CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9216**
Product / system:	smart card integrated circuit MN67S360 Smartcard IC, Version RV3, TV3
Product manufacturer:	Matsushita Electric Industrial Co., Ltd. 1 Kotari-yakemachi, Nagaokakyou Kyoto 617-8520, Japan
Customer:	see above
Evaluation facility:	TÜViT, evaluation body for IT security
Evaluation report:	*Version 1 as of 2004-10-04* Document-number: *20574429_TÜV_150.01* Author: Dr. Patrick Bödeker
Result:	EAL4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4
Evaluation stipulations:	none
Certifier:	Dr. Christoph Sutter
Certification stipulations:	none

Essen, 2004-10-11

Dr. Ernst-Hermann Gruschwitz Dr. Christoph Sutter

Contents

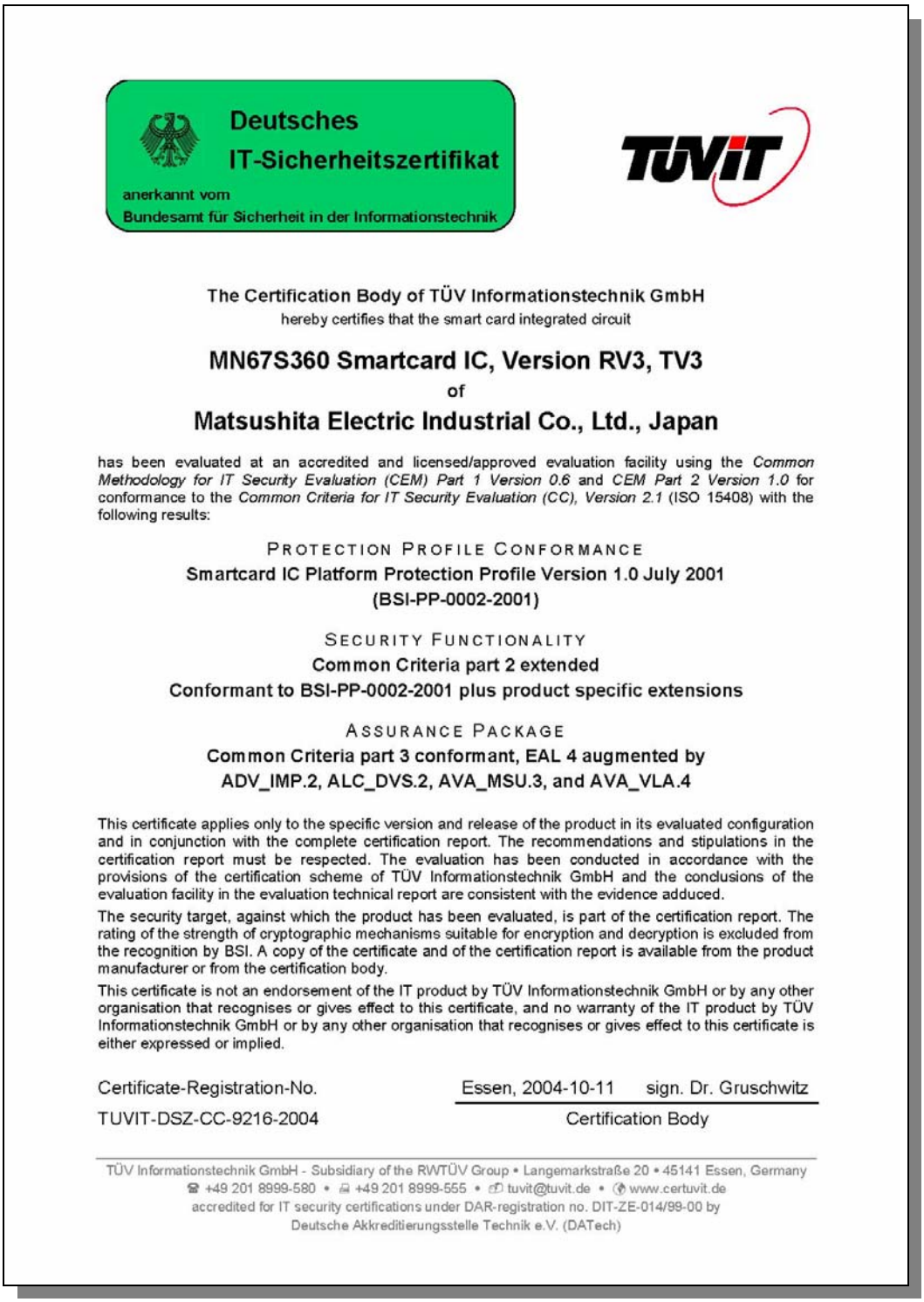
Part A

Certificate and Background of the Certification

Part A presents a copy of the issued certificate and summarizes

- information about the certification body,
- the certification procedure, and
- the performance of evaluation and certification.

