Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0334-2006

for

MN67S140, RV3, FV12 – EAST JAPAN RAILWAY COMPANY SuicaII Contactless Smart Card IC Chip

from

Matsushita Electric Industrial Co., Ltd.

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0334-2006

MN67S140, RV3, FV12 – EAST JAPAN RAILWAY COMPANY SuicaII Contactless Smart Card IC Chip

from

Matsushita Electric Industrial Co., Ltd.

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

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0002-2001**
Functionality:	**PP 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 (Development - Implementation of security functions) 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)

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, 16. March 2006

The President of the Federal Office
for Information Security

IT Security Certified

Dr. Helmbrecht L.S. SOGIS - MRA

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

Part A: Certification

Part B: Certification Results

Part C: Excerpts from the Criteria

Part D: Annexes

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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

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

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

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

[5] Proclamation of the Bundesministerium des Innern of 22 September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

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

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 MN67S140 Smartcard IC, RV3, FV12 has undergone the certification procedure at BSI.

The evaluation of the product MN67S140 Smartcard IC, RV3, FV12 was conducted by TÜV Informationstechnik GmbH. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

[6] Information Technology Security Evaluation Facility

The sponsor is:

Matsushita Electric Industrial Co., Ltd.
1 Kotari-yakemachi Nagaokakyo City
Kyoto 617-8520, Japan

The certification is concluded with

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

This work was completed by the BSI on 16. March 2006.

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.

4 Publication

The following Certification Results contain pages B-1 to B-23 and D1 to D-4.

The product MN67S140 Smartcard IC, RV3, FV12 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] Matsushita Electric Industrial Co., Ltd.
1 Kotari-yakemachi Nagaokakyo City
Kyoto 617-8520, 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 3

2 Identification of the TOE 9

3 Security Policy 10

4 Assumptions and Clarification of Scope 11

5 Architectural Information 11

6 Documentation 12

7 IT Product Testing 13

8 Evaluated Configuration 13

9 Results of the Evaluation 14

10 Comments/Recommendations 17

11 Annexes 18

12 Security Target 18

13 Definitions 19

14 Bibliography 21

1 Executive Summary

The Target of Evaluation (TOE) is MN67S140, RV3, FV12 - EAST JAPAN RAILWAY COMPANY SuicaII contactless Smart Card IC chip (further will be called as MN67S140, RV3, FV12). The Hardware is the complete chip composed of processing unit, Cryptographic Hardware, security components, RF interface, and volatile and non-volatile memories. The TOE also includes IC Dedicated Software with Version FV12.

This TOE is manufactured by Matsushita Electric Industrial Co., Ltd. in Kyoto indicated by the production line indicator '001' for Tonami and '010' for Kyoto (see part D. Annex A of this Report).

The MN67S140, RV3, FV12 is intended to be used for the applications requiring high security such as transportation and fare collection applications (the Commuter ticket), access control applications (ID cards), and government applications (the Basic Resident Register, health cards and driver license). These are only a few examples and its potentiality can be considered finite.

The whole TOE consists of

- Prossesing unit (CPU) contains the Core AM13C, Interrupt function that processes interrupt. The interrupt function speeds up interrupt response with circuitry that automatically loads the branch address to the corresponding interrupt processing program from an interrupt vector table, and processes non-maskable interrupts (NMI) and level interrupts.
- Cryptographic Hardware, the Cryptographic Hardware is capable of realizing the DES functionality in accordance with the Single-DES and Triple-DES; however, the Single-DES is outside the scope of evaluation.
- Security components, Security Circuit contains access control circuit and various security logics such as RNG (True Random Number), random current generator, sensors and filters (see [7]).
- RF Interface (radio frequency power and signal interface) in conformity to ISO/IEC 14443-2 and JICSAP (Japan IC Card System Application council) enables contactless communication between the chip and a reader/writer. The power supply and data are received by an antenna which consists of a coil with a few turns directly connected to the pads of the TOE.
- Memories consisting of ROM 42Kbytes, SRAM 2Kbytes, XRAM 0.5Kbytes, FeRAM 8Kbytes, PROM 96Bytes. The IC Dedicated Software is part of TOE and stored in ROM. The Smartcard Embedded Software is also stored in the ROM but not part of TOE. FeRAM can be accessed as both data memory and program memory. In PROM, data not allowed to be overwritten is stored.

Several security features independently implemented in hardware or controlled by software will be provided to ensure proper operations and integrity and confidentiality of stored data. This includes for example measures for memory protection, leakage protection and sensors to allow operations only under specified conditions.

The Security Target [6] is written using the Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001 [8]. With reference to this Protection Profile, the smart card product life cycle is described in 7 phases. The development, production and operational user environment are described and referenced to these phases. TOE delivery is defined at the end of phase 3 in form of sawn wafers (dice).

