# National Information Assurance Partnership


# Common Criteria Evaluation and Validation Scheme
# Validation Report

## IBM CORPORATION

## IBM Cryptographic Security Chip for PC Clients
## Manufactured by ATMEL (AT90SP0801)

**Report Number: CCEVS-VR-01-0005**

**Dated: October 10, 2001**

**Version: 1.0**

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6740**
**Fort George G. Meade, MD 20755-6740**

National Information Assurance Partnership

# Common Criteria Certificate

IBM Corporation

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate 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.

Product Name: IBM Cryptographic Security Chip for PC Clients Manufactured by ATMEL (AT90SP0801)
Version and Release Numbers: AT90SP0801
Evaluation Platform: N/A
Assurance Level: EAL3 Augmented

Name of CCTL: CygnaCom Solutions, Inc., an Entrust Company
Validation Report Number: CCEVS-VR-01-0005
Date Issued: 10 October 2001
Protection Profile Identifier: N/A

Original Signed

Director
Information Technology Laboratory
National Institute of Standards and Technology

Original Signed

Information Assurance
Director
National Security Agency


## ACKNOWLEDGEMENTS

### Validation Team

Jerome Myers
Stuart Schaeffer
Aerospace Corporation
Columbia, Maryland/El Segundo, California

### Common Criteria Testing Laboratory

Cygnacom Solutions, an Entrust Company
McLean, Virginia

## Table of Contents



## LIST OF TABLES

# 1 EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the CCEVS evaluation of the IBM Cryptographic Security Chip for PC Clients manufactured by Atmel Corporation (AT90SP0801). It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by Cygnacom Solutions and was completed on September 9, 2001. 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 conformant, Part 3 conformant,** and to meet the requirements of **EAL 3 augmented with CC component ADV_SPM.1**[1] (informal security policy model), resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The product is an integrated circuit chip interfacing with the Intel System Management Bus (SMBus) and mounted on a daughter card on the motherboard of an IBM desktop computer or surface-mounted on the motherboard of an IBM notebook computer. The product provides (1) RSA digital signature computation using internally stored 512-bit or 1024-bit keys, and (2) decryption of relatively small encrypted blocks of data bits (e.g., symmetric encryption keys that must be protected against disclosure) stored in a disk or memory component of the environment. For signature generation, an arbitrary number of user public key pairs, encrypted with a hardware (product-specific) public key, can be stored in the system in which the product is embedded. When a user requires a signature, the user's private key is decrypted by the product and stored in a register internal to the product. Access to product functions may optionally be controlled by password. Data within the product (decrypted keys) is not accessible by the surrounding system. The hardware private key may be changed by the possessor of a hardware password or locked to prevent its being changed.

The product is intended to protect the confidentiality and integrity of secret keys and to prevent unauthorized use of a key. It does not support any particular Organizational Security Policies (OSPs) but provides the general protections noted here.

All product related support functions must be provided as components of the environment. These functions include key pair generation, encryption of keys and data, hashing for signature generation, and movement of commands and data into and out of the chip via the SMBus. Environmental software provided by IBM for the product was available to facilitate some of the product analysis and testing. However, this environmental software, provided by IBM in the Secure PC client computing platforms, has not been subjected to a NIAP evaluation. In the configuration in which the chip is mounted on a daughter card, the card is also a component of the environment and was not an element of this evaluation.

It is assumed that the operating system is configured to meet installation security requirements, that administration of the computational environment is performed correctly and in a secure manner, and that adequate physical protection (power management, protection against physical tampering, etc) is provided.

The validation team 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 validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that Cygnacom Solution's findings are accurate, the conclusions justified, and the conformance results 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.

[1] The terminology in this sentence is defined in *CC Interpretation 008*, specifying new language for CC Part 1, section/Clause 5.4.

# 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 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 | IBM Cryptographic Security Chip for PC Clients Manufactured by ATMEL (AT90SP0801) |
| Protection Profile | Not Applicable |
| Security Target | IBM Cryptographic Security Chip for PC Clients Manufactured by ATMEL (AT90SP0801), Common Criteria Security Target Version 4.3, by Cygnacom Solutions. |
| Evaluation Technical Report | IBM Cryptographic Security Chip for PC Clients Manufactured by ATMEL (AT90SP0801), Common Criteria Evaluation Technical Report, by Cygnacom Solutions |
| Conformance Result | Part 2 conformant, Part 3 conformant, and EAL 3 augmented with CC component ADV_SPM.1. |
| Sponsor | IBM Personal Systems, 3039 Cornwallis Rd, Research Triangle Park, NC 27709 |
| Developer | IBM Personal Systems, 3039 Cornwallis Rd, Research Triangle Park, NC 27709<br>Atmel Corporation, 1150 E. Cheyenne Mtn. Blvd., Colorado Springs CO 80906 |
| Evaluators | Cygnacom Solutions<br>Ms. Kristina Rogers<br>Ms. Shari Galitzer<br>Government Participants<br>None |
| Validators | Mr. Jerome Myers (Aerospace Corporation)<br>Mr. Stuart Schaeffer (Aerospace Corporation) |

# 3 SECURITY POLICY

The following security policies are enforced by the product.