1 The Certificate



Deutsches
IT-Sicherheitszertifikat
anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

The Certification Body of TÜV Informationstechnik GmbH
hereby certifies that the smart card integrated circuit

MN67S360 Smartcard IC, Version RV3, TV3
of
Matsushita Electric Industrial Co., Ltd., Japan

has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM) Part 1 Version 0.6* and *CEM Part 2 Version 1.0* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.1* (ISO 15408) with the following results:

PROTECTION PROFILE CONFORMANCE
Smartcard IC Platform Protection Profile Version 1.0 July 2001
(BSI-PP-0002-2001)

SECURITY FUNCTIONALITY
Common Criteria part 2 extended
Conformant to BSI-PP-0002-2001 plus product specific extensions

ASSURANCE PACKAGE
Common Criteria part 3 conformant, EAL 4 augmented by
ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4

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 recommendations and stipulations in the certification report must be respected. The evaluation has been conducted in accordance with the provisions of the certification scheme of TÜV Informationstechnik GmbH and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The security target, against which the product has been evaluated, is part of the certification report. The rating of the strength of cryptographic mechanisms suitable for encryption and decryption is excluded from the recognition by BSI. A copy of the certificate and of the certification report is available from the product manufacturer or from the certification body.

This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

Certificate-Registration-No.
TUVIT-DSZ-CC-9216-2004

Essen, 2004-10-11 sign. Dr. Gruschwitz
Certification Body

TÜV Informationstechnik GmbH - Subsidiary of the RWTÜV Group • Langemarkstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-580 • 🖷 +49 201 8999-555 • 🖂 tuvit@tuvit.de • 🌍 www.certuvit.de
accredited for IT security certifications under DAR-registration no. DIT-ZE-014/99-00 by
Deutsche Akkreditierungsstelle Technik e.V. (DATech)

2 Certification Body – CERTÜViT

CERTÜViT, the Certification Body of *TÜV Informationstechnik GmbH*[1] – a subsidiary of the RWTÜV Group - was established in 1998 and offers a variety of services in the context of security evaluation and validation.

CERTÜViT was accredited in September 1999 for certification of IT security products according to ITSEC and Common Criteria by *Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik (Dekitz)* now *Deutsche Akkreditierungsstelle Technik e.V. (DATech), Frankfurt/Main* under DAR-registration no. DAT-ZE-014/99-01 and performs its projects under a quality management system certified against ISO 9001 by *Germanischer Lloyd, Hamburg*.

CERTÜViT is accredited by *Bundesamt für Sicherheit in der Informationstechnik*[2] to issue the "German IT Security Certificate" which is recognised by BSI as equivalent to the "German IT Security Certificate" of BSI.

3 Specifications of the Certification Procedure

The certification body conducts the certification procedure according to the criteria laid down in the following:

- DIN EN 45011
- TÜViT Certification Scheme
- TÜViT Certification Conditions
- Regulations on the "German IT Security Certificate" issued by the BSI and accepted in the contract of BSI and TÜViT as of November 20, 2002.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 2.1, August 1999.
- Common Methodology for Information Technology Security Evaluation (CEM) part 1, version 0.6, January 1997.
- Common Methodology for Information Technology Security Evaluation (CEM) part 2, version 1.0, August 1999.
- Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[1] in the following termed shortly TÜViT

[2] in the following termed shortly BSI

4 Recognition Agreements

In order to avoid multiple certification of the same product by different certification bodies a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC - under certain conditions was agreed. The CERTÜViT certificates are recognized by BSI – the national German certification body in international agreements – to be equivalent to its own certificates.

4.1 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4 was signed between the national participants of Australia and New Zealand, Austria, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, Israel, Italy, Japan, The Netherlands, Norway, Spain, Sweden, Turkey, United Kingdom and the United States.

4.2 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The arrangement on the mutual recognition of IT security certificates based on the CC was extended by these participants up to and including the evaluation assurance level EAL7.

5 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The smart card integrated circuit MN67S360 Smartcard IC, Version RV3, TV3 has undergone the certification procedure at TÜViT certification body. It was an initial certification.

The evaluation of the smart card integrated circuit MN67S360 Smartcard IC, Version RV3, TV3 was conducted by the evaluation body for IT-security of TÜViT and concluded on October 4, 2004. The TÜViT evaluation facility is recognised by BSI.