The assumptions, threats and objectives defined in this Protection Profile [8] are used. To address additional security features of the TOE (e.g cryptographic services), the security environment as outlined in the PP [8] is augmented by an additional policy, an assumption and security objectives accordingly.

The IT product MN67S140 Smartcard IC, RV3, FV12 was evaluated by TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit. The evaluation was completed on 03. March 2006. The TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor is

Matsushita Electric Industrial Co., Ltd.
1 Kotari-yakemachi Nagaokakyo City
Kyoto 617-8520, 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. The following table shows the augmented assurance components.

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 resistent

Table 1: Assurance components and EAL-augmentation

[8] Information Technology Security Evaluation Facility

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.1A	Cryptographic operation
FCS_COP.1B	Cryptographic operation
FDP	**User data protection**
FDP_ITT.1	Basic internal transfer protection
FDP_IFC.1	Subset information flow control
FPT	**Protection of the TOE Security Functions**
FPT_FLS.1	Failure with preservation of secure state
FPT_SEP.1	Domain separation
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_PHP.3	Resistance to physical attack
FRU	**Resource utilisation**
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 storage
FCS	**Cryptographic support**
FCS_RND.1	Quality metric for random numbers
FMT	**Security Management**
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability

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 [7] chapter 5.1.1 ff

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Import of user data without security attributes or Import of user data with security attributes or Cryptographic key generation,
FCS_CKM.4	Cryptographic key destruction,
FMT_MSA.2	Secure security attributes.

Table 4: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [7] chapter 5.2 ff.

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

TOE Security Function	Addressed issue
SF.RNG	Random Number Generator
SF.FAS	Filters and Sensors
SF.PHY	Tamper Resistance
SF.DPR	Data Protection
SF.MCT	Mode Control
SF.DES	DES
SF.AUTH	Mutual Authentication Function
SF.ACU	Access Control Unit
SF.ID	ID Injection

For more details please refer to the Security Target [7], chapter 6.

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]. 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 [9] 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 [9] 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.

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 Triple-DES and Mutual Authentication Function must be provided by the TOE according to an additional security policy defined in the Security Target.

Objectives are taken from the Protection Profile plus additional ones related to the additional policy.

1.5 Special configuration requirements

The TOE has two different operating modes, *user mode* and *API mode*. The test mode is deactivated before TOE is delivered. The application software being executed on the TOE can not use the *test mode*. The TOE is delivered as a hardware unit at the end of the IC manufacturing process (Phase 3). At this time the embedded software including operating system and the IC dedicated software are already stored in the non-volatile memories of the chip. The two operating modes mentioned above are determined depending on the program counter place. When the user program is executed, TOE transits to User mode. On the other hand, when the program of IC Dedicated Software is executed, a reset is issued, or power turns on, TOE transits to API mode.

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 have to be organised in a way that excludes all possibilities of physical manipulation of the TOE.

There are no special security measures for the start-up 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 and chapter 10 of this Report.

1.6 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile [9], the assumptions defined in section 3.2 of the Protection Profile are valid for the Security Target of this TOE. 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 from the PP:

The developer of the smart card 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 Smartcard embedded software including operating system have to use security relevant user data of the TOE (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

The following additional assumption is assumed in the Security Target:

- Key-dependent functions (if any) shall be implemented in the smart card Embedded Software in a way that they are not susceptible to leakage attacks (A.Key-Function).
- The developer of Smartcard Embedded Software must ensure the appropriate "Usage of triple-DES (A.DES)" while developing this software in Phase 1. It is assumed that the triple-DES algorithm shall be used as encryption algorithm.
- The developer of Smartcard Embedded Software must ensure the appropriate "Implementation of command interpreter (A.Interpreter)" while developing this software in Phase 1. It is assumed that the command interpreter used for the tests in Phase 4 and 5 shall be implemented. For further details see in [7].

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:

MN67S140, RV3, FV12 – EAST JAPAN RAILWAY COMPANY SuicaII Contactless Smart Card IC Chip

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	MN67S140	RV3, with production line indicator ‘001’ for Tonami and ‘010’ for Kyoto	Wafer (dice)
2	SW	IC dedicated software	FV12	Stored in ROM on IC
3	DOC	MN67S140 Smartcard IC Administrator Guidance for Card Manufacturer [10]	1.0	Pdf-file
4	DOC	MN67S140 Smartcard IC Administrator Guidance for Smartcard Embedded Software Developer [11]	1.0	Pdf-file

Table 5: Deliverables of the TOE

The TOE is identified by MN67S140 RV3 FV12. Another characteristic of the TOE is the chip version information. This information is stored in the ROM and can be read out by the user of the card via relevant command. For the format of the chip version information see [11] and Chapter 3.9.2.2. The answer to the relevant command contains 16 bytes where the relevant information can be found in:
Byte 1 - 2: 0x00, 0x02: MN67S140
Byte 3 - 4: 0x00, 0x03: RV3
Byte 5 – 6: 0x01 0x02: FV12.

