Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0421-2008

for

Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00

from

Atmel Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0421-2008

SmartCard IC

Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00

from	Atmel Corporation
PP Conformance:	Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002-2001, July 2001
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 04 December 2008
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became effective on 03 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all Evaluation Assurance Levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components ACM_SCP.3 and ADV_FSP.3, ADV_HLD.3, ADV_IMP.2, ADV_INT.1, ADV_RCR.2, ADV_SPM.3, ALC_DVS.2, ALC_LCD.2, ALC_TAT.2, ATE_DPT.2, AVA_CCA.1, AVA_MSU.3, AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox, Version 00.03.10.00 or 00.03.13.00 has undergone the certification procedure at BSI.

The evaluation of the product Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox, Version 00.03.10.00 or 00.03.13.00 was conducted by T-Systems GEI GmbH. The evaluation was completed on 29 October 2008. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

[6] Information Technology Security Evaluation Facility

For this certification procedure the sponsor and applicant is: Atmel Corporation

The product was developed by: Atmel Corporation

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox, Version 00.03.10.00 or 00.03.13.00 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Atmel Corporation
Corporate Headquarters
2325 Orchard Parkway
San Jose, Ca 95131

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Targets of Evaluation (TOE) are the Atmel Smartcard ICs AT90SC28872RCU and AT90SC28848RCU with the Atmel Cryptographic Toolbox, Version 00.03.10.00 or 00.03.13.00.

The TOE is offered to customers under two part numbers AT90SC28872RCU and AT90SC28848RCU, there is no difference in either hardware or software between the 2 part numbers.

The Atmel Toolbox, Version 00.03.10.00 contains the full Atmel Toolbox, with cryptographic functionality and AIS31 test commands. The Atmel Toolbox, Version 00.03.13.00 contains the AIS31 test commands without cryptographic functionality. For purposes of this evaluation Version 00.03.13.00 is considered a subset of the Atmel Toolbox, Version 00.03.10.00.

The TOE is a single chip microcontroller and is part of the AT90SC family. The devices in the AT90SC ASL family are based on Atmel's AVR RISC family of single-chip microcontroller devices. The AVR RISC family, with designed-in security features, is based on the industry-standard AVR RISC low-power HCMOS core and gives access to the powerful instruction set of this widely used device. Different AT90SC ASL family members offer various options. The AT90SC ASL family of devices are designed in accordance with the ISO standard for integrated circuit cards (ISO 7816), where appropriate.

The TOE IT functionalities consist of tamper resistant data storage and processing such as arithmetic functions (e.g. incrementing counters in electronic purses, calculating currency conversion in electronic purses), data communication and cryptographic operations (e.g. random number generation, data encryption, digital signature verification).

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002-2001, July 2001 [10].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2 - Life cycle support - Sufficiency of security measures, AVA_MSU.3 - Vulnerability assessment - Analysis and testing for insecure states and AVA_VLA.4 - Vulnerability assessment - Highly resistant.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] resp. [9], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	Addressed issue
Test Mode Entry (SF1)	Test mode entry permitted to authorized users only
Protected Test Memory Access (SF2)	Restricted access to memories in test mode
Test Mode Disable (SF3)	Irrevocable disabling of the test mode
RNG (SF4)	Hardware Random Number Generator (RNG) according to AIS 31
Data Error Detection (SF5)	Means for performing data error detection
Firewall (SF6)	Access control based on firewall rules
Event Audit (SF7)	Event Audit security function to enforce rules for monitoring audited events
Event Action (SF8)	Appropriate action for audited events
Unobservability (SF9)	Protection of TSF data from disclosure
Cryptography (SF10)	Protection of TSF data from data retrieval or modification
Package Mode Entry (SF11)	Package mode entry for authorized users only
Test Memory Access in Package Mode (SF12)	Restricted access to memories in package mode

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] resp. [9], chapter 6.1.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] resp. [9], chapter 6.1 is confirmed.

The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] resp. [9], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] resp. [9], chapters 3.2 – 3.4.