The sponsor as well as the developer is Matsushita Electric Industrial Co., Ltd.. Distributor of the product is Matsushita Electric Industrial Co., Ltd..

The certification was concluded with

- the comparability check and
- the preparation of this certification report.

This work was concluded on October 11, 2004. The confirmation of the evaluation

assurance level (EAL) only applies on the condition that

- all stipulations regarding generation, configuration and operation, as given in part B of this report, are observed,
- the product is operated – where indicated – in the environment described.

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

With regard to the meaning of the evaluation assurance levels (EAL) and the strength of function (SoF), please refer to part C of this report.

6 Publication

The following Certification Results consist of pages B-1 to B-8. The product MN67S360 Smartcard IC will be included in the BSI list of certified products which is published at regular intervals (e. g. in the Internet at http://www.bsi.bund.de) and the TÜViT certification lists (http://www.certuvit.de).

Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form at the internet address of CERTÜViT as stated above.

Part B

Certification Result

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 Result

1 Executive Summary

1.1 Target of Evaluation and Evaluation Background

The target of evaluation (TOE) is the smart card integrated circuit MN67S360 Smartcard ICVersion RV3, TV3 which consists of hardware including a processing unit, cryptographic coprocessor, security components, RF interface, and volatile and non-volatile memories. The TOE also includes IC Dedicated Software and documentation. The IC Dedicated Software is used for test purposes during production but also provide additional services to facilitate usage of hardware. All other software is called Smartcard Embedded Software, which is not part of the TOE.

The TOE consists of the following components:

component type	component name, version
hardware	MN67S360 Smartcard IC, Version RV3, TV3
software	Contact Test Software of MN67S360, V1.0 04/03/02
	IC Management Software (Firmware) of MN67S360, V1.0 04/06/09
documentation	see chapter 6

The TOE is intended to be used by multi-application operating systems such as Java Card that supports secure loading and deletion of applications. It fulfils the requirements of applications requiring high security such as banking and financial applications (credit/debit, E-Purse, E-Commerce), cellular telephony applications (SIM cards), and government applications (Basic Resident Register, health cards and driver license). As security features it provides:

- true random number generator;
- security sensors (temperature, frequency, voltage);
- physical countermeasures (such as sensing shield);
- cryptography (DES, RSA, EC, AES); and
- countermeasures for DFA, DPA, and SPA attacks.

DES key-length of 56 bit and RSA key length of 512 and 768 bit are not within the scope of evaluation and certification.

According to the Smartcard IC Platform Protection Profile, Version 1.0, July 2001 (BSI-PP-0002-2001) the TOE life cycle is separated into 7 phases. The IC is delivered in form of wafers after the production test at the end of phase 3.

The sponsor, vendor and distributor is “Matsushita Electric Industrial Co., Ltd., 1 Kotari-yakemachi, Nagaokakyou, Kyoto 617-8520, Japan“.

The TOE was evaluated against the claims of the Security Target[3] [ST] (public version attached in part D) by the "*evaluation body of TÜV Informationstechnik GmbH*" (TÜViT). The evaluation was completed on October 4, 2004. TÜViT's evaluation body is recognised by BSI.

1.2 Assurance Package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 4 (Evaluation Assurance Level 4) augmented by ADV_IMP.2 (Implementation representation – Implementation of the TSF), ALC_DVS.2 (Life cycle support – Sufficiency of security measures) AVA_MSU.3 (Misuse – Analysis and testing for insecure states), and AVA_VLA.4 (Vulnerability analysis - Highly resistant).

1.3 Strength of Functions

The TOE's strength of functions is rated "high" (SOF-high). The strength of functions rating does not include cryptographic algorithms for encryption and decryption. For more details see also chapter 9 of this report.

1.4 Functionality

Except the functional requirements FAU_SAS.1 (Audit storage), FCS_RND.1 (Quality metric for random numbers), FMT_LIM.1 (Limited capabilities), and FMT_LIM.2 (Limited availability) the TOE's security functional requirements were taken from CC part 2 (i. e. the set is CC part 2 extended) [CC]. They can be categorized in the following five categories:

1. Cryptographic support,
2. User data protection,
3. Security management,
4. Protection of the TSF.
5. Resource utilisation

Chapter 9 lists the security functional requirements in more detail. They are met by eleven suitable TOE security functions (TSF):

