
PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

# Certification Report DCSSI-2008/11

# ATMEL Secure Microcontroller AT90SC12818RCU rev. B

*Paris, 20th of May 2008*

# Courtesy Translation

# Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.
Certification does not, however, constitute a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.dcssi@sgdn.gouv.fr

*Certification report reference*

# DCSSI-2008/11

*Product name*

## ATMEL Secure Microcontroller AT90SC12818RCU rev. B

*Product reference*

## AT90SC12818RCU, reference AT58U14 revision B

*Protection profile conformity*

## PP BSI-PP-0002-2001

*Evaluation criteria and version*

## Common Criteria version 2.3

**compliant with ISO 15408:2005**

*Evaluation level*

## EAL 4 augmented

**AADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4**

*Developer*

## ATMEL Secure Microcontroller Solutions

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

*Sponsor*

## ATMEL Secure Microcontroller Solutions

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

*Evaluation facility*

## Serma Technologies

**30 avenue Gustave Eiffel, 33608 Pessac, France**

**Phone: +33 (0)5 57 26 08 75, email : e.francois@serma.com**

*Recognition arrangements*

**CCRA**

**SOG-IS**

IT Security Certified

**The product is recognised at EAL4 level.**

# Introduction

## The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

# Content

**1. THE PRODUCT ..... 6**

1.1. PRESENTATION OF THE PRODUCT ..... 6
1.2. EVALUATED PRODUCT DESCRIPTION ..... 6
*1.2.1. Product identification ..... 6*
*1.2.2. Security services ..... 6*
*1.2.3. Architecture ..... 7*
*1.2.4. Life cycle ..... 8*
*1.2.5. Evaluated configuration ..... 9*

**2. THE EVALUATION ..... 10**

2.1. EVALUATION REFERENTIAL ..... 10
2.2. EVALUATION WORK ..... 10
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS ..... 10
2.4. RANDOM NUMBER GENERATOR ANALYSIS ..... 10

**3. CERTIFICATION ..... 11**

3.1. CONCLUSION ..... 11
3.2. RESTRICTIONS ..... 11
3.3. RECOGNITION OF THE CERTIFICATE ..... 11
*3.3.1. European recognition (SOG-IS) ..... 11*
*3.3.2. International common criteria recognition (CCRA) ..... 12*

**ANNEX 1. EVALUATION LEVEL OF THE PRODUCT ..... 13**

**ANNEX 2. EVALUATED PRODUCT REFERENCES ..... 14**

**ANNEX 3. CERTIFICATION REFERENCES ..... 16**

# 1. The product

## 1.1. Presentation of the product

The evaluated product is the ATMEL Secure Microcontroller AT90SC12818RCU reference AT58U14 rev. B developed by ATMEL Secure Microcontroller Solutions.
This product belongs to the AVR ASL4 family developed by ATMEL Secure Microcontroller Solutions.

The microcontroller aims to host one or several software applications and can be embedded in a plastic support to create a Smartcard with multiple possible usages (secure identity documents, banking, health card, pay-TV or transport applications…) depending on the Embedded Software applications. However, only the microcontroller is evaluated. The software applications are not in the scope of this evaluation.

## 1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operation environment.

This security target is compliant to [PP0002] protection profile.

### *1.2.1. Product identification*

The configuration list [CONF] identifies the product's constituent elements.
The certified version of the product can be identified by the following elements:

- Product name: AT90SC12818RCU, and product identification number: AT58U14. This information can be checked using Serial number register SN_0, which content should be hexadecimal 0x31 (see [GUIDES], "AT90SC12818RCU Technical Data Sheet" section 23.1.1),
  Silicon revision: B. This information can be checked using Serial number register SN_1, which content should be hexadecimal 0x01 (see [GUIDES], "AT90SC12818RCU Technical Data Sheet" section 23.1.2),
- The TOE can be physically identified by the mask numbers visible on the metal layer, and listed in the "Patern and mask list" document (cf. [CONF]).

