATMEL Cryptographic Toolbox version 00.03.01.07 on the AT90SC Family of devices, developed by ATMEL Secure Microcontroller Solutions.

The product is the Cryptographic Software part of the AT90SC microcontrollers family that allows fast cryptographic algorithm implementations on the hardware AT90SC.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.
The security target is built in order to be compatible with the [PP0002] so that reuse or composition with a microcontroller including the toolbox and compliant to [PP0002] is possible.

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.
The certified version of the product can be identified using the "Selftest()" command, that should send back the identifier: "07 01 03 00".

1.2.2. Security services

The product provides the following cryptographic security services:

- Hash Function;
- RSA Without CRT Function;
- RSA With CRT Function;
- Prime/Test Generation;
- ECDSA Function;
- Elliptic Curve Point Addition;
- Elliptic Curve Point Doubling;
- Elliptic Curve Point Multiplication;
- Self test.

1.2.3. Architecture

The ATMEL Cryptographic Toolbox is a software library that allows fast cryptographic algorithm implementations (RSA, SHA-1, ECC, Prime Generation, …) on the hardware AT90SC. The Toolbox provides software cryptographic primitives to ease the customer proprietary software implementation of these algorithms (full multiply, square, partial multiply, division) as well as DSA and EC-DSA data signature.

This piece of software is to be embedded within smartcard based on AT90SC family of microcontroller. The Toolbox is merged with the Smartcard embedded software in Phase 2 of the life cycle (see §1.2.4).

1.2.4. Life cycle

The product's life cycle is organised as follow:

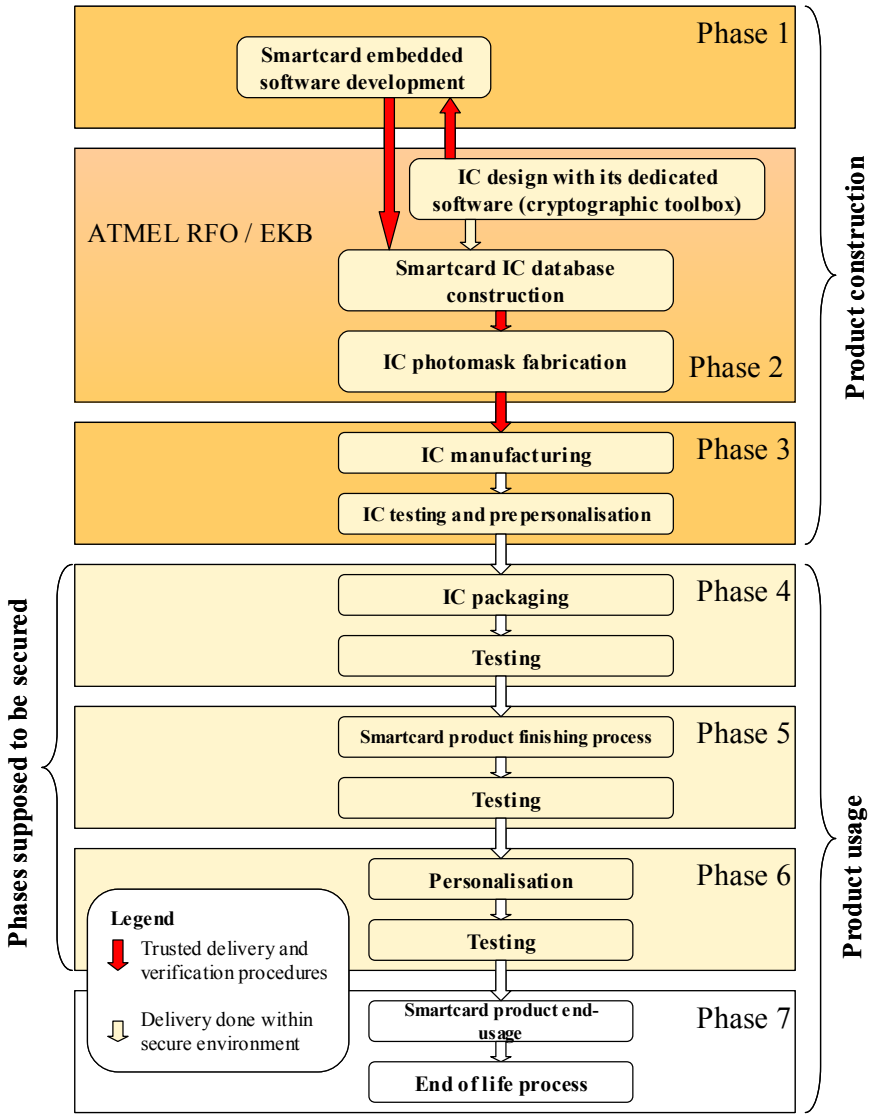

Figure 1 – standard IC life-cycle

The cryptographic toolbox is designed and tested by:

Atmel Rousset

Z.I. Rousset Peynier
13106 Rousset Cedex
France.