This certification covers the following configurations of the TOE: The evaluated derivates of the TOE are the AT90SC28872RCU and AT90SC28848RCU, both silicon revision D, product identification number AT58U07, with Atmel Toolbox, Version 00.03.13.00 or 00.03.10.00.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox, Version 00.03.10.00 or 00.03.13.00

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Atmel Smartcard IC	AT90SC28872RCU AT90SC28848RCU	secure shipping (approved carrier or hand carry)
2	SW	Atmel Toolbox	Version 00.03.10.00 Version 00.03.13.00	provided within ROM of the Hardware
3	DOC	AT90SC Addressing Modes & Instruction Set, Application Note, Atmel Corporation [12]	1323C_03May04	Paper copy or electronic file
4	DOC	AdvX for AT90SC Family, Technical Datasheet, Atmel Corporation [13]	TPR0116CX_13Dec06	Paper copy or electronic file
5	DOC	Efficient use of AdvX for Implementing Cryptographic Operations, Atmel Corporation [14]	TPR0142DX_10Sep07	Paper copy or electronic file
6	DOC	The Code Signature Module, Application Note, Atmel Corporation [15]	TPR0252AX_10Jan07	Paper copy or electronic file
7	DOC	Secured Hardware DES/TDES on the AT90SC ASL4 Products, Atmel Corporation [16]	TPR0063IX_SMS_05Dec07	Paper copy or electronic file
8	DOC	Using the Supervisor and User Modes on the AT90SC ASL4 products, Atmel Corporation [17]	ATPR0095BX_07Jun07	Paper copy or electronic file
9	DOC	Generating Random Numbers with a controlled Entropy on AT90SC Family, Application Note, Atmel Corporation [18]	TPR0166CX_SMS_17Apr08	Paper copy or electronic file
10	DOC	AT90SC28872RCU Errata Sheet, Atmel Corporation [19]	TPR0309BX_SPD_17Sep07	Paper copy or electronic file
11	DOC	Toolbox 00.03.13.xx Errata Sheet, Atmel Corporation [20]	TPR0345AX_SPD_18Sep07	Paper copy or electronic file
12	DOC	Toolbox 00.03.10.xx Errata Sheet, Atmel Corporation [21]	TPR0344AX_SPD_18Sep07	Paper copy or electronic file
13	DOC	Security Recommendations for the AT90SC ASL5 products, Atmel Corporation [22]	TPR0267CX_SPD_07Dec07	Paper copy or electronic file
14	DOC	Using Toolbox version 00.03.10.xx, Atmel Corporation [23]	TPR0259CX_SMS_21Apr08	Paper copy or electronic file

No	Type	Identifier	Release	Form of Delivery
15	DOC	Securing Toolbox Operations using version 00.03.10.xx on ASL5 products, Atmel Corporation [24]	TPR0260HX_SMS_21Apr08	Paper copy or electronic file
16	DOC	Using Toolbox version 00.03.13.xx, Atmel Corporation [25]	TPR0289CX_06Feb08	Paper copy or electronic file
17	DOC	Securing Toolbox Operations using version 00.03.13.xx on ASL5 products, Atmel Corporation [26]	TPR0290GX_SMS_21Apr08	Paper copy or electronic file
18	DOC	AT90SC28872RCU Technical Datasheet, Atmel Corporation [27]	TPR0235CX_22Nov07	Paper copy or electronic file
19	DOC	AT90SC Enhanced Security Technical Datasheet, Atmel Corporation [28]	TPR0255BX_SPD_22Nov07	Paper copy or electronic file
20	DOC	Wafer Saw Recommendations, Atmel Corporation [29]	TPG0079A-13Jun05	Paper copy or electronic file

Table 2: Deliverables of the TOE

The TOE can be identified as described in the ST [6] resp. [9], section 1.2 by means of reading value 0x3003 from SN_0 and SN_1 registers that corresponds to AT58U07 (AT90SC28872RCU / AT90SC28848RCU) and by reading Toolbox version strings 0x00031000 or 0x00031300 via self test API of the Toolboxes which correspond to Toolbox, Version 00.03.10.00 or 00.03.13.00.