### *1.2.2. Security services*

The product provides mainly the following security services:

- Test Mode Entry,
- Protected Test Memory Access,
- Test Mode Disable,
- TOE Testing,
- Data Error Detection,
- FireWall,
- Event Audit,
- Event Action,

- Unobservability,
- Cryptography,
- Package mode entry,
- Test Memory Access in Package Mode.

### *1.2.3. Architecture*

The AT90SC12818RCU microcontroller is made up of:

- AVR Risk processing unit,
- 96Kb of program ROM memory,
- 18Kb of EEPROM program/data memory including 128 bytes of One Time Programmable (OTP) memory and a 384-byte of bit-addressable area,
- 6Kb of static RAM memory,
- a Checksum Accelerator,
- a CRC-16/32 peripheral,
- a Random Number Generator,
- a fast hardware DES/3DES peripheral,
- a 32-bit Cryptographic Accelerator (AdvX for Public Key Operations), with 32kb of ROM memory dedicated to embed a cryptographic library,
- detectors which monitor voltage, frequency and temperature,
- a firewall that protects all memories, peripheral and IO register accesses,
- a power management system,
- logic peripherals including 2 timers, 1 serial port, an ISO7816 interface and an ISO7816 controller, a GPIO port and a SPI port,
- a dedicated test structure that can be used only in test mode for production testing, and sawn before IC packaging.

### *1.2.4. Life cycle*

The product's life cycle is organised as follow:

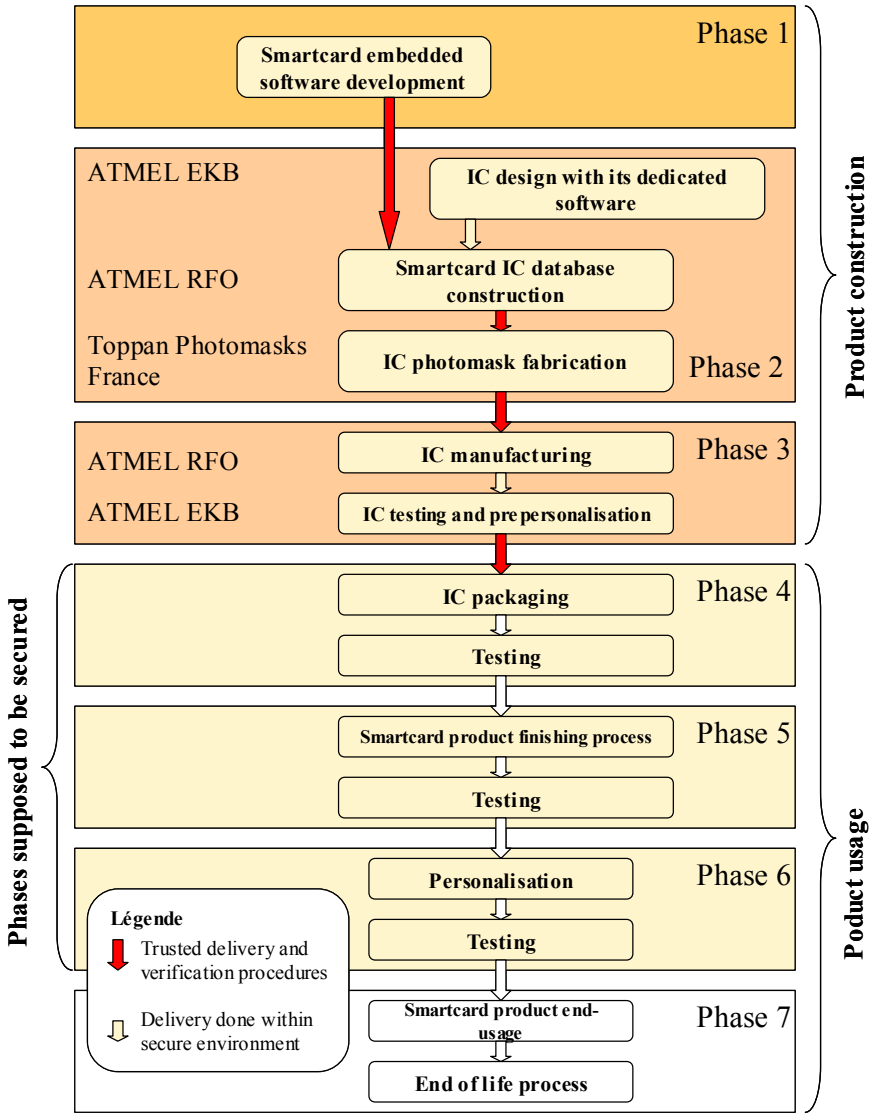


**Figure 1 – standard IC life-cycle**

The product is designed and tested by:

**Atmel East Kilbride**

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

The database of the product and the manufacturing of the product are performed by:

**Atmel Rousset**

Z.I. Rousset Peynier
13106 Rousset Cedex
France.

The photo masks of the product are manufactured by:

**Toppan Photomasks France**

224, bd John Kennedy
91100 Corbeil Essonnes
France.

The product can be in one of its three possible modes:

- "Test" mode: mode in which the microcontroller runs under the control of dedicated test software written to EEPROM via a test interface, and in conjunction with stimulus provided by an external test system. This mode is intended to be used solely by authorized development staff. After the testing activity, the tests interface is definitely deactivated by sawing the wafer and cannot be accessed any more.
- "User" mode: mode, in which the microcontroller runs under control of the smartcard embedded software. It is intended that customers and end-users will always use the microcontroller in user mode.
- "Package" mode: this mode is similar to Test Mode for testing returns from Phases 4-7. Package mode runs a limited subset of test commands via a test interface, and in conjunction with stimulus provided by an external test system. This mode is intended to be used solely by authorized staff.

### *1.2.5. Evaluated configuration*

This certification report applies to the microcontroller only. Any other software used for the evaluation are not part of the scope of certification. In particular, the "toolbox" cryptographic library developer by ATMEL is not part of the evaluation scope.
With regard to the life-cycle, the evaluated product is the one at the end of its manufacturing phase (phase 3).
For the evaluation needs, the product AT90SC12818RCU was provided to the ITSEF with a dedicated test embedded software, in a mode known as "open[1]".

[1] mode that enables to load and execute a native code in EEPROM and also to disable the configurable security mechanisms

# 2. The evaluation

## 2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC] and with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods consistent with [AIS 34], validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] guides have been applied.

## 2.2. Evaluation work

The evaluation technical report [ETR], delivered to DCSSI the 10th of April 2008, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

## 2.3. Cryptographic mechanisms robustness analysis

The evaluated product provides cryptographic services identified §1.2.3, but as these services do not concur to the products security they cannot be analysed from a cryptographic point of view; their robustness depends on the way they are used by the application embedded in the microcontroller.

## 2.4. Random number generator analysis

The evaluated product provides a hardware random number generator that can be used by the embedded software. The generator has been analysed by the evaluator.
The generator reaches [FIPS 140] requirements[1]. However, if the random number generator is used for cryptographic purposes, the hardware-generated numbers shall be reprocessed by a cryptographic algorithm as specified in the document [REF-CRY].

[1] Only the [FIPS 140-2] subset related to random number generators has been evaluated and only regarding the statistical tests specified in the standard.

# 3. Certification

## 3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product ATMEL secure microcontroller AT90SC12818RCU Rev. B submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented.

## 3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

This certificate provides a resistance assessment of the AT90SC12818RCU product to a set of attacks which remains generic due to the missing of any specific embedded application. Therefore, the security of a final product based on the evaluated microcontroller would only be assessed through the final product evaluation, which could be performed on the basis of the current evaluation results.