[3] hereinafter called ST

TSF	name	Description
SF.RNG	Random Number Generator	generates true random numbers that meet the randomness quality criteria for the P2 class SOF-high in [AIS31].
SF.FAS	Filters and Sensors	incorporates effective filters on the essential signal lines so as to eliminate the cause for possible faults. Moreover, the TOE has sensors to detect a variety of operating conditions that could lead to malfunctions, including frequency, voltages and temperatures.
SF.PHY	Tamper Resistance	comprises various physical measures that make tamper attacks more difficult and protects thereby data stored in the EEPROM and RAM from being modified or disclosed using the physical probing, in the course of processing or transferring.
SF.DPR	Data Protection	comprises security measures against unwanted leakage, particularly to protect against SPA, DPA and DFA
SF.MCT	Mode Control	prevents abuse of test functions after TOE delivery. The TOE has two modes, Test Mode and Normal Mode. Factory setting is the Normal Mode.
SF.DES	DES	realises the DES encryption/decryption and MAC generation (112 and 168 bit)
SF.RSA	RSA	realises the RSA encryption/decryption, signature generation, and signature verification (1024 bit)
SF.EC	Elliptic Curve	realises Elliptic Curve ElGamal encryption/decryption, DSA signature generation, and signature verification (160 bit).
SF.AES	Advanced Encryption Standard	realises the Advanced Encryption Standard (AES) encryption/decryption, and MAC generation (128, 192, and 256 bit).
SF.ACU	Access Control Unit	monitors all addresses. With reference to this function, three modes are selectable by the Secure Kernel Software: User Mode, API Mode, and Super Mode. In accordance with a mode selected, access-allowed or -inhibited areas in each corresponding memory are determined.
SF.ID	ID Injection	In the last function testing at phase 3, some data to uniquely identify the IC are injected into EEPROM using tester. This information can not be rewritten after deactivation of test circuits.

A more detailed description of the TOE security functions can be found in section 6.1 of the ST, which is attached as part D of this certification report.

1.5 Summary of Threats and Organisational Security Policies (OSPs)

Assets for the TOE comprise the integrity and/or confidentiality of user data and smart card embedded software as well as the correct operation of the TOE including its random number generator. Additional assets are critical information about the TOE which includes logical and physical design data, IC dedicated software and TSF data but also initialisation and pre-personalisation data, specific development aids, test and characterisation related data, material for software development support, and photo masks. Further assets are the random numbers generated by the TOE.

Any human user or a TOE external process acting on his behalf is regarded as an attacker.

The seven threats deal with loss of confidentiality and integrity of assets as well as correct operation of the TOE and deficiency of random numbers.

The two organisational security policies deal with a secure TOE development and production environment and additional cryptographic functionality the TOE has to provide.

A more detailed description of the threats and organisational security policies can be found in sections 3.3 and 3.4 of the ST, which is attached as part D of this certification report.

1.6 Special Configuration Requirements

The TOE is delivered in one fixed configuration and no further generation takes place after delivery to the customer.

1.7 Assumptions about the Operating Environment

Depending on the life-cycle phase of the TOE (see section 2.2 of the ST) the following assumptions are applicable:

- Appropriate “Protection during Packaging, Finishing and Personalisation (A.Process-Card)” must be ensured after TOE Delivery up to the end of Phase 6, as well as during the delivery to Phase 7 as specified below.

  A.Process-Card Protection during Packaging, Finishing and Personalisation

  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).

- The developer of the Smartcard Embedded Software must ensure the appropriate "Usage of Hardware Platform (A.Plat-Appl)" while developing this software in Phase 1 as specified below.

  A.Plat-Appl Usage of Hardware Platform

  The Smartcard Embedded Software is designed so that the requirements from the following documents are met:

  (i) "MN67S360 Smartcard IC Administrator Guidance for Smartcard Embedded Software Developer Version 1.3, 17.07.2003", and

  (ii) Findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

- The developer of the Smartcard Embedded Software must ensure the appropriate "Treatment of User Data (A.Resp-Appl)" while developing this software in Phase 1 as specified below.

  A.Resp-Appl Treatment of User Data

  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.

A more detailed description of the assumptions can be found in section 3.2 of the ST, which is attached as part D of this certification report.

1.8 Independence of the Certifier

Within the last two years, the certifier did not render any consulting- or other services for the company ordering the certification and there was no relationship between them that might have an influence on his assessment.

The certifier did not participate at any time in test procedures for the product, which forms the basis of the certification.