During the production tests a unique production line indicator is written into each TOE. This information can be read out by the user of the card via the relevant command. For the format of the production line indicator see [11] and chapter 3.9.2.1. The answer to the command contains 16 bytes where the relevant information concerning the production site can be found in: Lower three bits of Byte 3: 001 for Tonami and 010 for Kyoto.

3 Security Policy

The security policy of the TOE is to provide basic Security Functions to be used by the smartcard operating system and the smartcard application thus providing an overall 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 generator. 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 Triple-DES), 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 smartcard embedded software including operating stored in the User ROM and 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 sawn wafers (dice) at the end of the chip manufacturing process (phase 3 of the life cycle defined). At this specific point in time the embedded software including operating system 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 Matsushita Electric Industrial Co., Ltd. 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. For those aspects refer to part B, chapter 9.2 of this report.

The full evaluation results are applicable only for TOE chips from the semiconductor factory in Tonami and Kyoto (labelled by the production line indicator „001“ for Tonami and ‘010’ for Kyoto).

5 Architectural Information

The MN67S140 Smartcard IC, RV3, FV12 with IC dedicated software are integrated circuits (IC) providing a platform to a smart card operating system and smart card application software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target [7]. The complete description of the TOE for card manufacturer and embedded software developer is to be found in guidance documents delivered to the customer, see table 5.

For the implementation of the TOE Security Functions basically the components processing unit (CPU), XRAM,SRAM, ROM, FeRAM, PROM, security logic, interrupt module, bus system, Random Number Generator (RNG), RF-Interface and the DES module for cryptographic operations of the chip are used. Security measures for physical protection are realised within the layout of the whole circuitry.

The electrical interface of the TOE to the external environment is the coil pads to which the RF antenna is connected.The CPU instructions and the various on-chip memories provide the interface to the software using the Security Functions of the TOE. The IC dedicated software has two parts, IC dedicated support software and IC dedicated test software. The TOE IC dedicated test software, stored on the chip is used for testing purposes during production only and is completely separated from the use of the embedded software by disabling before TOE delivery. The TOE IC Dedicated Support Software stored in ROM can be used by the users embedded software. The following table 6 summarizes the functions of whole IC dedicated software:

Sorting of IC Dedicated Software	Name	Purpose
IC Dedicated Support Software	I/O Preprocessor API	To operate the contactless communications
	Memory API	To operate the accesses to SRAM, FeRAM, and XRAM
	Cryptographic API	To operate the Cryptographic processing and mutual authentication processing
	Timer API	To operate Timers
	Utility API	To acquire the system information and execute such as CRC calculation
	Issuance API	To execute functionality tests by card manufacture after the TOE delivery
	Secure Startup	To execute the hardware initial setup and the interrupt handling
IC Dedicated Test Software	Contact Test Software	To test FeRAM and security functions

Table 6

6 Documentation

The documentation [10] – [23] is provided with the products by the developer to the customer for secure usage of the TOE in accordance with the Security Target.

Note that the customer who buys the TOE is normally the developer of the embedded software including 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.

To support a composite evaluation as defined in AIS 36 [4], the document ETR-lite [24] is provided for the composite evaluator.

7 IT Product Testing

The tests performed by the developer were divided into six categories:

(i) tests which are performed in a simulation environment for analogue and for digital simulations;

(ii) functional production tests, which are done as a last step of the production process (phase 3. These tests are done for every chip to check its correct functionality;

(iii) qualification tests to release the TOE to production to determine the behaviour of the chip with respect to different operating conditions (often also referred to as characterisation tests);

(iv) special verification tests on functionality of the chip which were done with samples of the TOE in user mode and API mode;

(v) special verification tests on Security Functions which were done with samples of the TOE in user mode and API mode;

(vi) layout tests as part of the design and release process by testing the implementation by optical control, in order to verify statements concerning the layout design.

The developer tests cover all Security Functions and all security mechanisms as identified in the functional specification, the high level design and the low level design. Chips from the production site in Kyoto (see part D, annex A of this report) were used for tests.

For this evaluation, the developer provided test evidence for chips from the production site Kyoto. The test results confirm the correct implementation of the TOE Security Functions.

The evaluators supplied evidence that the actual version of the TOE with production line indicator “001” for Tonami and “010” for Kyoto (Japan) provides the Security Functions as specified.