The smartcard product life-cycle consists of 7 phases as described in the ST [6] resp. [9], chapter 2.2. The limits of the evaluation correspond to phases 2 and 3, including the phase 1 delivery and verification procedures and the TOE delivery to the IC packaging manufacturer. Procedures corresponding to phases 4, 5, 6 and 7 are outside the scope of the Security Target. Electronic transfers of Atmel modules and data bases are done by FTP using the PGP encryption algorithm. Delivery of hardware (e.g. wafers or customer samples) is done by secure shipping (approved carrier or hand carry).
Documents are either delivered in electronic form (the delivery is PGP encrypted to the named end recipient, the docs are personalised and a record of delivery is sent, signed by the recipient and returned to Atmel, all deliveries and reception information is recorded on a database) or they are sent as paper copies (the docs are personalised and a record of delivery is sent, signed by the recipient and returned to Atmel, all deliveries and reception information is recorded on a database).

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: Controlled entry to test and package mode, access control to the test memories in test and package mode, test mode disabling, generation of random numbers, data error detection, access control to memories in user mode, logging of and reaction to security relevant events, protection of operations against observing and provision of cryptographic operations.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: Usage of Hardware Platform, Treatment of User Data, Protection during TOE Development and Production, Protection during Packaging, Finishing and Personalisation. Details can be found in the Security Target [6] resp. [9] chapter 4.2.

5 Architectural Information

The CPU of the Atmel Smartcard ICs AT90SC28872RCU and AT90SC28848RCU (further on only the AT90SC28872RCU is mentioned for both versions) has an 8-bit RISC architecture which supports the instruction set of the Atmel AVR family of microprocessors. Instructions are encoded as words of 16 bits. Some instructions with long parameters (e.g. absolute jumps) use an additional word for operand data.

The AT90SC28872RCU operates with a nominal supply voltage between 2.7 and 5.5 V. The nominal external clock frequency range is 1 to 5 MHz. An internal oscillator which provides higher speed can also be used as clock source. The controller provides power saving modes with reduced activity (idle mode and power down mode).

The device includes ROM (256 KB for application code, 32 KB for cryptographic library, this can be loaded with an Atmel Cryptographic Toolbox or the customer may supply their own toolbox), RAM (8 KB, a part of which is shared between CPU and AdvX coprocessor) and EEPROM (72 KB). The processor uses a Harvard architecture which separates code and data space. The EEPROM is mapped into both program and data space, while code execution from RAM is not possible.

The CPU of the AT90SC28872RCU provides different CPU modes, of which two are relevant in the operational phase: supervisor modes and user mode. The supervisor modes provide unlimited access to the hardware components and can be used to configure the restrictions of the user modes. In the user modes the access is restricted to the CPU, configurable parts of RAM and EEPROM, and only specific special function registers. The memory management does not use virtual addresses, but the access conditions are enforced through a system termed firewall. The firewall can be configured only by software running in supervisor mode.

After reset and when an interrupt is serviced, the CPU executes in supervisor mode. User modes is entered automatically as soon as the current program address is within the configurable user program space.

The on-chip hardware components are controlled by the operating system and the applications via special function registers. These special function registers are related to the activities of the CPU, the memory management unit, interrupt control, I/O configuration, EEPROM, timers, UART and the co-processors. The communication with the AT90SC28872RCU can be performed through an UART (ISO controller) or direct usage of the I/O port.

The AT90SC28872RCU provides an interrupt system for interrupts generated by the peripheral hardware. One interrupt vector, the security interrupt, is triggered by security violations. The type of security violation can be determined based on the value of two special function registers. The security interrupt can be masked for some sources (e.g.

illegal access attempts by the user modes software) but not for others (e.g. illegal instruction interrupt).

For the hardware security detectors (voltage, frequency, temperature) the reactions can be configured to be either the triggering of the security interrupt or the transition to a secure frozen state which halts the processor until an external reset is generated. The AT90SC28872RCU has an active shield.

