National Information Assurance Partnership

™

Common Criteria Evaluation and Validation Scheme
Validation Report

Atmel Corporation
Atmel AT97SC3201 Trusted Computing Module (TPM)

Report Number: CCEVS-VR-05-0098

Dated: April 8, 2005

Version: 1.0

Table of Contents

List of Tables

1   EXECUTIVE SUMMARY

This report documents the NIAP validator's assessment of the CCEVS evaluation of the Atmel AT97SC3201 Trusted Computing Module (TPM). It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by CygnaCom Solutions and was completed on April 6, 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by CygnaCom and submitted to the validators. The evaluation determined the product to be Part 2 Common Criteria version 2.1 extended conformant, Part 3 Common Criteria version 2.1 conformant, and to meet the requirements of EAL3 augmented with CC components ADV_SPM.1 (informal security policy model) and ALC_FLR.1 (basic flaw remediation), resulting in a "pass" in accordance with CC Part 1, paragraph 175.

The product is an integrated circuit chip designed to be included in personal computers and other embedded systems. The AT97SC3201 implements a Trusted Computing Module (TPM) in accordance with version 1.1b of the TCG Main Specification issued by the Trusted Computing Group. The TPM provides security primitives in a secure environment. The primitives include digital signatures, random number generation, and protected storage and binding information to the TPM. The TPM is described in detail in the TCG Main Specification.

The TOE comprises the Atmel AT97SC3201 and its embedded firmware. The TOE performs RSA key generation and digital signature, data decryption, user identification and authentication, secure hash, and software random number generation. The TSF boundary is the same as the TOE boundary. The TPM supports the following protocols and algorithms:

- Algorithms: RSA, SHA-1, HMAC
- Random number generation
- Key generation
- Self-tests

The TOE is designed to be integrated into personal computers and other embedded systems. All communication between the host system and the TOE is through the LPC (Low Pin Count bus) interface on the TOE.

The TOE is offered to OEM manufacturers as a turnkey solution, including the embedded firmware. In addition, Atmel provides the necessary driver software for integration into certain operating systems, along with BIOS drivers. Users of the TOE are OEMs and application programmers. End users of equipment in which the TOE is embedded are not "users" in terms of the evaluation.

Operation of the TOE is possible only after initialization of the TOE at the user site. Initialization is not performed at the factory.

The validator monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed selected evaluation evidence, and reviewed the individual work units and successive versions of the ETR. The validator found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). The validator concludes that CygnaCom Solutions' findings are accurate, the conclusions are justified, and the conformance results are correct.

The Validation Report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

2 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTL)s using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations.   Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides the information needed to completely identify the product, including:

- the Target of evaluation (TOE): the fully qualified identifier of the product as evaluated,
- the Security Target (ST), describing the security features, claims, and assurances of the product,
- the conformance result of the evaluation,
- the organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Atmel AT97SC3201 Trusted Computing Module
Protection Profile	Not applicable
Security Target	AT97SC3201 Security Target, Version 2.3, February 21, 2005
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation at EAL3 augmented (In two volumes, Volume 1 for the ST evaluation and Volume 2 for the TOE Evaluation) Trusted Platform Module Atmel AT97SC3201, Security Target version 2.3, February 21, 2005, ETR Version 2.0, April 6, 2005
Conformance Result	Part 2 extended, Part 3 conformant, and EAL3 augmented with CC components ADV_SPM.1 and ALC_FLR.1
Sponsor	Atmel Corporation, 1150 E. Cheyenne Mountain Blvd., Colorado Springs, CO 80906
Developer	Atmel Corporation, 1150 E. Cheyenne Mountain Blvd., Colorado Springs, CO 80906
Evaluators	CygnaCom Solutions Ms. Jean Petty Mr. Peter Kukura Ms. Nithya Rachamadugu Government Participants - None
Validator	Mr. Stuart Schaeffer (Aerospace Corporation)

Tables 2 and 3 identify the NIAP and International interpretations applicable to the TOE for this evaluation.

