Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0245-2005

for

SM4128 (V3) A5-step module

from

Sharp Corporation

Deutsches
IT-Sicherheitszertifikat

erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI
Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0245-2005

SM4128 (V3) A5-step module

from

Sharp Corporation

IT Security Certified

SOGIS-MRA

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, Part 1 Version 0.6*, *Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

Functionality:	**product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 augmented by** **ADV_IMP.2 (Implementation of the TSF),** **ALC_DVS.2 (Sufficiency of security measures),** **AVA_MSU.3 (Analysis and testing for insecure states) and** **AVA_VLA.3 (Moderately resistant)**

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 20. September 2005
The President of the Federal Office
for Information Security

Common Criteria

Dr. Helmbrecht   L.S.

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 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.

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)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
- Part 1, Version 0.6
- Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

[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 7 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 22nd September 2000 in the Bundesanzeiger p. 19445

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.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 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 levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

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 SM4128 (V3) A5-step module, has undergone the certification procedure at BSI.

The evaluation of the product SM4128 (V3) A5-step module, was conducted by TNO ITSEF BV. TNO ITSEF BV is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Sharp Corporation

2613-1, Ichinomoto-cho,

Tenri, Nara 632-8567

Japan

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 20. September 2005.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-22 and D1 to D4.

The product SM4128 (V3) A5-step module, has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Sharp Corporation
2613-1, Ichinomoto-cho,
Tenri, Nara 632-8567
Japan

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.

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) is the SM4128 (V3) A5-step module (a packaged IC), hereafter called SM4128 (V3). This Sharp dual interface type module has interfaces for contact and contact-less communications, physical and logical protection mechanisms, DES and RSA/ECC coprocessors.

This module is intended for exclusive use with the Sharp software in national ID cards and electronic passports. It is not intended for general usage.

The TOE physically consists of a packaged module containing the following:

- The circuitry of an IC (hardware, including the physical memories RAM, ROM and Flash ROM (FROM))
- TSF data stored in the IC
- The following IC dedicated software:
- BootROM (including DRNG function)
- TestROM (test functionality is disabled before TOE delivery)

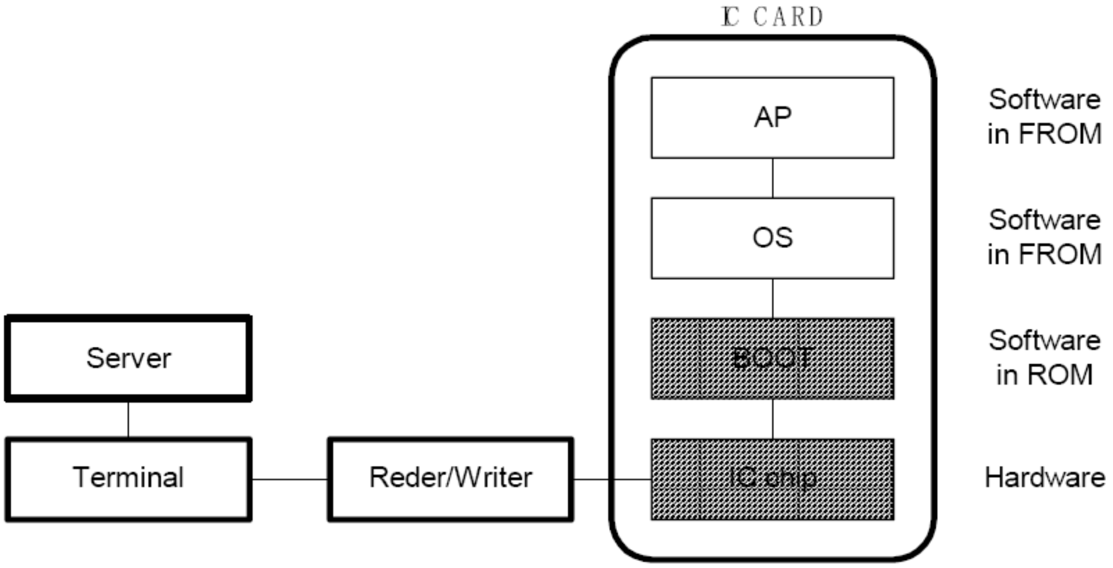


Figure 1: System Configuration

A detailed description of the TOE can be found in chapter 5 of this document.