The DES coprocessor supports single DES and Triple-DES operations. Triple-DES is supported for double-length keys. The AdvX coprocessor provides basic arithmetic operations with large integers to support the implementation of asymmetric cryptographic algorithms. Atmel provides a cryptographic library (Toolbox) which implements such algorithms including counter measures against side channel attacks.

The AT90SC28872RCU protects secret data stored and used by the application against physical tampering. Within the composition of this smartcard controller with an operating system and various applications the Security Functionality of the hardware must be supported at least by the operating system based on the described dependencies between the smartcard security features and the functions on top provided by the operating system.

The AT90SC28872RCU has a hardware testing mode which is further divided into two modes: The Test Mode allows full access to hardware components during wafer testing, but is inaccessible after dicing because a test mode fuse is sawn off. The Package Mode can also be entered after packaging but requires a secret entry sequence, a full EEPROM erase is performed before the test functions are enabled, and access is restricted to the EEPROM block (i.e. no access to the ROM, logic or analogue parts). These test modes use special hardware state machines and operate independent of the CPU. The AT90SC28872RCU does not contain any test ROM. Production tests requiring CPU program execution are performed by temporarily loading test software into EEPROM.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

The tests performed by the developer can be divided into following categories:

- Module tests which are performed in a simulation environment for analogue and for digital simulations as early on the life cycle of the TOE.
- Tests which are performed for the Toolbox software within dedicated test environment.
- Validation, qualification and security tests to release the TOE to production, mainly:
    - used to determine the behaviour of the chip with respect to different operating conditions and varied process parameters (characterization tests) and
    - special verification tests for Security Functions which were done with samples of the TOE (referred also as security testing).
- Production (functional) tests, which are done for every chip to check its correct functionality as a last step of the production process (phase 3 of the TOE life cycle).

The developer tests cover all Security Functions and all security mechanisms as identified in the Functional Specification, and in the High and Low Level Designs.

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developers' sites. They performed independent tests to supplement, augment and to verify the positive results of tests performed by the developer. Besides repeating exactly the developers' tests, test parameters and test equipment are varied and additional analysis was done. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

The evaluators supplied evidence that the actual version of the TOE provides the Security Functions as specified by the developer in the Security Target. The test results confirm the correct implementation of the TOE Security Functions.

For penetration testing the evaluators took all Security Functions into consideration. Intensive penetration testing was planed based on the analysis results and performed for the underlying mechanisms of Security Functions using bespoke equipment and expert know how. The penetration tests considered both the physical tampering of the TOE and attacks that do not modify the TOE physically (i.e. DPA/SPA testing). The overall judgement on the results of penetration testing is that there are no exploitable vulnerabilities to an attacker with high attack potential in the intended operational environment as defined by the Security Target.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE is a smartcard controller hardware with cryptographic support software. The TOE is identified by Atmel under the part numbers AT90SC28872RCU and AT90SC28848RCU, the silicon revision of the device is D, the Cryptographic Toolbox is identified as Atmel Cryptographic Toolbox, Version 00.03.13.00 or 00.03.10.00.

In the evaluated configuration only the secure versions of the services RSA with CRT, RSA without CRT and prime generation (Miller Rabin) are allowed to be used for secure data (see ST [6] resp. [9], chapter 6.1.10) (only applicable to Atmel Toolbox, Version 00.03.10.00).

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) The Application of Attack Potential to Smartcards

(iii) Functionality classes and evaluation methodology of physical random number generators

(see [4], AIS 25, AIS 26, AIS 31) were used.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 5 package as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 - Life cycle support - Sufficiency of security measures, AVA_MSU.3 - Vulnerability assessment - Analysis and testing for insecure states and AVA_VLA.4 - Vulnerability assessment - Highly resistant augmented for this TOE evaluation.

According to AIS 38 (see [4]) evaluation results related to product type specific (PTS) aspects of certain development and production sites including related site audits have been re-used as they were performed by the French Certification Scheme in the course of the certification procedure of the Atmel Smartcard IC AT90SC12872RCFT (certification-ID 2006/15). As required by the AIS 38 the developer provided an Impact Analysis [30] with a description of the changes concerning the Security Assurance Classes ACM, ADO and ALC and a rational why the results of the certification under the ID 2006/15 are still valid.