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

## 3.3. Recognition of the certificate

### *3.3.1. European recognition (SOG-IS)*

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:


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

### *3.3.2. International common criteria recognition (CCRA)*

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[1], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

1 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

# Annex 1. Evaluation level of the product

| Class | Family | Components by assurance level | | | | | | | Assurance level of the product | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 4+ | Name of the component |
| **ACM Configuration management** | ACM_AUT | | | | **1** | 1 | **2** | 2 | **1** | Partial CM automation |
| | ACM_CAP | **1** | **2** | **3** | **4** | 4 | **5** | 5 | **4** | Configuration support and acceptance procedures |
| | ACM_SCP | | | **1** | **2** | **3** | 3 | 3 | **2** | Problem tracking CM coverage |
| **ADO Delivery and operation** | ADO_DEL | | **1** | 1 | **2** | 2 | 2 | **3** | **2** | Detection of modification |
| | ADO_IGS | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Installation, generation and start-up procedures |
| **ADV Development** | ADV_FSP | **1** | 1 | 1 | **2** | **3** | 3 | **4** | **2** | Fully defined external interfaces |
| | ADV_HLD | | **1** | **2** | 2 | **3** | **4** | **5** | **2** | Security enforcing high-level design |
| | ADV_IMP | | | | **1** | **2** | **3** | 3 | **2** | Implementation of the TSF |
| | ADV_INT | | | | | **1** | **2** | **3** | | |
| | ADV_LLD | | | | **1** | 1 | **2** | 2 | **1** | Descriptive low-level design |
| | ADV_RCR | **1** | 1 | 1 | 1 | **2** | 2 | **3** | **1** | Informal correspondence demonstration |
| | ADV_SPM | | | | **1** | **3** | 3 | 3 | **1** | Informal TOE security policy model |
| **AGD Guidance** | AGD_ADM | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | Administrator guidance |
| | AGD_USR | **1** | 1 | 1 | 1 | 1 | 1 | 1 | **1** | User guidance |
| **ALC Life-cycle support** | ALC_DVS | | | **1** | 1 | 1 | **2** | 2 | **2** | Sufficiency of security measures |
| | ALC_FLR | | | | | | | | | |
| | ALC_LCD | | | | **1** | **2** | 2 | **3** | **1** | Developer defined life-cycle model |
| | ALC_TAT | | | | **1** | **2** | **3** | 3 | **1** | Well-defined development tools |
| **ATE Tests** | ATE_COV | | **1** | **2** | 2 | 2 | **3** | 3 | **2** | Analysis of coverage |
| | ATE_DPT | | | **1** | 1 | **2** | 2 | **3** | **1** | Testing: high-level design |
| | ATE_FUN | | **1** | 1 | 1 | 1 | **2** | 2 | **1** | Functional testing |
| | ATE_IND | **1** | **2** | 2 | 2 | 2 | 2 | **3** | **2** | Independent testing – sample |
| **AVA Vulnerability assessment** | AVA_CCA | | | | | **1** | **2** | 2 | | |
| | AVA_MSU | | | **1** | **2** | 2 | **3** | 3 | **3** | Analysis and testing of insecure states |
| | AVA_SOF | | **1** | 1 | 1 | 1 | 1 | 1 | **1** | Strength of TOE security function evaluation |
| | AVA_VLA | | **1** | 1 | **2** | **3** | **4** | 4 | **4** | Highly resistant |