1.9 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 with regard to generation, configuration and operation as detailed in this certification report. This certificate is not an endorsement of the IT product by the TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH 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 the smart card integrated circuit MN67S360 Smartcard IC, Version RV3, TV3 and consists of the components listed in section 1.1 of this certification report. The software and documentation is sent signed and encrypted to the SW developer and/or card manufacturer. The hardware is delivered trustworthy in form of wafers to the card manufacturer together with a checking key. TOE name and version number can be read out of the IC via the verify command. The answer to the command contains 11 bytes where the relevant information can be found in:

- Byte 1: 0x01 (for MN67S360)
- Byte 10: 0x03 (for RV3)
- Byte 11: 0x03 (for TV3)

3 Security Policy

The overall security policy of the TOE is to provide a secure platform for smartcard embedded software and to protect against tampering and abuse of functionality. The TOE ensures, that especially critical user data is stored and processed in a secure way and is protected against attacks like physical probing and manipulation. The TOE provides the cryptographic algorithms triple-DES, RSA, EC, and AES for encryption, decryption, MAC generation, and signature generation and verification and protects the operation against leakage of information to ensure the confidentiality of e. g. cryptographic keys.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The following usage assumptions are defined in the ST and must be regarded when using the TOE. The TOE-specific assumptions are as follows:

- The developer of Smartcard Embedded Software must ensure the appropriate “Usage of triple-DES (A.DES)” while developing this software in Phase 1 as specified below.

  A.DES Usage of triple-DES

  It is assumed that the triple-DES algorithm shall be used as encryption algorithm though product also supports single-DES algorithm if it is necessary to keep high-level security, because the algorithm is to be attackable by high-level attacker.

- The developer of Smartcard Embedded Software must ensure the appropriate “Usage of Cryptographic key with sufficient strength (A.Key-Length)” while developing this software in Phase 1 as specified below.

  A.Key-Length Usage of Cryptographic key with sufficient strength

  It is assumed that the key length of 1024 bits shall be used for RSA though product also supports the key length of 512, 768, and 1024 bits if it is necessary to keep high-level security, because the algorithm is to be attackable by high-level attacker.

4.2 Environmental Assumptions

It is assumed that the TOE is used in the environment described in section 1.7 of this certification report.

4.3 Clarification of Scope

The following sites for the development and production of the TOE were considered in this certification under assurance classes **ACM** (ACM_AUT.1, ACM_CAP.4, ACM_SCP.2), **ADO** (ADO_DEL.2, ADO_IGS.1), and **ALC** (ALC_DVS.2, ALC_LCD.1, ATE_TAT.1):

Moriguchi: Corporate System LSI Development Division, Semiconductor Company, Matsushita Electric Industrial Co., Ltd., 3-1-1 Yagumo-naka-machi, Moriguchi City, Osaka, 570-8501, Japan

Nagaokakyo: Corporate System LSI Development Division, Semiconductor Company, Matsushita Electric Industrial Co., Ltd., 1 Kotari-Yakemachi, Nagaokakyo, Kyoto, 617-8520, Japan

Nishikadoma: AV-Core Technology Development Center, Matsushita Electric Industrial Co., Ltd., 1006 Ojikadoma, Kadoma City, Osaka 571-8501, Japan

Tonami: Tonami Factory, Corporate Manufacturing & Development Division, Semiconductor Company, Matsushita Electric Industrial Co., Ltd., 271 higashi-kaihatsu, Tonami-city, Toyama 939-1312, Japan

Topan Printing: Toppan Printing Co., Ltd., 1101-20, Myohoji-cho, Yokaichi-city, Shiga 527-8566, Japan

The hardware part of the TOE is produced exclusively at the Tonami site.

Smartcard Embedded Software, i.e. the smart card operating software and the application software, stored in ROM and EEPROM are not part of the TOE

DES operation with 56 Bit keys and RSA operation with 512 or 768 bit keys are not within the scope of this certification (see assumptions A.DES and A.Key-Length).

5 Architectural Information

The TOE consists of the following 8 hardware (HW) and 8 firmware (FW) subsystems which can be summarised as follows:

Name of Subsystem	Description
Analog – HW	This subsystem provides functions for contact less communication, various filters and sensors, a sensing shield, true random number generator, functions for random current, I/O pre-processor, generation of clock signal and reset signal, selection of transmit/receive data, and bus encryption
ROM – HW	This subsystem stores critical software such as IC Dedicated Software and Smartcard Embedded Software and ensures the integrity of them. It also contains a circuit for ROM self tests.
RAM – HW	This subsystem is intended for use in retaining data to be temporarily stored in RAM without compromising its integrity and privacy when IC Dedicated Software or Smartcard Embedded Software is running. For this purpose address and data scrambling is equipped in the subsystem.
EEPROM – HW	This subsystem contains critical software such as IC Dedicated Software and Smartcard Embedded Software (program code) and ensures the integrity and confidentially of them (scrambling and bus cryptography functions). EEPROM is partitioned into two parts: 32-Kbyte normal area and 256-Byte PROM area.
Cryptographic Hardware – HW	This subsystem performs multiple precision calculations for RSA and Elliptic Curve Cryptography and also calculations for triple-DES encryption/decryption.
Security Circuit – HW	This subsystem performs access control to RAM, ROM, controls bus scrambling and bus cryptography, random current, true random number generator, sensors and sensing shield.
CPU – HW	This subsystem contains CPU Core functions and functions such as DMA controller, memory controller, interrupt controller, watchdog timer. Additionally it realises bus encryption/decryption for a secure data transfer to each subsystem.
Test Circuit – HW	This subsystem executes defective product tests by using test pads. Test pads are disconnected by dicing. Writing of pad deactivating code disarms the test functions.
I/O Preprocessor API – FW	This subsystem controls non-contact communication on the basis of ISO14443 Type B for the Analog Subsystem (Initialization of I/O Preprocessor API, request for transmitting data to / receiving data from Analog Subsystem, getting receiving information on the data from Analog Subsystem, getting Analog Subsystem Tx/Rx mode, request for setting up bit rate to Analog Subsystem).

Name of Subsystem	Description
EEPROM API – FW	This subsystem controls certain operations such as programming, reading and erasing data to/from EEPROM, by using the hardware in EEPROM Subsystem.
Cryptographic API – FW	This subsystem calls cryptographic HW to realize RSA en-/decryption, RSA signature generation/signature verification, elliptic curve ElGamal en-/decryption, Elliptic Curve DSA signature generation/verification, Elliptic Curve MR signature generation/verification, DES en-/decryption, MAC generation by DES, AES en-/decryption, MAC generation by AES, SHA-1 Hash. Furthermore, true random numbers are acquired from Analog Subsystem.
Timer API – FW	This subsystem implements on/off control of the timer functions provided for internal use in the smart card.
Utility – FW	This subsystem provides the Smartcard Embedded Software developers with the functionality to directly acquire system information, execute CRC calculation, and acquire a firmware version without accesses to Hardware.
Issuance API – FW	This subsystem has the functions: transport key verification, internal authentication, card-manufactured information acquisition and smart card ES issuance (all used after phase 4).
Secure Kernel – FW	This subsystem is IC Dedicated Software that is activated in the first place when the CPU reset is released. It initial sets up hardware units. Besides, this it executes the security functions such as accessible areas setup, shield line delay time comparison, random current control, and software reset at dispatch occurrence.
Contact Test Software – FW	This subsystem tests the IC functionality of the EEPROM, sensing shield function, and sensors function incorporated in the IC.

6 Documentation

The following documentation is provided with the product by the developer to the SW developer and/or card manufacturer:

- MN67S360 Smartcard IC Administrator Guidance for Smartcard Embedded Software Developer, Version 1.3, 17.07.2003
- MN67S360 Smartcard IC Administrator Guidance for Card Manufacturer, Version 1.2, 16.07.2004
- further specifications and manuals [SPEC_MAN]

7 IT Product Testing

The developer tested the TOE with the overall objectives to verify that the TOE satisfies all requirements specified in Functional Specifications (FSP) and that it is a correct and complete implementation of the High Level Design (HLD) description.

The developers tests can be divided in four categories:

(i) Simulation tests:
Objective of the testing is the proof of the correctness of the logic with the help of simulation before starting the production.

(ii) Production Tests:
Objective of this testing with the TOE is to check whether each TOE is functioning correctly and to guarantees that no defect chips are delivered.

(iii) Hardware Tests:
With these tests the security mechanisms of the security function are tested in detail at the produced TOE. To be able to tests all mechanisms special prepared chips are used for some tests.

(iv) Qualification tests:
With these tests the product reliability is assured.

The evaluation body repeated the tests of the developer and performed independent penetration testing. The testing confirmed that the TOE is resistant against attacks based on the level of high attack potential, that all the obvious vulnerabilities were considered and that the vulnerabilities identified are non-exploitable in the intended operational environment of the TOE.

8 Evaluated Configuration

The TOE is delivered in one fixed configuration and no further generation takes place. Therefore the evaluated configuration is identical to the TOE, which can be identified as described in chapter 2 of this certification report.

9 Results of the Evaluation

The Evaluation Technical Report [ETR] was provided by TÜViT's evaluation body according to the requirements of the Scheme, the Common Criteria [CC], the Methodology [CEM] and the Application Notes and Interpretations of the Scheme [AIS].