The IT product SM4128 (V3) A5-step module, was evaluated by TNO ITSEF BV. The evaluation was completed on 29.07.2005. TNO ITSEF BV is an evaluation facility (ITSEF)[8] recognised by BSI.

[8] Information Technology Security Evaluation Facility

The sponsor ,vendor and distributor is

Sharp Corporation
2613-1, Ichinomoto-cho,
Tenri, Nara 632-8567
Japan

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented ADV_IMP.2 (Implementation of the TSF), ALC_DVS.2 (Sufficiency of security measures), AVA_MSU.3 (Analysis and testing for insecure states) and AVA_VLA.3 (Moderately resistant)).

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 conformant as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Identifier**
FDP	**User data protection**
FDP_IFC.1	Subset information flow control
FDP_ITT.1	Basic internal transfer protection
FPT	**Protection of the TSF**
FPT_FLS.1	Failure with preservation of secure state
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_PHP.3	Resistance to physical attack
FPT_SEP.1	TSF domain separation
FRU	**Fault tolerance**
FRU_FLT.2	Limited fault tolerance

Table 1:SFRs CC part 2 conformant

The following SFRs are CC part 2 extended:

Security Functional Requirement	**Identifier**
FAU	**Security audit**
FAU_SAS.1	Audit review
FCS	**Cryptographic support**
FCS_RND.1	Audit review
FMT	**Security management**
FMT_LIM.1	Security management
FMT_LIM.2	Security management

Table 2:SFRs CC part 2 conformant

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target [6], chapter 5.

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

SF.Passivation
The complete top layer of the IC, except for the bond pads, is covered with a passivation layer making physical attack difficult.

SF.Module
The IC (including the passivation layer) is covered with resin making physical attack difficult.

SF.Flat_Layout
The TOE's wiring rule for the logic circuits, which is called "Flat-layout", does not have hierarchies. This makes it difficult for an attacker to find the signals between the logical circuits (CPU, CPU Bus, Reset Circuit, Clock Circuit, I/O Port, Timer, UART, SCI, Memory Protect Circuit, Flash Interface, Protocol Controller, Type C Protocol Controller, Contact/Contact-less Detector, RF Interface, Crypto Accelerator, DES Circuit, PLL Lock Detector, Test Circuit).

SF.Narrow_Wiring
The wiring space of the IC is very narrow, making it difficult to change the IC or read data from it.

SF.Bus_Scrambling
The bus between the CPU and memories (Flash, ROM, RAM and coprocessor RAM) is scrambled, making it difficult to read data from it.

SF.Shielding_Layer
The two top layers of the IC (part of the TOE) are shielding layers, one passive

and one active.If the active shield is broken, the TOE does not operate, making physical attacks difficult.

SF.Watchdog_Timer
The TOE has a watchdog timer, which resets the TOE when it times out.

SF.Odd_Address
The TOE resets when it detects an odd address violation.

SF.Illegal_Instruction
The TOE resets when it detects an illegal instruction.

SF.Abnormal_Internal_Clock
The TOE resets when it detects that the period of the high level or low level of the internal clock is outside of the range FSYS_tmin specified in [FSP].

SF.Abnormal_RF_Clock
The TOE resets when, in contact-less mode, it detects that the period of the high level or low level of the RF clock outside of the range RFCS_tmin specified in [FSP].

SF.Abnormal_Temperature
The TOE resets when it detects a temperature higher than TMPS_Tmax or lower than TMPS_Tmin specified in [FSP].

SF.Abnormal_Voltage_Flash
Flash memory uses 2 power-sources. One is the internal voltage. The other is the internal program voltage.
The TOE resets when it detects the internal voltage for the flash component is less then VFFS_VL or more then VFFS_VH specified in [FSP]

SF.Abnormal_Voltage_Logic
The TOE resets when it detects an internal voltage for the logic components is less then VDDS_VL or more then VDDS_VH specified in [FSP]

SF.Over-Voltage_Protector
Should the voltage of the internal supply power (VCC) become too high, then the TOE will absorb excess power up to a limit. If the absorbed power is too high, the TOE will disable itself permanently.

SF.Power_Regulator
The TOE regulates the internal power voltages VAA, VDD, VFF and VPPO from the internal supply power VCC.

SF.PLL
The TOE regulates the internal clock in contact operation.