Table 1. Applicable NIAP Interpretations

#	Title
I-0347	Including Sensitive Information In Audit Records
I-0350	Clarification Of Resources/Objects For Residual Information Protection
I-0352	Rules Governing Binding Should Be Specifiable
I-0375	Elements Requiring Authentication Mechanism
I-0381	Relationship Between FPT_PHP And FMT_MOF
I-0389	Recovery To A Known State
I-0393	A Completely Evaluated ST Is Not Required When TOE Evaluation Starts
I-0395	Security Attributes Include Attributes Of Information And Resources
I-0405	American English Is An Acceptable Refinement
I-0406	Automated Or Manual Recovery Is Acceptable
I-0407	Empty Selections Or Assignments
I-0409	Other Properties In FMT_MSA.3 Should Be Specified By Assignment
I-0410	Auditing Of Subject Identity For Unsuccessful Logins
I-0411	Guidance Includes AGD_ADM, AGD_USR, ADO, And ALC_FLR
I-0412	Configuration Items In The Absence Of Configuration Management
I-0414	Site-Configurable Prevention Of Audit Loss
I-0415	User Attributes To Be Bound Should Be Specified
I-0416	Association Of Access Control Attributes With Subjects And Objects
I-0417	Association Of Information Flow Attributes W/Subjects And Information
I- 0418	Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3
I-0420	Attribute Inheritance/Modification Rules Need To Be Included In Policy
I-0421	Application Notes In Protection Profiles Are Informative Only
I-0422	Clarification Of ``Audit Records''
I-0423	Some Modifications To The Audit Trail Are Authorized
I-0424	FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical
I-0425	Settable Failure Limits Are Permitted
I-0426	Content Of PP Claims Rationale
I-0427	Identification Of Standards
I-0429	Selecting One Or More
I-0459	CM Systems May Have Varying Degrees Of Rigor And Function

Table 2. Applicable International Interpretations

#	Title
003	Unique identification of configuration items in the configuration list
004	ACM_SCP.*.1C requirements unclear
006	Virtual machine description
008	Augmented and Conformant overlap
009	Definition of Counter
013	Multiple SOF claims for multiple domains in a single TOE
016	Objective for ADO_DEL
019	Assurance Iterations
024	COTS product in TOE providing security
025	Level of detail required for hardware descriptions
027	Events and actions
031	Obvious vulnerabilities
032	Strength of Function Analysis in ASE_TSS
033	CC use of "Check"
037	ACM on Product or TOE?
043	Meaning of "clearly stated" in APE/ASE_OBJ.1
049	Threats met by environment
051	Use of documentation without C & P elements.
055	Incorrect Component referenced in Part 2 Annexes, FPT_RCV
058	Confusion over refinement
064	Apparent higher standard for explicitly stated requirements
065	No component to call out security function management
067	Application notes missing
069	Informal Security Policy Model
074	Duplicate informative text for ATE_COV.2-3 and ATE_DPT.1-3
075	Duplicate informative text for different work units
084	Aspects of objectives in TOE and environment
085	SOF Claims additional to the overall claim
095	SCP Dependency in ACM_CAP
098	Limitation of refinement
116	Indistinguishable work units for ADO_DEL
120	Sampling of process expectations unclear
127	Work unit not at the right place
128	Coverage of the delivery procedures
133	Consistency analysis in AVA_MSU.2
138	Iteration and narrowing of scope

3   SECURITY POLICY

The product enforces the following security policies.

3.1 Password Policy

Access to product functions and internally stored data requires "authorization data" in the form of an 8-byte password associated with an entity. An entity is defined as a specific key pair or data encrypted or hashed with a specific key. The product maintains a count of all password check failures in an internal register.

Statistically, some failed authorization attempts will occur under normal usage and because of this, the failure counter mechanism involves two stages. Failed attempts up to the value of the failure modulus (an internal counter that is initially set to 1 in the evaluated configuration) do not cause any lockout. The very next failure, however, causes a delay in the form of a lockout period. After the delay times out, additional attempts are permitted before the next delay is imposed. The length of the delay increases geometrically each time with the first delay lasting 1.1 minutes, the second lasting 2.2 minutes, and so on.

3.2 Role Differentiation Policy

The product supports exactly three roles:

- TPM Owner,
- Owners of entities,
- TPM manufacturer or designee.

Users are associated with roles. The role of TPM owner is defined as the entity that knows and can successfully present the owner authorization data. The role of entity owner is defined as the entity that knows and can successfully present the entity authorization data. The role of TPM manufacturer or designee is defined as the entity that knows and can successfully present manufacturer authorization data and proof of physical presence.

3.3 Identification and Authentication Policy

In this product, user and administrator identity are not expressed as a character string associated with an individual. A claim of identity is implicit in a command sent to the chip for execution.

The identification and authentication capability is used to authenticate an entity owner and to authorize use of an entity. The basic premise is proof of knowledge of a shared secret, i.e., an 8-byte password, when a command requiring authorization is passed to the TPM. Authorization data is created and associated with the TPM Owner and each entity (a key pair, for example) that the TPM controls. The authorization data for the TPM Owner and the Storage Root Key are held within the TPM itself and the authorization data for other entities are held with the entity, in a storage medium outside the TPM.

There is a separate password (authorization data) for each entity. The TPM Owner authorization data, required for taking ownership of the TPM, allows the Owner to prove ownership of the TPM and to perform certain commands that are available only to the TPM Owner. Proving ownership of the TPM does not allow access to all entities – the TPM Owner is not a "super user" and additional authorization data must be provided for each protected entity or operation.

