PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/22

Card ASEPcos-CNS/CIE: AT90SC12872RCFT microcontroller embedding the software ASEPcos-CNS/CIE with Digital Signature Application

Paris, 28th of July 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-2008/22

Product name

Card ASEPcos-CNS/CIE: AT90SC12872RCFT microcontroller embedding the software ASEPcos-CNS/CIE with Digital Signature Application

Product reference

ASEPCOS Version 1.70 Build 001 on AT90SC12872RCFT reference AT58803 rev. M with Toolbox Version: 00.03.01.07

Protection profile conformity

Protection Profile - Secure Signature-Creation Device Type 2 Version: 1.04

Protection Profile - Secure Signature-Creation Device Type 3 Version: 1.05

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4 augmented

AVA_MSU.3, AVA_VLA.4

Developers

Athena Smartcard Solutions, Inc.

Regus House, 10 Lochside Place, Edinburgh Park, Edinburgh, EH12 9RG, Scotland, United Kingdom

ATMEL Secure Products Division

Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR - Scotland, United Kingdom

Sponsor

Athena Smartcard Solutions, Inc.

1-14-16, Motoyokoyama-cho,
Hachioji-shi, Tokyo, 192-0063, Japan

Evaluation facility

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Phone: +33 (0)5 61 28 16 51, email : ceaci@cnes.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 smart card ASEPcos-CNS/CIE, consisting of the AT90SC12872RCFT rev. M microcontroller with its software library Toolbox version: 00.03.01.07, developed by ATMEL Secure Products Division, and embedding the software "ASEPcos" with Digital Signature Application "CNS/CIE", developed by Athena Smartcard Solutions, Inc.. The reference of the software embedded in ROM memory is "ASEPcos-CNS/CIE version 1.70 Build 001".

The product is a smart card is to be used as a secure signature-creation device (SSCD) of type 2 and 3.

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 "Secure Signature-Creation Device Type 2 Version: 1.04" protection profile (cf. [PP0005]) and "Secure Signature-Creation Device Type 3 Version: 1.05" protection profile (cf. [PP0006]).

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 several elements, using the "Get Data" command, among which:

- The operating system ASEPcos with Digital Signature Application "CNS/CIE", version 1.70 Build 001, identified by:
  - Operating system identifier;
  - Operating system version number;
  - Operating system build number.
- The microcontroller: AT90SC12872RCFT rev. M, identified by:
  - IC version;
  - IC serial number;
  - Cryptographic library (toolbox) version.

The assigned values for these identifiers are defined in the user and administrator guidance (Cf. [GUIDES]).

1.2.2. Security services

The ASEPcos-CNS/CIE product enforces the security functions required for digital signature and supports usage only through secure trusted communication channels. The application implements a Secure Signature Creation Device (SSCD) which allows the generation and importation of signature creation data (SCD) and of signature verification data (SVD) and the

creation of qualified electronic signatures. The TOE protects the SCD and ensures that only an authorized Signatory can use it.

1.2.3. Architecture

The product is a smartcard that consists of:

- The microcontroller "AT90SC12872RCFT rev. M" with its software cryptographic library;
- The ASEPcos operating system;
- The application related to digital signature;
- Other command outside the scope of the evaluation.

The architecture of the product is summarised in the following picture:

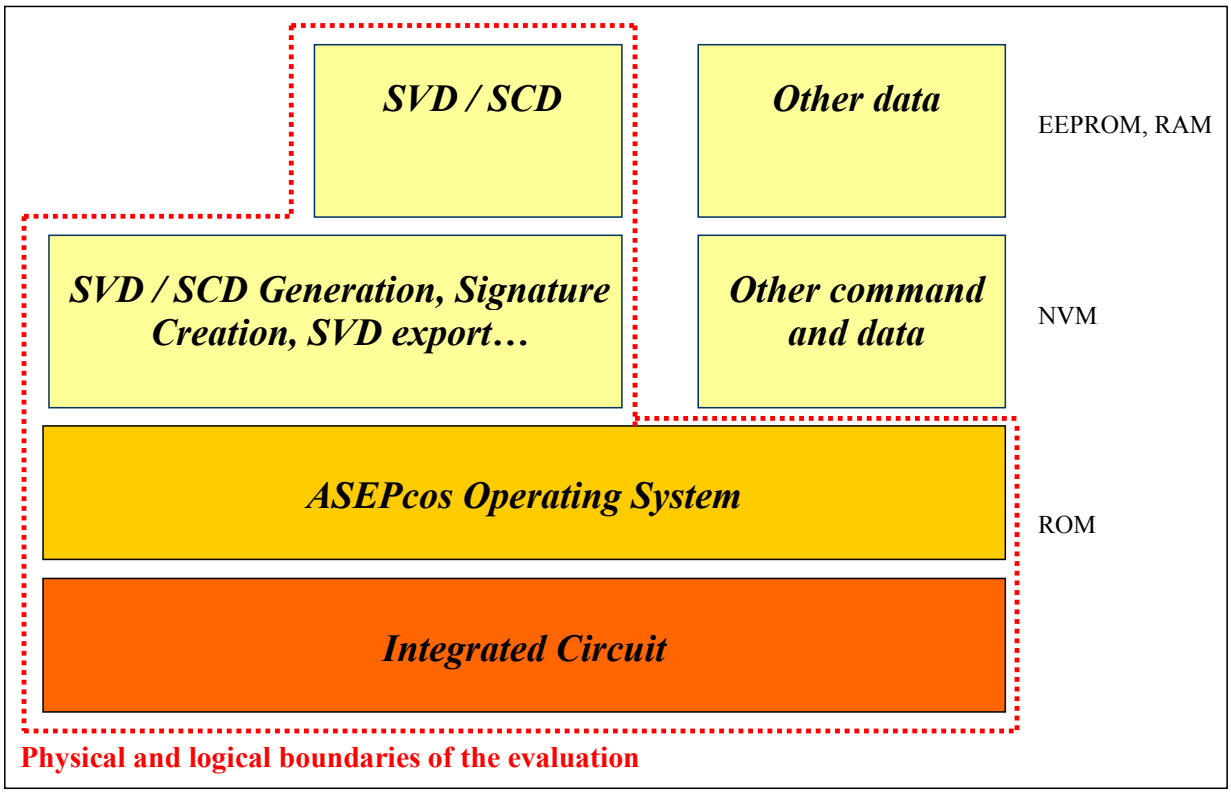

Figure 1 – Architecture of the product

1.2.4. Life cycle

The product's life cycle is organised as follow:

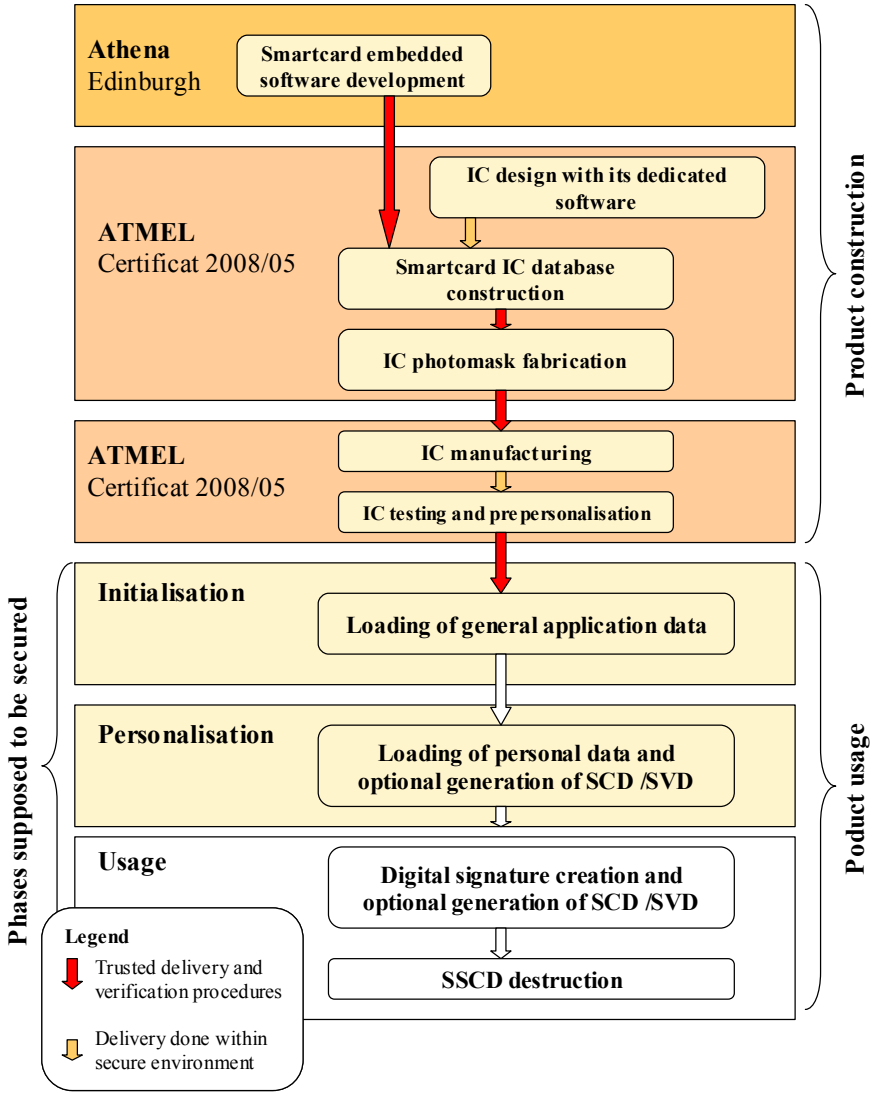

Figure 2 – Life cycle of the product

The embedded software was developed on the following site:

Athena Smartcard Solutions

Regus House, 10 Lochside Place, Edinburgh Park,
Edinburgh, EH12 9RG,
Scotland, United Kingdom

The microcontroller and its cryptographic software library were developed by Atmel Secure Products Division:

Atmel Secure Products Division

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

1.2.5. Evaluated configuration

The certificate applies to the following functionalities:

- Access Control,
- Identification and Authentication,
- Signature Creation,
- Secure Messaging,
- Crypto,
- Protection.

With regard to the life cycle, the evaluated product is the product that comes out the manufacturing, test and pre-personalization phase.

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 has been performed according to the composition scheme as defined in the guide [COMP] in order to assess that no weakness is introduced from the integration of the software in the microcontroller already certified.
Therefore, the results of the evaluation of the microcontroller "AT90SC12872RCFT rev M" at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [PP9806] protection profile, have been used. This microcontroller has been certified the 27th of February 2008 under the reference DCSSI-2008/05 (cf. (2008/05]).

The evaluation relies on the evaluation results of the ASEPcos-CNS/CIE product in version 1.60, certified the 8th of November 2007 under the reference DCSSI-2007/22 (cf. [2007/22]).

The evaluation technical report [ETR], delivered to DCSSI the 11th of July 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 for 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 "Card ASEPcos-CNS/CIE: AT90SC12872RCFT microcontroller embedding the software ASEPcos-CNS/CIE with Digital Signature Application" 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.

The user of the certified product shall respect the operational environmental security objectives summarized specified in the security target [ST] chapter 4.2 and shall respect the recommendations in the guidance [GUIDES].

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:

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

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

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	**1**	Subset of the 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	**1**	Indentification 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

[2007/22]	Certification Report DCSSI-2007/22 - Card ASEPcos-CNS/CIE: AT90SC144144CT microcontroller embedding the software ASEPcos-CNS/CIE with Digital Signature Application, 8th of November 2007, SGDN/DCSSI
[2008/05]	Certification Report DCSSI-2008/05 - ATMEL Secure Microcontroller AT90SC12872RCFT / AT90SC12836RCFT rev. M, 27th of February 2008, SGDN/DCSSI
[ST]	Reference security target for the evaluation: - ASEPCOS-CNS/CIE ROM Security Target, Version 2.1, 25 March 08, Athena Smartcard Solution For the needs of publication, the following security target has been provided and validated in the evaluation: - ASEPCOS-CNS/CIE ROM Public Security Target, Version 1.0, 18 July 08 Athena Smartcard Solution
[ETR]	Evaluation Technical Report - Project: AURORA_ROM, Reference: ARO_ETR_v2.0, CEACI
[CONF]	The configuration list is made of the following documents: - ASEPcos-CNS/CIE (ROM) Source Configuration List,, Version 1.2, 10 Jan. 08 Athena Smartcard Solutions - ASEPcos-CNS/CIE (ROM) Scripts Configuration List, Version 1.2, 10 Jan. 08 Athena Smartcard Solutions - ASEPcos-CNS/CIE (ROM) Document Configuration List, Version 1.3, 9 Jun. 08 Athena Smartcard Solutions - ASEPcos-CNS/CIE (ROM) Binary Configuration List, Version 1.2, 10 Jan. 08 Athena Smartcard Solutions
[GUIDES]	Administration guidance: - ASEPCOS CNS/CIE ROM Administrator Guidance - Part 1: Generic Guidance, Version 0.4, 7 Feb. 2008 Athena Smartcard Solutions - ASEPCOS CNS/CIE ROM Administrator Guidance - Part 2: ASEPCOS CNS/CIE ROM with EU-compliant Digital Signature Application dedicated guidance, Version 0.4, 15 May. 2008 Athena Smartcard Solutions User guidance:

	- ASEPCOS CNS/CIE ROM User Guidance, Version 0.5, 18 Jan. 08 Athena Smartcard Solutions
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certified by DCSSI under the reference PP/9806.*
[PP0005]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0005-2002T.*
[PP0006]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certified by BSI(Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0006-2002T.*

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-2008-04-001 version 2.5 revision 1, April 2008.
[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, Bundesamt für Sicherheit in der Informationstechnik