## 3.1 Password Policy

Access to product functions and internally stored data requires a password. There are three classes of password:

- Hardware password, stored in a register in the chip. The hardware password is required for all administration and configuration actions. It is required to be set at system (i.e., chip) initialization.
- Failure Counter Reset password, stored in a register in the chip. The Failure Counter Reset password can be used to reset the Password Failure Counter. It must be set at system initialization.
- User password. A user may optionally specify a password to control access to his/her key when the key is stored in a buffer within the chip. If no user password is associated with a buffered user key, anyone may access the key buffer.

The product maintains a count of all password check failures (for all three types of password) in an internal register, the Failure Counter. When the failure count reaches a multiple of 32, the chip is locked for a period of time corresponding to the count as shown in Table 2.

**Table 2: Lockout Time vs. Cumulative Password Failure Count**

| Cumulative Failure Count | Lockout Period |
|---|---|
| 32 | 1.2 Minutes |
| 64 | 2.4 Minutes |
| 96 | 4.8 Minutes |
| … | … |
| 224 | 1 Hour, 17 Minutes |
| 256 | 2 Hours, 34 Minutes |
| … | … |
| 384 | 1.7 Days |
| … | … |
| 512+ | 27.2 Days |

When ten unsuccessful authentication attempts occur related to the hardware password and the Failure Counter Reset password, the Failure Count is modified If it is less than 224, it is incremented to 224. If greater than 224, it is incremented to the next multiple of 32. The lockout period then begins.

## 3.2 Role Differentiation Policy.

The product supports exactly two roles:

- Administrator
- User (sometimes also referred to as Operator)

An Administrator is defined as any person who can provide the hardware password.
All other persons are users.

## 3.3 Identification and Authentication Policy.

In this product, user (or administrator) identity is 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.

For an administrator, issuing the *Hardware Key Password Check* command asserts the claim of administrator identity. The claim is authenticated if the hardware password is provided as command input. Password authentication is mandatory for an administrator.

For a user, issuing the *User Key Password Check* command asserts that the issuer claims the identify of "owner" of the encryption key in one of two internal chip buffers, specified in the command; the identity claim is "the current owner of nticated if the user password, provided as command input, matches the user password (if any) associated with the chip buffer.

A user buffer may be flagged as requiring no password, in which case any user can access the buffer (and use the key).

User identities are not maintained across power cycles.

## 3.4 Access Control Policy

### 3.4.1 Access to hardware key.

Only an administrator may generate a signature using the hardware key. Any user may use the hardware key to decrypt an externally stored key pair.

### 3.4.2 Access to user buffers.

User buffer access control is discretionary: a user specifies whether the buffer is password protected when loading key data into one of the buffers.

If a user buffer is password protected, only the owner (a user providing the password) can
(1) decode[2] the user's externally stored encrypted private key data and store it in a user buffer, and
(2) use the key in the buffer for signature generation or decryption.

If a user buffer is not password protected, any user can perform these operations.

## 3.5 Security Management Policy

Only an administrator may issue the following commands:

- Lock the hardware key (i.e., make the current hardware key permanently unchangeable).
- Change the hardware password.
- Change the Failure Counter Reset password.
- The maximum size of a data block that can be read from the chip (i.e., returned by a *read* command).
- Enable clearing of chip data.
- *Hardware Key Password Check* command.
- The command to reset the Password Failure Counter.

[2] "Decode" is the term used by the product manufacturer for this decryption operation.

# 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 System Administrator's Guide.
- The hardware password is changed from its default (factory-set) value when the chip is initialized.
- Users do not disclose their passwords to unauthorized users.
- Passwords are cleared from the chip after use to avoid unauthorized reuse.
- Administrators and users follow the guidance documents.
- The chip clear function is disabled during initialization to avoid a denial of service attack

## 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 functions in the environment (e.g., the operating system).
- Key pairs and passwords are correctly generated by environmental functions.

## 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 chip has an authentication failure handling mechanism to protect against password cracking attacks. After a specified number of failed password attempts, the chip 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 on the chip. Key pairs and passwords are generated in the environment and must be protected in the environment (i.e., in off-chip storage) by other means.
- The product does not protect against access to its functions by individuals not authorized to use the system in which the chip is embedded. 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:

800-007 IBM Cryptographic Security Chip for PC Clients Manufactured by Atmel (AT90SP0801) Common Criteria Security Target, Rev B.