SF.Blocked_Test_Pins
The test pins, which are defined in [FSP], of the TOE are irreversibly blocked before the TOE is shipped to the customer

SF.Memory_Protect
The TOE enforces the following memory protection:
If the Memory Protect is On: read/write access to the RAM is allowed except for:

- Read/write access to the OS stack area
- Read/write access to the OS working area
- Read/write access to the co-processor shared RAM area unless explicitly enabled

read/write access to all other memory areas is denied, except for:

- Read access to the application area
- Read/write access the General Purpose Registers except the SYS register.

SF.Memory_Protect_On: The TOE ensures that only Software running with the Memory Protect Off can turn the Memory Protect On.

SF.Memory_Protect_Off: The TOE ensures that Software running with the Memory Protect On can turn the Memory protect Off only by:

- returning control to the Software in the SCALL relief area with the SCALL instruction, or
- returning control to the Software in the SRET relief area with the SRET instruction, or
- to the interrupt handling Software by generating an interrupt.

SF.FLASH
The TOE has flash memory capable of storing initialisation data and/or pre-personalisation data and/or supplements of the Smartcard Embedded Software.

SF.RNG
The TOE has Deterministic Random Number Generator that meets the AIS20 K3 requirements.

1.3 Strength of Function

The TOE’s strength of functions is claimed high (SOF-high) for SF.RNG. 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).

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats which were partly taken from [8] for the evaluation and averted by the TOE are specified in the Security Target [6]:

- T.Leak-Inherent
- T.Phys-Probing
- T.Malfunction
- T.Phys-Manipulation

- T.Leak-Forced
- T.Abuse-Func
- T.RND
- T.Mem-Acess

The OSP is also specified in the Security Target:

- P.Process-TOE

1.5 Special configuration requirements

The TOE has two different operating modes, user mode and test mode. The application software being executed on the TOE cannot use the test mode. The TOE is delivered as a hardware unit at the end of the IC packaging process (Phase 4). At this point in time the operating system software is already stored in the non-volatile memories of the chip and the test mode is disabled. Thus there are no special procedures for generation or installation that are important for a secure use of the TOE. The further production and delivery processes, like the Smartcard finishing process, personalisation and the delivery of the smartcard to an end user, have to be organized in a way that excludes all possibilities of physical manipulation of the TOE. There are no special security measures for the startup of the TOE besides the requirement that the controller has to be used under the well-defined operating conditions and that the requirements on the software have to be applied as described in the user documentation.

1.6 Assumptions about the operating environment

- It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use
- It is assumed that the Smartcard Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software
- It must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context. Details must be specified in the application context

1.7 Disclaimers

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

No	Type	Identifier	Release	Form of Delivery
1	Hardware	Hardware SM4128 (V3)	A5 step	Packaged module
2	Software	HERMES_BOOT_V100.hex	1.0.0	included in BootROM
3	Software	IC dedicated test software	1.4	included in TestROM
4	Documentation	Technical Document of SM4128 (V3) [9]	1.4.0	paper
5	Documentation	Combination Type Smart Card LSI HERMES Bootstrap program Functional Specification [10]	0.6.0	paper

Table 3: Deliverables to customer

3 Security Policy

The TOE Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phase 2 up to TOE Delivery, refer to [7]) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data shall be guaranteed; access to samples, development tools and other material shall be restricted to authorised persons only; scrap will be destroyed etc. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Smartcard Embedded Software and therefore especially to the Smartcard Embedded Software itself. This includes the delivery (exchange) procedures for Phase 1 and the Phases after TOE Delivery as far as they can be controlled by the TOE Manufacturer. An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

The security policy of the TOE is to provide basic security functions to be used by the smartcard operating system and the smartcard application thus providing an overall smartcard system security. Therefore the TOE will provide a random number generatior of appropriate quality.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE shall:

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of security functions (security mechanisms and associated functions) provided by the TOE.

4. Assumptions and Clarification of Scope

4.1 Usage assumptions

- It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery (refer to Sections 2.1 and 8.1 of [8]) are assumed to be protected appropriately. For a preliminary list of assets to be protected refer to paragraph 80 (page 22) [8].
- The Smartcard Embedded Software has to be designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software. Note that particular requirements for the Smartcard Embedded Software are often not clear before considering a specific attack scenario during vulnerability analysis of the smartcard integrated circuit (AVA_VLA). Therefore, such results from the TOE evaluation (as contained in the Evaluation Technical Report (ETR)) can be given to the developer of the Smartcard Embedded Software in an appropriate and authorised form (e.g. ETR Lite for composition according to AIS 36 [4]) and be taken into account during the evaluation of the software. This may also hold for additional tests being required for the combination of hardware and software.
- All User Data are owned by Smartcard Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context. Details must be specified in the application context.