# Annex 2. Evaluated product references

| | |
|---|---|
| [ST] | Reference security target for the evaluation:<br>- Artemis Security Target,<br>Reference : Artemis_ST_V1.3_07Oct07<br>Atmel Secure Microcontroller Solutions<br>For the needs of publication, the following security target has been provided and validated in the evaluation:<br>- AT90SC12818RCU Security Target Lite,<br>Reference: TPG0166A_06Mar08<br>Atmel Secure Microcontroller Solutions |
| [ETR] | Evaluation technical report :<br>- ARTEMIS project - Evaluation Technical Report - AT90SC12818RCU,<br>Reference: ARTEMIS_ETR_V1.0<br>Serma Technologies<br>For the needs of composite evaluation with this microcontroller a technical report for composition has been validated:<br>- Evaluation Technical Report Lite – ARTEMIS project,<br>Référence : ARTEMIS_ETR_Lite_V1.0<br>Serma Technologies |
| [CONF] | The configuration list is:<br>- Artemis_Design Configuration List,<br>Reference: Artemis_DCL_V1.0_27Apr07<br>Atmel Secure Microcontroller Solutions<br>- Artemis Manufacturing Configuration List,<br>Reference: Artemis_MCL_V1.1_RevB_10Apr07<br>Atmel Secure Microcontroller Solutions<br>- Artemis Pattern and Mask list,<br>Reference: Artemis PML V1.0_13Jun07<br>Atmel Secure Microcontroller Solutions<br>- Artemis Deliverables list,<br>Reference: Artemis_EDL_V1.15_19Mar08<br>Atmel Secure Microcontroller Solutions |
| [GUIDES] | Guidance of the product:<br>- AT90SC CC AGD Interface,<br>Reference: AT90SC_GUID_V1.5_19Jul07<br>Atmel Secure Microcontroller Solutions<br>- AT90SC12818RCU Technical Datasheet,<br>Reference: TPR0249AX_16May07<br>Atmel Secure Microcontroller Solutions<br>- AT90SC Addressing Modes and Instruction Set,<br>Reference: 1323C-03May04<br>Atmel Secure Microcontroller Solutions |

| | |
|---|---|
| | - Using the supervisor and user modes on the AT90SC ASL4 products,<br>Reference: TPR0095BX_07Jun07<br>Atmel Secure Microcontroller Solutions<br>- Security Recommendations for AT90SC ASL4 Products,<br>Reference: TPR0066H_31Jan08<br>Atmel Secure Microcontroller Solutions<br>- Secure Hardware DES and Triple DES on AT90SC ASL4 Products,<br>Reference: TPR0063IX_05Dec07<br>Atmel Secure Microcontroller Solutions<br>- Generating unpredictable random numbers on the AT90SC family devices,<br>Reference: 1573CX_SMIC_21mar03<br>Atmel Secure Microcontroller Solutions<br>- Generation of Random Numbers with a Controlled Entropy on AT90SC,<br>Reference: TPR0166BX_27Jun06<br>Atmel Secure Microcontroller Solutions<br>- Efficient use of AdvX for Implementing Cryptographic Operations,<br>Reference: TPR0142CX_14Jun05<br>Atmel Secure Microcontroller Solutions<br>- AdvX™ for AT90SC Family Datasheet,<br>Reference: TPR0116CX_13Dec06<br>Atmel Secure Microcontroller Solutions<br>- Wafer Saw Recommendations,<br>Reference: TPG0079A_13Jun05<br>Atmel Secure Microcontroller Solutions |
| [PP0002] | Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0002-2001.* |

# Annex 3. Certification references

| | |
|---|---|
| Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems. | |
| [CER/P/01] | Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation:<br>Part 1: Introduction and general model,<br>August 2005, version 2.3, ref CCMB-2005-08-001;<br>Part 2: Security functional requirements,<br>August 2005, version 2.3, ref CCMB-2005-08-002;<br>Part 3: Security assurance requirements,<br>August 2005, version 2.3, ref CCMB-2005-08-003.<br>The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005. |
| [CEM] | Common Methodology for Information Technology Security Evaluation: Evaluation Methodology,<br>August 2005, version 2.3, ref CCMB-2005-08-004.<br>The content of CEM version 2.3 is identical to the international ISO/IEC 18045:2005. |
| [CC IC] | Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006. |
| [CC AP] | Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2007-04-001 version 2.3, revision 1, April 2007. |
| [CC RA] | Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000. |
| [SOG-IS] | «Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group. |
| [REF-CRY] | Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.10, 14th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR |
| [AIS 34] | Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, Bundesamt für Sicherheit in der Informationstechnik |
| [FIPS 140] | Security Requirements for Cryptographic Modules |

| | |
|---|---|
| | Reference: FIPS PUB-140-2:1999, NIST |