800-002 IBM Secure Signature Chip Administrator Guide, Rev B

800-001 IBM Secure Signature Chip User Guide, Rev B

800-004 IBM Secure Signature Chip Secure Installation Generation Start-up Procedures, Rev B

Datasheet AT90SP0801, 1495AX-07/05/01

Additional unevaluated consumer documentation related to the product is available at
**http://www.pc.ibm.com/ww/security/securitychip.html**

# IT PRODUCT TESTING

## 6.1 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 RIO PC, and testing the chip functions. Most testing is automated using scripts written in the *tcl* language. The *tcl* scripts generate commands on the IBM PC, send commands to the chip, collect results returned from the chip to the PC, and save the commands and results for analysis. The tests 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 developer testing is now exhaustive; all TOE Security Functions in the ST are tested.

The chip is tested as manufactured, with register settings as specified in ***800-002 IBM Secure Signature Chip Administrator Guide, Rev B,* Table 3.1 "Required System Configuration"** (see **Section 8, EVALUATED CONFIGURATION,** below).

## 6.2 Evaluator Testing

The evaluator performed approximately 80% of the developer's test suite of 52 *tcl* test scripts. The evaluator executed 43 of the scripts on the 20-pin SOIC package and 41 of the scripts on the 28-pin package. The only scripts not executed were long-running scripts that test lockout due to authentication failure and a script that permanently locks the chip.

The only security function not tested by the evaluator was the function that permanently locks the chip.

The evaluator also devised a test subset that:

- Covered all classes of security functionality claimed by the Security Target (Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, and Protection of the TSF), and
- Tested the Strength of Function claim.

The following test cases[3] were specified as part of independent team testing and scripted in *tcl*. The test environment and chip configuration were the same as previously described.

0. **Verification of TSF Interface:** Check that commands generated by tcl scripts are sent to the chip and that chip responses displayed by the tcl manager actually came from the chip.

1. **Password Length:** Check that users cannot use a password of length less than eight characters.

2. **Digital Signature with 512 and 1024 bit keys**: Verify that cryptographic functionality is working by decoding a user key and using it to sign a message

3. **Password Mode Byte**: Check sample of cases of password mode byte

4. **Reset Failure Counter with Hardware Password:** Check that authentication with the hardware (administrative) password resets the failed password attempt counter.

[3] The numbering scheme is that used in the Evaluation Technical Report.

5. **Attempt to change Bit 2 of the "Configuration Information Register":** Attempt to write "0" to Bit 2 of the Configuration Information Register ***CONFIG_R***. Bit 2 of this register is supposed to be permanently set to "1".

6. **Comparison of Power Cycle, Reset, and Chip Clear:** Compare register settings and password flags before and after power cycle, chip clear, and reset

7. **Undocumented Commands:** Attempt to perform an invalid command

8. **Undocumented Registers:** Attempt to store into and load from undocumented registers.

All tests gave 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.

# 7 EVALUATED CONFIGURATION

The TOE is a monolithic integrated circuit chip and has no subsystems or discrete components that can be added, removed, or rearranged. It is manufactured in two physical packages, a 20-pin SOIC (Small Outline Integrated Circuit) package and a 28-pin TSSOP (Thin Shrink Small Outline Package) package. The two physical configurations are logically and functionally identical. Both were tested for the evaluation.

The evaluated configuration was as delivered from the factory and described in the document ***800-007 IBM Cryptographic Security Chip for PC Clients Manufactured by Atmel (AT90SP0801) Common Criteria Security Target, Rev B***, with register settings for initialization (including enablement) and operation as specified in ***800-002 IBM Secure Signature Chip Administrator Guide, Rev B,*** **Table 3.1 "Required System Configuration"**.

# 8 RESULTS OF THE EVALUATION[4]

The evaluation determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of **EAL 3 augmented with CC component ADV_SPM.1** (informal security policy model).

# 9 EVALUATOR COMMENTS

There are no Evaluator Comments.

# 10 ANNEXES

There are no annexes to this report.

# 11 SECURITY TARGET

The ST, *IBM Cryptographic Security Chip for PC Clients Manufactured by Atmel (AT90SP0801) Common Criteria Security Target, Rev B,* is included here by reference.

[4] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

# 12 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 |
| SOIC | Small Outline Integrated Circuit |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| TSFI | TSF Interface |
| TSSOP | Thin Shrink Small Outline Package |

# 13 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] IBM Cryptographic Security Chip for PC Clients Manufactured by Atmel (AT90SP0801) Common Criteria Security Target, Rev B.

[8] 800-002 IBM Secure Signature Chip Administrator Guide, Rev B

[9] 800-001 IBM Secure Signature Chip User Guide, Rev B

[10] 800-004 IBM Secure Signature Chip Secure Installation Generation Start-up Procedures, Rev B

[11] Datasheet AT90SP0801, 1495AX-07/05/01