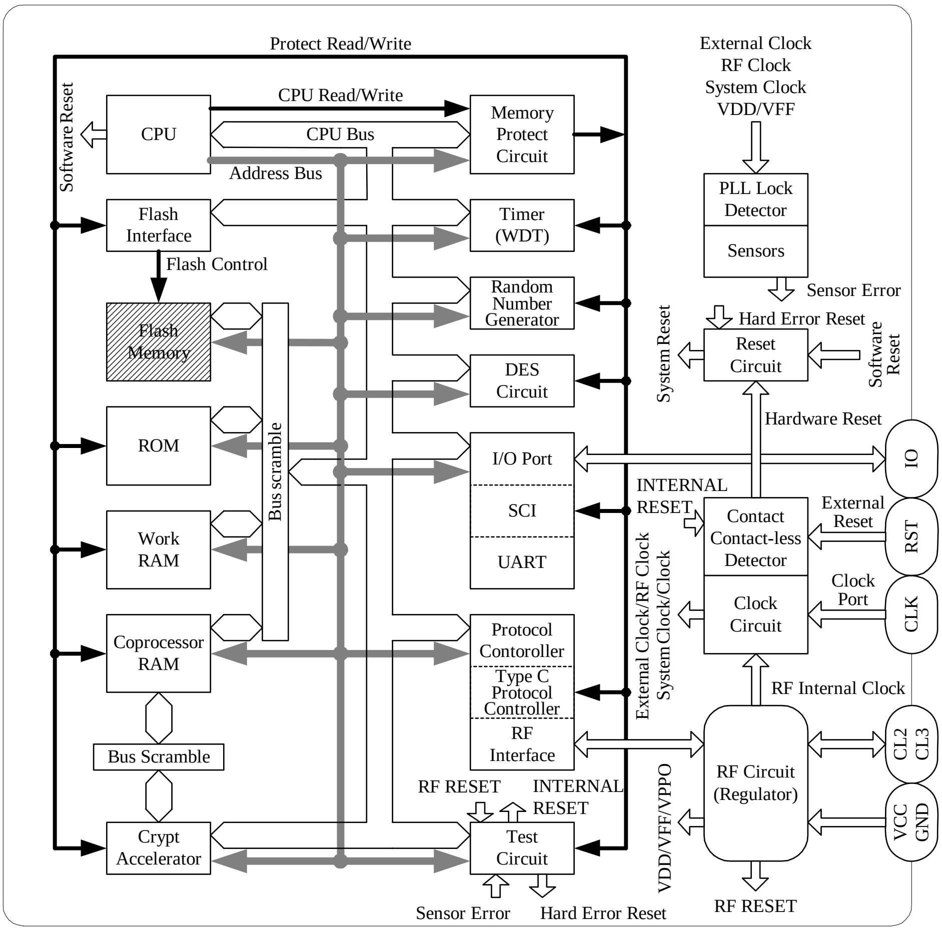
4.2 Clarification of scope

The SM4128 (V3) A5-step module is intended for exclusive use with the Sharp software electronic passports. It is not intended for general usage. Smartcard Embedded Software (outside of TOE) may be loaded in and executed from the

Flash ROM (logically outside the TOE). DES and RSA/ECC encryption and the functionality of the corresponding modules are also not considered as part of the TSF.

5. Architectural Information

The TOE looks like this internally:



NOTE: □ is powered by VDD

▨ is powered by VDD/VFF/VPPO

⬭ is powered by VCC

Figure 2: Block diagram of the TOE

The TOE is intended for use in an E-passport application with Sharp software only.

The TOE physically consists of a packaged module containing the following:

The circuitry of an IC (hardware, including the physical memories RAM, ROM and Flash ROM (FROM))