The verdicts for the CC, part 3 assurance classes and components (according to EAL4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4 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
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	ATE_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 of insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

All assurance components were assessed with the verdict PASS. This includes that all evaluator action elements being part of the assurance components are also assessed with PASS. Therefore, the TOE as defined in the security target is considered to be Part 3 conformant.

Section 5.3.1 of the ST, which is attached as part D of this certification report, lists the following TOE security functional requirements.

ID	**Class**/Component
FAU	**Security Audit**
FAU_SAS.1	Audit storage
FCS	**Cryptographic support**
FCS_COP.1	Cryptographic operation
FCS_RND.1	Quality metric for random numbers
FDP	**User data protection**
FDP_IFC.1	Subset information flow control
FDP_ITT.1	Basic internal transfer protection
FMT	**Security management**
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
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	Domain separation
FRU	**Resource utilisation**
FRU_FLT.2	Limited fault tolerance

Apart from FAU_SAS.1, FCS_RND.1, FMT_LIM.1, and FMT_LIM.2 the security functional requirements were taken from [CC] part 2, i. e. they are [CC] part 2 extended.

The evaluation performed in accordance to EAL4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4 has shown that the TOE security functional requirements are correctly realised by the TOE security functions. Thus, in realising these functional requirements, it is assured that the TOE will meet the security objectives claimed in the ST.

The TOE is conformant to the Smartcard IC Platform Protection Profile, Version 1.0, July 2001 (BSI-PP-0002-2001).

TSF *SF.RNG* and *SF.DPR* fulfil the SOF-rating high (SOF-high). The strength of functions rating does not include cryptographic algorithms for encryption and decryption, like triple-DES in TSF *SF.DES*. The cryptographic algorithm RSA with key length of 1024 Bit are published in the Bundesanzeiger No. 30 – p. 2537-2538, 2004-02-13 as suitable for the qualified electronic signature and therefore fulfil the requirements for SOF-high.

The sponsor must advise the certification authority about any modification of the TOE or its guidance documentation. The certification authority will then check whether the certification results are still valid and, if necessary, initiate all further steps concerning a re-evaluation. The results of the evaluation are only applicable to the product "*MN67S360 Smartcard IC, Version RV3, TV3*". 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.

10 Evaluation Stipulations, Comments, and Recommendations

There are no evaluation stipulations.

The following comments and recommendations for the user are contained in the evaluation report [ETR]:

The TOE is delivered to Card Manufacturer and the Smartcard Embedded Software Developer. The actual end user obtains the TOE from the operating system producer together with the application which runs on the TOE.

The Smartcard Embedded Software Developer receives all necessary recommendations and hints in form of the delivered guidance documentation.

The following assumptions and requirements concerning external security measures, documented have to be considered:

- The development environment of the Smartcard Embedded Software Developer has to be secure, in order to be able to guarantee the security of the TOE on the whole.
- The Smartcard Embedded Software Developer has to follow the usage hints given in [ADM_SW] for each security function in the related sub-chapter (e.g. not to set up registers directly).
- The Smartcard Embedded Software Developer has to follow the assumptions given in chapter 6 of [ADM_SW].

The Card Manufacturer receives all necessary recommendations and hints in form of the delivered guidance documentation.

The following assumptions and requirements concerning external security measures have to be considered:

- The production environment of the Card Manufacturer has to be secure, in order to be able to guarantee the security of the TOE on the whole.

- The Card Manufacturer has to follow the initialisation procedure described in chapter 4 of [ADM_CM] (e. g. dicing procedure, verification of transport key).
- The Card Manufacturer has to follow the assumptions given in chapter 6 of [ADM_CM].

11 Certification Stipulations and Notes

There are no stipulations.

12 Security Target

The public version [ST-lite] of the security target [ST] for *MN67S360 Smartcard IC* is included in part D of this certification report.

13 Definitions

13.1 Acronyms

ADM	Administrator Guidance
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation (referenced to as [CC])
CEM	Common Methodology for Information Technology Security Evaluation (referenced to as [CEM])
CM	Configuration Management
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EC	Elliptical Curve
EEPROM	Electrical Erasable and Programmable Read Only Memory
ES	Embedded Software
FSP	Functional Specification
HLD	High-level Design
IC	Integrated Circuit
IF	Interface
IGS	Installation, Generation and Start-up
MAC	Message Authentication Code

OS	Operating System
OSP	Organisational Security Policy
PP	Protection Profile
RSA	Signature Algorithm of Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIF	Sub-interface
SOF	Strength of Function
SPA	Simple Power Analyis
SS	Sub-system
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Function Interfaces
TSP	TOE Security Policy
USR	User Guidance
VLA	Vulnerability Analysis

