Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0389-2007

for

SM4148 LSI module for Smart Card

from

Sharp Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0389-2007

SM4148 LSI module for Smart Card

from

Sharp Corporation

Common Criteria Arrangement
for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, version 2.3* (ISO/IEC 15408:2005) 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 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0002-2001**
Functionality:	**BSI-PP-0002-2001 conformant plus product specific extensions 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 (Sufficieny of security measures), AVA_MSU.3 (Analysis and testing for insecure states) and AVA_VLA.4 (Highly 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, 3. July 2007

The Vice President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Hange L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

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 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

---

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

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

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

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

2 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 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been 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). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of 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 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 the arrangement has been signed by the national bodies of:

Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America.

The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

This evaluation contains the components ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of these assurance families are relevant.

3 Performance of Evaluation and Certification

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

The product SM4148 LSI module for Smart Card has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0245-2005.

The evaluation of the product SM4148 LSI module for Smart Card was conducted by Brightsight. Brightsight is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Sharp Corporation
System-Flash Division IC Group
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 3. July 2007.

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-18 and D1 to D-4.

The product SM4148 LSI module for Smart Card, 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
System-Flash Division IC Group
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 SM4148 LSI module for Smart Card (a packaged IC) produced in the 4th factory of Sharp Corporation at Fukuyama, hereafter called SM4148.

The SM4148 is a dual interface type module providing a hardware platform to a smard card operating system and smard card application software with interfaces for contact and contactless communications, physical and logical protection mechanisms, DES and modular multiplication coprocessors.

The SM4148 is intended for use in high security applications, for example national ID cards and electronic passports.

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

- The circuitry of an IC (hardware including physical memories RAM, ROM and Flash ROM (FROM) providing a secure execution environment for programs and the physical interaction with the reader/writer
- TSF data stored in the IC
- The following IC dedicated software:
  - BootROM, IC dedicated software for starting the OS (OS itself is outside of the TOE and a DRNG function
  - TestROM (test functionality is disabled before TOE delivery)

The SM4148 was evaluated by Brightsight. The evaluation was completed on 27. April 2007. Brightsight is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Sharp Corporation
System-Flash Division IC Group
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). The following table shows the augmented assurance components.

[8] Information Technology Security Evaluation Facility

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+ ADV_IMP.2	Development – Implementation of the TSF
+ ALC_DVS.2	Life cycle support – Sufficiency of security measures
+ AVA_MSU.3	Vulnerability assessment - Analysis and testing for insecure states
+ AVA_VLA.4	Vulnerability assessment - Highly resistant

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

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

The following SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
FCS	**Cryptographic support**
FCS_COP.1 [DES]	Cryptographic operation
FDP	**User data protection**
FDP_ACC.1	Security attribute based access control
FDP_ACF.1	Subset access control
FDP_IFC.1	Subset information flow control
FDP_ITT.1	Basic internal transfer protection
FMT	**Security management**
FMT_MSA.1 [On]	Management of security attributes
FMT_MSA.1 [Off]	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
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 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Addressed issue
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 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.

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

TOE Security Function	Addressed issue
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 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.
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 is scrambled, making it difficult to read data from it.
SF.Shielding_Layer	The two top layers of the IC 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 allowed range.
SF.Abnormal_RF_Clock	The TOE resets when, in contactless mode, it detects that the period of the high level or low level of the RF clock outside of the allowed range.
SF.Abnormal_Temperature	The TOE resets when it detects a temperature outside of the allowed range.
SF.Abnormal_Voltage_Flash	Flash memory uses 2 power-sources. One is the internal

TOE Security Function	Addressed issue
	voltage. The other is the internal program voltage. The TOE resets when it detects the internal voltage for the flash component is outside of the allowed range.
SF.Abnormal_Voltage_Logic	The TOE resets when it detects an internal voltage for the logic components is outside of the allowed range.
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 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.DES	The TOE has a coprocessor capable of providing DES encryption and decryption. This coprocessor is difficult to analyse with SPA/DPA and difficult to influence with DFA.
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.

Table 4: Security Functions

For more details please refer to the Security Target [7], chapter 6.1.

1.3 Strength of Function

The TOE's strength of functions is claimed 'high' (SOF-high) for specific functions as indicated in the Security Target [7, chapter 6.2].

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

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

The threats which were assumed for the evaluation and averted by the TOE and the organisational security policies defined for the TOE are specified in the Security Target [7] and can be summarised as follows.

It is assumed that the attacker is a human being or a process acting on behalf of him.