The evaluation has confirmed:

- PP Conformance: Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002-2001, July 2001 [10]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by
  ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function : high

  Test Mode Entry (SF1)
  Protected Test Memory Access (SF2)
  RNG (SF4)
  Event Audit (SF7)
  Unobservability (SF9)
  Cryptography (SF10)
  Package Mode Entry (SF11)
  Test Memory Access in Package Mode (SF12)

  In order to assess the Strength of Functions the scheme interpretation AIS 31 (see [4]) was used.

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The following cryptoalgorithms were part of the rating of the Strength of Functions:

- the TOE Security Function SF 10 Cryptography (SHA algorithm, Miller Rabin algorithm)

The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for:

- the TOE Security Function SF 10 Cryptography (TDES algorithm, RSA without CRT algorithm, RSA with CRT algorithm).

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. Especially, the following aspects need to be fulfilled when using the TOE:

- Regarding storage of secret data in the ROM [22], section 4.3 has to be observed.
- The effectiveness of the memory management especially depends on the configuration by the smartcard embedded software. Therefore the implementation of routines that serve the different exceptions/interrupts shall fulfil the recommendations provided in [22], especially sections 3.2 and 3.6.
- The TOE provides a lot of security features to detect malfunctions. It is not possible to find areas on the chip where a fault can be induced without forcing exceptions or sensor resets. The smartcard embedded software shall implement an appropriate handling of such exceptions and sensor events. The user must follow the guidance for secure operation. Especially [22], sections 3.4, 3.14, 4.1 and 4.8 are to be observed. For the services provided by the Toolbox (especially secure hash algorithms, secure variants of RSA with CRT, RSA without CRT and prime generation Miller Rabin) the user must consider the effect of faults in the returned (by the Toolbox procedures) data. Related guidance is provided also in [23], sections 2, 3.3.5 and 3.6.7.
- The RNG has to be used as described in guidance [26], section 3.3 (or the same text in [24], section 4.3) and the recommendations in the sample routine in [26], section 3.3.2 (or [24], section 4.3.2) have to be observed.
- The user must follow the guidance for securing DES/TDES operations, [16]. Especially the measures stated in table 2 and in section 4 shall be implemented.
- When using the Toolbox services secure RSA, secure RSA/CRT, secure prime generation (Miller Rabin) the user must follow the user guidance to protect against side channel attacks. The user guidance [24], sections 3.5 and 3.6 describes the countermeasures that must be implemented by the user. When using prime generation (Miller Rabin) Toolbox service the user must follow the user guidance [23], section 5.3.2.1.
- The user must take care about side channel attacks when using the ADVx coprocessor with secret key data. Similar is also the case when using any of the hash services of the Toolbox with secret key data (i.e. keyed hash) and the CRC hardware engine as the hash services implementation and the implementation of the CRC engine is not claimed to be side channel resistant and therefore its respective resistance was not tested. Only the security of DES/TDES, RNG, and secure variants RSA with CRT, RSA without CRT and prime generation (Miller Rabin) against side channel attacks has been evaluated as it could be assessed without knowledge of actual implementation of the smartcard embedded software.

11 Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

AdvX	32-bit Crypto Accelerator developed and produced by Atmel
AVR	8-bit RISC processor developed and produced by Atmel
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CPU	Central Processing Unit
CRC	Cyclic Redundancy Code
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory
HCMOS	High Speed Complementary Metal Oxide Semiconductor
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
RAM	Random Access Memory
RISC	Reduced Instruction Set Core
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, & Adleman (public key encryption technology)
SF	Security Function
SPA	Simple Power Analysis
SOF	Strength of Function
ST	Security Target
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UART	Universal Asynchronous Receiver-Transmitter

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[8]

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-0421-2008, Version 2.2, 14.04.2008, Roper Security Target, Atmel Corporation (confidential document)