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from Part3 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

[ADM_CM] MN67S360 Smartcard IC Administrator Guidance for Card Manufacturer, Version 1.2, 16.07.2004

[ADM_SW] MN67S360 Smartcard IC Administrator Guidance for Smartcard Embedded Software Developer, Version 1.3, 17.07.2003

[AIS] Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[CEM] Common Methodology for Information Technology Security Evaluation, Part 1: Introduction and general model, version 0.6, revision 11.01.1997, Part 2: Evaluation Methodology, version 1.0, revision August 1999

[ETR] Evaluation Technical Report, version 1, 2004-10-04, TÜV Informationstechnik GmbH, document-number: 20574429_TÜV_150.01

[SPEC_MAN]
- MN103S Series Assemblers User's Manual, version 5, 2002-11-01
- MN103S Series C Compiler User's Manual Usage Guide, version 5, 2003-06-01
- MN1030/MN103S/MN103E Series C Compiler User's Manual Language description, version 5.1, 2001-04-01
- MN1030/MN103S/MN103E Series C Compiler User's Manual Library Reference, version 3, 2001-04-01
- MN10300 Series C Source Code Debugger User's Manual, version 5, 2003-06-01
- MN1030/MN103S Series C Source Code Debugger for Windows® User's Manual, version 6, 2003-06-01
- MN1030/MN103S Series Installation Manual, version 4, 2002-06-01
- MN1030/MN103S Series Instruction Manual, version 4, 2003-01-01
- MN10300 Series Easy implementation Real Time OS (PR103-4C) - User’s Manual, version 0.6, 2001-04-01
- PCI/PC Card Installation Manual, version 6, 2003-04-01
- Specification Cryptographic Processing Engine API, version 1.1, 2001-12-26
- Specification Device Driver Basic Design, version 1.3, 2003-01-10
- Specification Dicing, version 0.5, 2004-01-13

[ST] MN67S360 Smartcard IC Security Target, Version 2.1, 2004-08-31 confidential document

[ST-lite] MN67S360 Smartcard IC Security Target (ST-Lite), Version 1.1, 2004-09-01
public version of the Security Target [ST]

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

- conformance results
- assurance categorization
- evaluation assurance levels
- strength of security function
- vulnerability analysis

CC Part 1:

Conformance results (section 5.4 of CC part 1 with 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 predefined 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.“

CC Part 3:

Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in *Table 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 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

„Table 2 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 CC 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_IMT					**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 2: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested

“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

“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

“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

“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

“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

“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

“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)

AVA_SOF Strength of TOE security functions

“Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function). Even if such functions cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat them by direct attack. A level or a specific metric may be claimed for the strength of each of these functions. Strength of function analysis is performed to determine whether such functions meet or exceed the claim. For example, strength of function analysis of a password mechanism can demonstrate that the password function meets the strength claim by showing that the password space is sufficiently large.”

Three levels exist: SOF-basic, SOF-medium, and SOF-high.

Vulnerability analysis (AVA_VLA)

AVA_VLA Vulnerability analysis

“Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: (1) the completeness of the TSF (does the TSF counter all the postulated threats?) and (2) the dependencies between all security functions. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the TOE.”

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.

The intent of the developer analysis is to confirm that no identified security vulnerabilities can be exploited in the intended environment for the TOE and that the TOE is resistant to obvious penetration attacks.

Obvious vulnerabilities are considered to be those that are open to exploitation that requires a minimum of understanding of the TOE, skill, technical sophistication, and resources. These might be suggested by the TSF interface description. Obvious vulnerabilities include those in the public domain, details of which should be known to a developer or available from an evaluation authority.

Performing a search for vulnerabilities in a systematic way requires that the developer identify those vulnerabilities in a structured and repeatable way, as opposed to identifying them in an ad-hoc fashion. The associated evidence that the search for vulnerabilities was systematic should include identification of all TOE documentation upon which the search for flaws was based.

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. To accomplish this intent, the evaluator first assesses the exploitability of all identified vulnerabilities. This is accomplished by conducting penetration testing. The evaluator

should assume the role of an attacker with a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential when attempting to penetrate the TOE. Any exploitation of vulnerabilities by such an attacker should be considered by the evaluator to be “obvious penetration attacks” (with respect to the AVA_VLA.*.2C elements) in the context of the components AVA_VLA.2 through AVA_VLA.4.”

Part D

Security Target

Attached is the public version of the Security Target for MN67S360 Smartcard IC

Author: Matsushita Electric Industrial Co., Ltd.

Date: 2004-09-01

Version: 1.1