So called standard high-level security concerns defined in the Protection Profile [8] were derived from considering the end-usage phase (phase 7 of the life cycle as described in the Security Target) as follows:

- manipulation of user data and of the smart card Embedded Software (while being executed/processed and while being stored in the TOE's memories),
- disclosure of user data and of the smart card Embedded Software (while being processed and while being stored in the TOE's memories) and
- deficiency of random numbers.

These high-level security concerns are refined in the Protection Profile [8] and used by the Security Target [7] by defining threats on a more technical level for

- Inherent Information Leakage,
- Physical Probing,
- Physical Manipulation,
- Malfunction due to Environmental Stress,
- Forced Information Leakage,
- Abuse of Functionality and
- Deficiency of Random Numbers.

In addition, a threat concerning Memory Access Violation is specified.

Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions (see below).

The development and production environment starting with phase 2 up to TOE Delivery are covered by an organisational security policy outlining that the IC developer / manufacturer must apply the policy "Protection during TOE

Development and Production (P.Process-TOE)" so that no information is unintentionally made available for the operational phase of the TOE. The Policy ensures confidentiality and integrity of the TOE and its related design information and data. Access to samples, tools and material must be restricted.

A specific additional security functionality for DES encryption and decryption must be provided by the TOE according to an additional security policy defined in the Security Target.

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

With respect to the life cycle defined in the Security Target, Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by these assumptions:

The developer of the Smartcard Embedded Software (Phase 1) must ensure:

- the appropriate "Usage of Hardware Platform (A.Plat-Appl)" while developing this software in Phase 1. Therefore, it has to be ensured, that the software fulfils the assumptions for a secure use of the TOE. In particular the assumptions imply that developers are trusted to develop software that fulfils the assumptions.
- the appropriate "Treatment of User Data (A.Resp-Appl)" while developing this software in Phase 1. The smart card operating system and the smart card application software have to use security relevant user data (especially keys and plain text data) in a secure way. It is assumed that the Security Policy as defined for the specific application context of the environment does not contradict the Security Objectives of the TOE. Only appropriate secret keys as input for the cryptographic function of the TOE have to be used to ensure the strength of cryptographic operation.

Protection during Packaging, Finishing and Personalisation (A.Process-Card) is assumed after TOE Delivery up to the end of Phase 6, as well as during the delivery to Phase 7.

Following additional assumptions are assumed in the Security Target:

- Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (A.Key-Function).

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

The Target of Evaluation (TOE) is called:

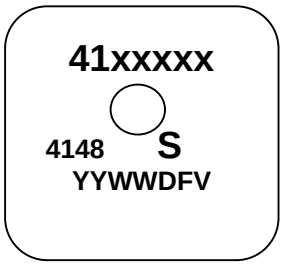
SM4148 LSI module for Smart Card,

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	SM4148 module		packaged module
2	SW	Hermes Bootstrap Program (including DRNG function)	1.2.0	included in BootROM
3	SW	IC dedicated test software	1.0.0	included in TestROM
4	DOC	Programmers Manual of SM4148	1.3.0	paper
5	DOC	Combination Type Smart Card LSI HERMES Bootstrap program Functional Specification	1.0.0	paper
6	DOC	Secure Programming Guidance for SM4148	1.0	paper
7	DOC	Handling Guidance for SM4148	1.0	paper

Table 5: Deliverables of the TOE

The TOE can be identified by examining the module:



4148 identifies the SM4148 while the „F“ identifies the production line (factory) and must be „1“ (identifying the 4th factory at Fukuyama).

3 Security Policy

The security policy of the TOE is to provide basic security functions to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a random number generation 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

The smart card operating system and the application software stored in the FROM are not part of the TOE. The code in the Test ROM of the TOE (IC dedicated software) is used by the TOE manufacturer to check the chip function before TOE delivery. This was considered as part of the evaluation under the CC assurance aspects ALC for relevant procedures and under ATE for testing.

The TOE is delivered as a module at the end of the IC packaging into modules (phase 4 of the life cycle defined). At these specific points in time the operating system software is already stored in the non-volatile memories of the chip and the test mode is completely disabled.

The smart card applications need the security functions of the smart card operating system based on the security features of the TOE. With respect to security the composition of this TOE, the operating system, and the smart card

application is important. Within this composition the security functionality is only partly provided by the TOE and causes dependencies between the TOE security functions and the functions provided by the operating system or the smart card application on top. These dependencies are expressed by environmental and secure usage assumptions as outlined in the user documentation.