The cryptographic toolbox is merged with the software application by:

Atmel East Kilbride

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

The other phases of production are not within the scope of this evaluation.

1.2.5. Evaluated configuration

The toolbox can be compiled in two different modes:

- "Test" mode: mode that allows having an explicit test of all parameters during the development phase. This mode provide the developers of OS with a way to analyse the state of the parameter memory area (Advx Ram…) during their developments;
- "Release" mode: mode that allows executing quickly the code, which is more interesting for the end-user.

The evaluated configuration is the "release" mode.

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 technical report [ETR], delivered to DCSSI the 21st of December 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 evaluated product provides the cryptographic services identified §1.2.2 of this report.
As these services do not concur to the products security they cannot be analysed from a cryptographic point of view; their robustness depends on the way they are used by the application that uses the evaluated library.

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 ATMEL Cryptographic Toolbox version 00.03.01.07 on the AT90SC Family of devices, 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 Cryptographic Toolbox to a set of attacks that remains generic due to the missing of any specific embedded application. Therefore, the security of a final product based on the evaluated toolbox would only be assessed through the final product evaluation, which could be performed on the basis of the current evaluation results.

The developers using the certified product shall respect the operational environmental security objectives summarized in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- To ensure that the toolbox is used in a secure manner the smartcard embedded software shall be designed so that the requirements from the following documents are met:
  - Toolbox guidance [GUIDES];
  - Findings of the toolbox ETR for composition [ETR-Lite] relevant for the smartcard embedded software.
- Security relevant user data (especially cryptographic keys) are treated by the smartcard embedded software as required by the security needs of the specific application context;
- The security of the hardware platform on which the toolbox is loaded, must be of a sufficient quality to fully protect the toolbox and its assets. The security of the hardware platform is especially relevant when taking into account the RNG used in conjunction with the toolbox to produce cryptographic keys. The hardware platform random number generator must be tested against a recognised quality metric.

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 Republic of Korea, Malaysia, the Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the 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

[ST]	Reference security target for the evaluation: - Atmel Toolbox 00.03.01.07 on the AT90SC Family of devices - Security Target, Reference: TBX_00.03.01.xx_ST_V1.5_05Oct07 Atmel Secure Microcontroller Solutions For the needs of publication, the following security target has been provided and validated in the evaluation: - Atmel Toolbox 00.03.01.07 on the AT90SC Family of devices - Security Target Lite, Reference: TPG0159A_05Oct07 Atmel Secure Microcontroller Solutions
[ETR]	Evaluation Technical Report - Project: Toolbox 7, Reference: TBX_ETR_V2.0 CEACI
[ETR-Lite]	For the needs of composite evaluation with this microcontroller a technical report for composition has been validated: - ETR for composite evaluation – Toolbox 7, Reference: TBX_ETR_Lite v1.0 CEACI
[CONF]	The configuration list is made of: - Crypto Library Configuration List Library Version 00.03.01.07, Reference: TPR0150FX_01Oct07 Atmel Secure Microcontroller Solutions - TBX7 deliverables list, Reference: TBX_00.03.01.xx_EDL_09Oct07 Atmel Secure Microcontroller Solutions
[GUIDES]	Guidance of the product: - Toolbox 3.x on AT90SCxxxxC Family with AdvX™, Reference: TPR0133DX_01Aug06 Atmel Secure Microcontroller Solutions - Securing Cryptographic Operations on AT90SC Products with Toolbox 3x, Reference: TPR0141EX_14Aug07 Atmel Secure Microcontroller Solutions - Toolbox 00.03.01.xx Errata, Reference: TPR0163DX_10Jul07 Atmel Secure Microcontroller Solutions
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) 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, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2007-04-001 version 2.3, revision 1, April 2007.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1 September 2007
[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.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.10, 14th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR

[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)