[7] Evaluation Technical Report, Version 1.06, 27.10.2008, Evaluation Technical Report Summary BSI-DSZ-CC-0421, T-Systems GEI GmbH (confidential document)

[8] Configuration list for the TOE, Version 1.50, 23.10.2008, Roper Evaluation Deliverables List (confidential document)

[9] Security Target BSI-DSZ-0421-2008, Version TPG0139C, 04.11.2008, AT90SC28872RCU / AT90SC28848RCU Security Target Lite, Atmel Corporation (sanitised public document)

[10] Smart Card IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001, developed by Atmel Smart Card ICs, Hitachi Ltd., Infineon Technologies AG, Philips Semiconductors

[11] ETR-lite for composition according to AIS 36 for the Product AT90SC28872RCU / AT90SC28848RCU, Version 1.06, 08.10.2008, T-Systems GEI GmbH (confidential document)

---

[8] specifically

- AIS 25, Version 3, 06 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 26, Version 3, 06 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 31, Version 1, 25 September 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 01 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document resp. CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document resp. CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[12] AT90SC Addressing Modes & Instruction Set, Application Note, 1323C_03May04, Atmel Corporation

[13] AdvX for AT90SC Family, Technical Datasheet, TPR0116CX_13Dec06, Atmel Corporation

[14] Efficient use of AdvX for Implementing Cryptographic Operations, TPR0142DX_10Sep07, Atmel Corporation

[15] The Code Signature Module, Application Note, TPR0252AX_10Jan07, Atmel Corporation

[16] Secured Hardware DES/TDES on the AT90SC ASL4 Products, TPR0063IX_SMS_05Dec07, Atmel Corporation

[17] Using the Supervisor and User Modes on the AT90SC ASL4 products, ATPR0095BX_07Jun07, Atmel Corporation

[18] Generating Random Numbers with a controlled Entropy on AT90SC Family, Application Note, TPR0166CX_SMS_17Apr08, Atmel Corporation

[19] AT90SC28872RCU Errata Sheet, TPR0309BX_SPD_17Sep07, Atmel Corporation

[20] Toolbox 00.03.13.xx Errata Sheet, TPR0345AX_SPD_18Sep07, Atmel Corporation

[21] Toolbox 00.03.10.xx Errata Sheet, TPR0344AX_SPD_18Sep07, Atmel Corporation

[22] Security Recommendations for the AT90SC ASL5 products, TPR0267CX_SPD_07Dec07, Atmel Corporation

[23] Using Toolbox version 00.03.10.xx, TPR0259CX_SMS_21Apr08, Atmel Corporation

[24] Securing Toolbox Operations using version 00.03.10.xx on ASL5 products, TPR0260HX_SMS_21Apr08, Atmel Corporation

[25] Using Toolbox version 00.03.13.xx, TPR0289CX_06Feb08, Atmel Corporation

[26] Securing Toolbox Operations using version 00.03.13.xx on ASL5 products, TPR0290GX_SMS_21Apr08, Atmel Corporation

[27] AT90SC28872RCU Technical Datasheet, TPR0235CX_22Nov07, Atmel Corporation

[28] AT90SC Enhanced Security Technical Datasheet, TPR0255BX_SPD_22Nov07, Atmel Corporation

[29] Wafer Saw Recommendations, TPG0079A-13Jun05, Atmel Corporation

[30] AIS38 Report, Version 1.5, 18 April 2008, Atmel Corporation

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/ or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment 37

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0421-2008

Evaluation results regarding development and production environment

The IT product Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox, Version 00.03.10.00 or 00.03.13.00 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 13 November 2008, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.3),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.2, ALC_TAT.2),

are fulfilled for the development and production sites of the TOE listed below:

(a) Atmel Secure Products Division, Scottish Technology Par, East Kilbride, Scotland, United Kingdom, G75 0QR (Design and Test Centre)

(b) Toppan Photomasks, 224 Bd Kennedy, Corbeil, France (Maskshop)

(c) Atmel Rousset, Zone Industrielle, 13106 Rousset Cedex, France (Waferfab)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]). The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] resp. [9]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.