1. CPU Sharp original 16 bit CPU
   - General purpose register construction, 16 bit x 16
   - 62 basic commands including bit manipulation command, bit transfer instruction and bit branch instruction suitable for controlling application.
   - High speed multiplication and division instructions (16 bit x 16 bit, 16 bit / 16 bit, 32 bit /16 bit)
   - 10 types of addressing mode
   - 16M bytes address space
   - Data automatic transfer function (DTS) for highly functional interrupt processing. It is possible to automatically transfer data using hardware instead of interrupt processing when generating the demand for interrupt. Continuous operation of each type of function block is possible using DTS and continuous storage of the results and data is possible.
   - CPU clock switching function.
     CONTACT Mode: Multiplication x 3 of the CLK PORT which is input from the CLK pin and x 3/8 can be selected.
     CONTACT-LESS Mode: Multiplication x 1 of the RF CLOCK and x 1/8 can be selected.
2. Memory
   - ROM 8k Byte
   - RAM 8k Byte
   - Coprocessor RAM 1664 Byte
   - Flash memory 1024k Byte
3. Terminal for IC card ISO/IEC 7816 base
   - Communications method
   - <Contact operation>
   - ISO/IEC 7816 base T=0 & T=1 protocol
   - Operating power voltage: 2.7 - 5.5V
   - Input clock frequency: 1.0 - 5.0 MHz
   - <Contact-less operation>
   - ISO14443-2 TypeB 106kbps - 424kbps
   - The anti-collision is compatible with the slot marker method
4. Interrupt
   - In addition to a total of 15 types of interrupt, software interrupt is also possible.
   - Mask capable interrupt 15 types (external 1: internal 14)
   - Non-maskable interrupt 6 types

5. Crypto Accelerator
    - RSA/ECC Crypto Accelerator integrated.
    - DES Circuit integrated.
6. Timer
    - 16 bit compare type timer 2
    - 8 bit watch dog timer 1
7. Serial interface: Asynchronous simultaneous (UART) 1 channel
8. PLL: Integrated PLL generates an operating clock for CPU and for Crypto Accelerator in contact operation.
9. Base Register: By storing the start address of the applications in Base Register, multi applications are available easily.
10. Hardware seed generator for the software DRNG
11. Watchdog Timer: The SM4128(V3) is reset when the time out occurs.
12. Odd Address Access: The SM4128(V3) is reset when the violation of the odd address access occurs.
13. Illegal Instruction: The SM4128(V3) is reset when the illegal instruction occurs.
14. Sensors: The SM4128(V3) is reset when the sensors detect an out of the specified value.
15. Over-voltage Protector: The SM4128(V3) limits the internal voltage VCC.
16. Voltage Regulator: The SM4128(V3) generates four voltages such as VPPO, VFF, VDD and VAA from the VCC voltage.
17. Memory Protection: The SM4128(V3) is reset when the violation of the memory protection occurs.
18. Bus Scramble: The data bus between the CPU and the memory is scrambled as the countermeasure for the physical attacks such as the reading and the rewriting the data bus with the probing.
19. Module: The chip is covered with a resin. The module prevents an attacker from looking at the circuits of the chip because it is difficult to scratch the resin off.
20. Passivation: The surface of the chip is covered with a passivation. The passivation prevents an attacker from probing the circuits directly.
21. Shielding Layer (Wire Break Down Sensor): The shielding layer covers the circuits. The wire break down sensor responds and the SM4128(V3) is reset when the shielding layer is scratched off.

The following is the software of the TOE:

BootROM (including DRNG function)

TestROM (test functionality is disabled before TOE delivery)

6 Documentation

The following documentation is provided with the product by the developer to the customer for secure usage of the TOE in accordance with the Security Target:

- Technical Document of SM4128 (V3), Version 1.4.0, December 28th, 2004 [9]
- Combination Type Smart Card LSI HERMES Bootstrap program Functional Specification, Version 0.6.0, January 13th, 2005 [10]

7 IT Product Testing

The develover tests cover all Security Functions and all security mechanisms as identified in the fuctional specification and the high level design.

The functional testing of SM4128 (V3) can be devided in

- tests which are performed in a simulation environment for analogue and digital simulations,
- layout tests by testing the implementation by optical control, in order to verify statements concerning the layout design.
- functional tests

The evaluators conducted the independent testing and penetration testing in conjunction.

- Independent testing: The evaluators designed a series of tests to test special security functions. All test results were as expected.
- The penetration testing effort can be summarized as follows:

1. The evaluators assessed all possible vulnerabilities found during evaluation of the classes. This resulted in a shortlist with a number of possible vulnerabilities to be tested.
2. The evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis has assessed all information. The attack tree technique was used for this assessment.
3. The evaluators tested the claims made by the developer, which the evaluators deemed worth further investigation, based on the vulnerability analysis.

All test results were as expected.

8 Evaluated Configuration

The TOE is identified by SM4128 (V3) A5-step module. There is only one evaluated configuration of the TOE. All information of how to use the TOE and its security functions by the software is provided within the user documentation.