The TPM treats knowledge of the authorization data as complete proof of ownership of the entity.

3.4 Access Control Policy

The TPM provides access control for
- Subjects (commands executing on behalf of users),
- Objects (keys and user data), and
- Operations (signature generation, encryption, or decryption)

by requiring authorization before execution of commands involving protected operations. This authorization is given only after the requestor has demonstrated knowledge of the appropriate user

authorization secret information when loading the key, and again when any command that uses the loaded key is transmitted to the TPM.

Access control policy is enforced on objects based on security attributes stored as nonvolatile fields within a data structure (the *keyInfo* structure) created when the key is originally generated by the TPM. The attributes recorded in the *keyInfo* structure include:

- a flag indicating whether access to a key requires authorization
- flags indicating whether a key is migratable or volatile
- a key usage data structure defining the operation — signing, storage, identity, etc. — for which the key can be used.

The TPM enforces rules to determine if an operation among controlled subjects and controlled objects is allowed:

- If is not required, access is not restricted and is available to the world. If owner authorization is required, then access is restricted to the owner of the authorization secret. If unauthorized access is requested for a key or data that requires authorization, the TPM returns an error code.
- Cryptographic operations for each key are limited according to the key usage data. For each requested operation, the TPM determines whether a key can be used for the specified operation. If the operation is not allowed for the specified key type, the TPM returns an error code.

3.5 Security Management Policy

The TOE restricts the ability to *disable or enable* the functions to:

- Reset the Authorization Failure Counter to 0 (once per delay session). TPM Owner authorization is required.
- Change the operating mode of the Authorization Failure Counter. TPM Owner authorization is required.
- Initialize and lock the FIPS operating mode to the TPM owner. TPM Owner authorization is required.

Security attributes restrict the ability to create the security attributes associated with a particular entity, including key usage data, authorization required data, migratability, and volatility, to the entity owner. Authorization data for the parent key (the root of the key hierarchy of which the key of interest is a member) is required to execute this command.

The management of TPM data is performed according to the requestor's role and the function performed as follows:

- For the role TPM Owner and the function *modify*, the TOE restricts the ability to modify the identification and authentication data associated with the Endorsement Key and Storage Root Key and Migration authorization data to the TPM Owner. The Endorsement Key is generated prior to establishment of an Owner, and is used in the process of taking ownership. Once created, there is no means to modify or delete the Endorsement Key by the Owner or by any other entity or identity. The Storage Root Key authorization data and/or the Owner authorization data can be modified. Presentation of the current Owner authorization data is required.
- For the role TPM Owner and the function *create*, the TOE restricts the ability to generate the Storage Root Key and *TPMProof*, a random number (nonce) that each TPM maintains to validate that the data originated at this TPM, to the TPM Owner. Both the Storage Root Key and *TpmProof* are generated by the TPM during the process of taking ownership. Presentation of the Owner authorization data is required.
- For the role Entity Owner, the TOE restricts the ability to modify the Identification and Authentication data associated with entity to the *entity Owner*. Presentation of entity authorization data for both the key to be modified and the parent of that key is required.
- For the role Manufacturer, the TOE restricts the ability to generate the *Endorsement Key Pair* to the TPM manufacturer or designee. The TPM is shipped with no Endorsement Key Pair generated

or present on board the TPM. Atmel designates the platform manufacturer as the authorized entity to create the endorsement key pair.

4   ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 Usage Assumptions

The evaluation made the following assumptions concerning product usage:

- The product is properly installed in a desktop or laptop personal computer.
- The product is configured according to the Administrator and User Guidance document.
- Users follow password policies and other guidance described in the Administrator and User Guidance document.
- Ownership of the product is established as early as possible, since the product is vulnerable to attack prior to establishment of ownership.

4.2 Environmental Assumptions

The evaluation made the following assumptions concerning the environment:

- The product is physically protected, since it cannot protect itself against physical tampering.
- Access to key data stored outside the chip is controlled by the functions of the environment (e.g., the operating system).

4.3 Clarification of Scope

Certain threats are outside the scope of the product's capabilities to counter, and the product makes no claims of protection against them:

- The product has an authentication failure handling mechanism to protect itself against password cracking attacks. After a specified number of failed password attempts, the product locks users out for progressively longer periods of time. If an attacker intentionally sends multiple bad passwords to the chip, this can cause denial of service for authorized users. The product does not claim that it can protect itself against such attacks.
- The product protects only information under its control, i.e., stored in the chip.
- The product does not protect against access to its functions by individuals not authorized to use the system in which the product is installed. In a practical application, the environment, typically the operating system, is expected to provide any such protection.

5   ARCHITECTURAL INFORMATION

The product is a single system (a single monolithic integrated circuit chip) with no subsystems.