Within this evaluation of the TOE several aspects were specifically considered to support a composite evaluation of the TOE together with an embedded smart card application software (i.e. smart card operating system and application). This was necessary as Sharp Corp. is the TOE developer and manufacturer and responsible for specific aspects of handling the embedded smart card application software in its development and production environment.

5 Architectural Information

The top level block diagram and a list of subsystems can be found within the TOE description of the Security Target [7]. The Programmers Manual [10] contains the description of the complete instruction set and the hardware description (but only the part relevant for smartcard application software developers).

For the implementation of the TOE Security Functions basically the components Sharp original 16 bit CPU, DES coprocessor, Deterministic Random Number Generator, Flash Memory, RAM, ROM, Memory Protect Circuit, I/O and filters are used.

Security measures for physical protection are realised within the layout of the whole circuitry.

The TOE IC Dedicated Software, stored on the chip, is used for testing purposes during production only and is completed separated from the use of the embedded software by disabling before TOE delivery.

6 Documentation

The documentation [10] to [13] is provided with the product by the developer to the customer for secure usage of the TOE in accordance with the Security Target [7].

Note that the customer who buys the TOE is normally the developer of the operating system and/or application software which will use the TOE as hardware computing platform to implement the software (operating system / application software) which will use the TOE.

7 IT Product Testing

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

The functional testing of SM4148 can be divided 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 summarised as follows:
  - 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.
  - 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.
  - 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 SM4148 LSI module for Smart Card (a packaged IC) produced in the 4th factory at Fukuyama. 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 test mode is irreversibly disabled before the TOE leaves the factory. Its was tested whether it was possible to re-enable this test mode but that proved to be not possible. 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), [8] 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) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards and

(see [4, AIS 25, AIS 26])

and [4, AIS 20 (Functionality classes and evaluation methodology for deterministic random number generators) 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 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
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS

Assurance classes and components		**Verdict**
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
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
Highly resistant	AVA_VLA.4	PASS

Table 6: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conform to the Smartcard IC Platform Protection Profile, BSI-PP-0002-2001 [9]
- 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 by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function:
  - SF.DES (Coutermeasures of the DES coprocessor against side channel attacks),
  - SF.RNG (Deterministic Random Number Generator)

  The scheme interpretations AIS 26 and AIS 20 (see [4]) were used.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for the TOE Security Function SF.DES (DES coprocessor).

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

The results of the evaluation are only applicable to the TOE SM4148 LSI module for Smart Card (a packaged IC) produced in the 4th factory at Fukuyama as identified in chapter 2. The evaluation results cannot be extended to further versions/derivates of the TOE and/or another production sites without any extra investigations.

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 [10] to [13] 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 [7] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete security target [7] used for the evaluation performed.

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
CPU	Central Processing Unit
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
FROM	Flash ROM
IC	Integrated Circuit
I/O	Input/Output

IT	Information Technology
OS	Operating System
PLL	Phase Locked Loop
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
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 2.3, August 2005

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

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

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

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

[6] Security Target BSI-DSZ-CC-0389, version 1.5, 11 April 2007, SM4148 LSI for IC cards Security Target, Sharp Corporation (confidential document)

[7] Security Target BSI-DSZ-CC-0389, version 1.5, 11 April 2007, SM4148 LSI for IC cards Security Target, Sharp Corporation (sanitized public document)

[8] Evaluation Technical Report, version 2.0, April 20th, 2007, Evaluation Technical Report SHARP SM4148 Module –EAL4+ (confidential document)

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

[10] Programmers Manual of SM4148, Ver. 1.3.0, April 18, 2007

[11] Combination Type Smard Card LSI HERMES Bootstrap program Functional Specification, Ver. 1.0.0, December 20, 2005

[12] Secure Programming Guidance for SM4148, Ver. 1.0, September 15, 2006

[13] Handling Guidance for SM4148, Ver. 1.0, September 15, 2006

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

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

a) **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.

b) **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:

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

CC Part 3:

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0389-2007

Evaluation results regarding development and production environment

The IT product SM4148 LSI module for Smart Card, (Target of Evaluation, TOE) has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, version 2.3 (ISO/IEC 15408:2005), 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 2.3 (ISO/IEC15408: 2005).

As a result of the TOE certification, dated 3. July 2007, 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) 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 (production site)

(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 BSI-DSZ-CC-0389, version 1.5, 11 April 2007, SM4148 LSI for IC cards Security Target, Sharp Corporation.

The evaluators verified, that the threats and the security objectives for the life cycle phases 2, 3 and 4 up to delivery at the end of phase 4 as stated in the Security Target [7] are fulfilled by the procedures of these sites.

This page is intentionally left blank.