The TOE has two different operating modes, user mode and test mode. The application software being executed on the TOE can not use the test mode. Thus, the evaluation was mainly performed in the user mode. For all evaluation activities performed in test mode, there was a rationale why the results are valid for the user mode, too.

9 Results of the Evaluation

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 identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4], AIS 34]).

For smart card IC specific methodology the CC supporting documents

(i.) Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators

(ii.) The Application of CC to Integrated Circuits and

(iii.) Application of Attack Potential to Smartcards

(see [4], AIS 20, AIS 25, AIS 26]) were used. The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.3 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		Verdict
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Modularity	ADV_INT.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Sufficiency of security measures	ALC_DVS.2	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS

Assurance classes and components		**Verdict**
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Analysis and testing for insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Moderately resistant	AVA_VLA.3	PASS

Table 3: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.3
- The following TOE Security Function fulfil the claimed Strength of Function:
  SF.RNG according to AIS 20 [4]
  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). DES and RSA/ECC functionality and vulnerability assessment was not part of the evaluation.

The results of the evaluation are only applicable to the SM4128 (V3) A5-step module, produced in the sites as listed in part D, Annex A of this report.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documents [9] - [10] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

Annex A: Evaluation results regarding the development and production environment (see part D of this report).

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 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.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

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

- AIS 20, Version 1, 2 December 1999 for: CC Supporting Document, - Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators, version 2.0, 2 December 1999
- AIS 25, Version 2, 29 July 2002 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 1.2, July 2002
- AIS 26, Version 2, 6 August 2002 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 1.1, July 2002
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 36 Version 1, 29 July 2002 for CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2, March 2002

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

[6] Security Target BSI-DSZ-0245-2005, Version 1.8.5, March 29th, 2005, SM4128(V3) LSI FOR USE IN NATIONAL IDS AND PASSPORTS WITH SHARP SOFTWARE SECURITY TARGET,

[7] Evaluation Technical Report, Version 3.0, July 29th, 2005, Evaluation Technical Report Sharp SM4128(V3) A5 step - EAL4+ (confidential document)

[8] Protection Profile BSI-PP-0002-2001 - „Smartcard IC Platform Protection Profile“, Version 1.0, July 2001

[9] Technical Document of SM4128(V3), Version 1.4.0, December 28th, 2004

[10] Combination Type Smart Card LSI HERMES Bootstrap program Functional Specification, Version 0.6.0, January 13th, 2005

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class 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
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping

Evaluation assurance levels (chapter 6)

„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 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 6.1)

Table 6.1 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 2 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 CC 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 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„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 6.2.2)

„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 6.2.3)

„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 6.2.4)

„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 6.2.5)

„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 6.2.6)

„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 6.2.7)

„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 14.3)

AVA_SOF Strength of TOE security functions

„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 14.4)

AVA_VLA Vulnerability analysis

„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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0245-2005

Evaluation results regarding development and production environment

The IT product, SM4128 (V3) A5-step module (Target of Evaluation, TOE) has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0, extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC15408: 1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

As a result of the TOE certification, dated 20. September 2005, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

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

are fulfilled for the development and production sites of the TOE listed below ((a) – (e)):

(a) Sharp Makuhari, 1-9-2, NAKASE, MIHAMA-KU, CHIBA-SHI, CHIBA 261-8520, Japan

(b) Sharp Tenri, 2631-1, ICHINOMOTO-CHO, TENRI-SHI, NARA 632-8567, Japan

(c) Toppan Printing Co. Ltd., 1101-20, MYOHOJI-CHO, YOHKAICHI-SHI, SHIGA 527-8566, Japan

(d) Sharp Fukuyama, 1, ASAHI, DAIMON-CHO, FUKUYAMA-SHI, HIROSHIMA 721-8522, Japan

(e) Sharp Takaya Electronic Industry Co. Ltd., 3121-1, SATOMI, SATOSHO-CHO, ASAKUCHI-GUN, OKAYAMA 719-0301, Japan

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target (Security Target BSI-DSZ-0245-2005, Version 1.8.5, March 29th, 2005, SM4128 (V3) LSI FOR USE IN NATIONAL IDS AND PASSPORTS WITH SHARP SOFTWARE SECURITY TARGET).

The evaluators verified, that the threats and the security objective for the life cycle phases 2, 3 and 4 up to delivery at the end of phases 3 or 4 as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.