6   DOCUMENTATION

The following product documentation is provided to consumers:

- AT97SC3201 Security Target, Version 2.3, February 21, 2005
- AT97SC3201 Technical Data Sheet (Atmel Lit. No. 2015)
- Low Pin Count (LPC) Interface Specification, Revision 1.0, September 29, 1997
- Atmel – Specific Commands for TCPA Chip, Version 0.17, 4/12/02

- Atmel Trusted Platform (AT97SC3201) Administrator and User Guide, Version 1.1, November 10, 2004.

7 IT PRODUCT TESTING

7.1 Developer Testing

The TOE is a mass-replicated integrated circuit chip, and the developer tests manufacturing samples for conformance to specifications. This testing is performed by placing the test sample into a test platform, an IBM PC, and testing the chip functions. Most testing is automated using scripts written in the PERL language. The PERL scripts generate commands on the PC, send commands to the chip, collect the results returned from the chip to the PC, and save the commands and results for analysis. Test setup steps that are not automated are those requiring operator intervention: pushing a button to reset the chip, cycling power, and monitoring the lockout period with a clock.

As originally presented for evaluation, the developer's testing was not exhaustive. The evaluator worked with the developer to create additional tests for all cases not included in the developer's test suite. The developer has incorporated these additional tests into their standard test suite, and the developer testing is now exhaustive; all TOE Security Functions in the ST are tested.

The product is tested as manufactured, with register settings as specified in the Atmel Trusted Platform (AT97SC3201) Administrator and User Guide, Version 1.1. The test procedures and expected results are documented in the Atmel AT97SC3201 Master Verification Coverage document, version 1.9.

7.2 Evaluator Testing

The evaluator performed the entire developer test suite of 65 PERL scripts. The evaluator tested all security functions, and the test results were analyzed and checked to ensure that expected results were returned in all cases.

The evaluator also specified and ran five additional tests as part of the independent testing. These tests were specified based on the evaluator's analysis of the vendor test coverage and the vendor's vulnerability assessment. Programs to perform these tests were written in the C programming language by the vendor according to the evaluator's specifications. The evaluator verified the programs to ensure that the tests were coded as specified. The five additional tests were:

1. Test of the command *TPM_SelfTestFull*, which demonstrates a full self test, which is available upon request.
2. Test of the command *TPM_GetTestResult*, which provides a report of the success or failure of the Power-on self-test function. This result is usually passed to an application, i.e., is not accessible to a user and the evaluator requested a test to show the power-on self test result.
3. Test of the command *TPM_Reset*, which demonstrates that the TPM_Reset command clears all volatile memory, but no PCR registers or loaded keys are affected.
4. Test of the command *TPM_EvictKey*, including positive and negative tests showing that the key is loaded and then evicting the key, making any subsequent attempt to access keys return a Key Not Found message.
5. Test for the Failed Authentication Attempts Counter demonstrating the lockout feature of the chip.

All tests gave the expected (correct) results. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities.

8 EVALUATED CONFIGURATION

The TOE is a monolithic integrated circuit chip and has no subsystems or discrete components that can be added, removed, or rearranged. The evaluated configuration was as delivered from the factory and described in the document AT97SC3201 Technical Data Sheet (Atmel Lit. No. 2015), with register settings for initialization (including enablement) and operation as specified in the Atmel Trusted Platform (AT97SC3201) Administrator and User Guide, Version 1.1.

9   RESULTS OF THE EVALUATION

The evaluation determined the product to be Part 2 extended, Part 3 conformant and to meet the requirements of EAL 3 augmented with CC components ADV_SPM.1 (informal security policy model) and ALC_FLR.1 (basic flaw remediation).

10 EVALUATOR COMMENTS

There are no Evaluator comments.

11 ANNEXES

There are no annexes.

12 SECURITY TARGET

The ST, *AT97SC3201 Security Target*, Version 2.3, February 21, 2005, is included here by reference.

13 GLOSSARY

CC	Common Criteria
CCEL	Common Criteria Evaluation Laboratory
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
ETR	Evaluation Technical Report
MRA	Mutual Recognition Arrangement
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
OR	Observation Report
PP	Protection Profile
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

14 BIBLIOGRAPHY

[1]   Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2]   Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3]   Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4]   Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5]   Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6]   Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0

[7]   AT97SC3201 Security Target, Version 2.3, February 21, 2005

[8]   AT97SC3201 Technical Data Sheet (Atmel Lit. No. 2015)

[9]   Low Pin Count (LPC) Interface Specification, Revision 1.0, September 29, 1997

[10]   Atmel – Specific Commands for TCPA Chip, Version 0.17, 4/12/02

[11]   Atmel Trusted Platform (AT97SC3201) Administrator and User Guide, Version 1.1, November 10, 2004