For this evaluation the evaluators assessed the penetration testing and confirmed the results. Intensive penetration testing was performed at that time to consider the physical tampering of the TOE using highly sophisticated equipment and expertised know-how. Specific additional penetration attacks were performed in the course of this evaluation.

8 Evaluated Configuration

The TOE is identified by the version MN67S140 Smartcard IC, RV3, FV12,- EAST JAPAN RAILWAY COMPANY SuicaII contactless Smart Card IC chip and IC dedicated Software with production line indicator ‘001’ (Tonami) and “010” (Kyoto). The TOE has only one fixed evaluated configuration at the time of delivery.

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 *API mode*. The test mode is disabled. The application software being executed on the TOE can not use the *test mode*. Thus, the evaluation was mainly performed in the *user mode* and *API mode*. For all evaluation activities performed in *test mode,* there was a rationale why the results are valid for the *user mode* and *API mode*, too.

9 Results of the Evaluation

9.1 Evaluation of the TOE

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 and AIS 26]) and [4, AIS 31] (*Functionality classes and evaluation methodology for physical 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

Assurance classes and components		Verdict
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
Development tools 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
Semiformal functional specification	ADV_FSP.2	PASS
Semiformal high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Semiformal correspondence demonstration	ADV_RCR.1	PASS
Formal 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
Standardised life-cycle model	ALC_LCD.1	PASS
Compliance with implementation standards	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: low-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 7: 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.DPR (Data encryption) and
  SF.RNG (Random number generation)
  The scheme interpretations AIS 26 and AIS 31 (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

(i) the TOE Security Function SF.DES -- which is

Triple DES encryption and decryption by the cryptographic hardware and

(ii) for other usage of encryption and decryption within the TOE.

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

The code in the Test ROM of the TOE (IC Dedicated Test 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 results of the evaluation are only applicable to the TOE as identified in table 5, produced in the semiconductor factory in Tonami and in Kyoto (Japan), labelled by the production line indicator „001“ and „010“, the firmware and software versions as indicated in table 5 and the documentation listed in chapter 6.

The validity can be extended to new versions and releases of the product or to chips from other production and manufacturing sites, 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.

9.2 Additional Evaluation Results

- The evaluation confirmed specific results of a previous smart card IC evaluation regarding assurance aspects for the development and production environment. This is outlined in part D of this report, annex A.
- To support a composite evaluation of the TOE together with a specific smart card embedded software additional evaluator actions were

performed during the TOE evaluation. The results are documented in the ETR-lite [24] according to [4, AIS 36]. Therefore, the interface between the smart card embedded software developer and the developer of the TOE was examined in detail.

10 Comments/Recommendations

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 to develop his software in form of the delivered documentation.

- The operational documents [10] - [23] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

In addition the following assumptions and requirements concerning external security measures, explicitly documented in the singles evaluation reports, have to be fulfilled:

- Requirement resulting from ADV_LLD:

  Since the hardware can not guarantee the storage of correct data in case of power loss during memory write operations the software has to implement appropriate measures to check if security relevant data are correctly written.

- Requirement resulting from ADO_DEL:

  As the TOE is under control of the user software, the chip manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the Smartcard Embedded Software Developer to include mechanisms in the implemented software which allows detection of modifications after the delivery.

- Requirement resulting from AGD_ADM and AGD_USR:

In the environment, the assumptions listed in [11], chapter 6 have to be taken into consideration from the Smartcard Embedded Software Developer:

- OS development
- Deal with user data
- Key to be used for cryptographic processing
- Use of private key cryptographic DES
- Implementation of command interpreter

The following requirements of the environment listed in [11] chapter 7 have to be taken into consideration from the Smartcard Embedded Software Developer:

- “Cryptographic key generation“ resulting from FCS_CKM.1, or “Import of user data without security attributes” resulting from FDP_ITC.1, or “Import of user data with security attributes” resulting from FDP_ITC.2,
- “Cryptographic key destruction“ resulting from FCS_CKM.4, and
- “Secure security attributes” resulting from FMT_MSA.2.

- Requirement resulting from AVA_VLA:
    - The TOE is protected by light sensors against DFA light attacks (e.g. with laser). Nevertheless there is still a possibility that the running program would be manipulated with a focused laser. The Smartcard Embedded Software Developer has to implement sufficient countermeasures in his software to counter such attacks, too.

The Card Manufacturer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

- All security hints described in [10] have to be considered.

In addition the following assumptions and requirements concerning external security measures, explicitly documented in the singles evaluation reports, have to be fulfilled:

- Requirement resulting from AGD_ADM and AGD_USR:

  In the environment the following assumptions listed in [10] chapter 6 have to be taken into consideration from the Card Manufacturer:
    - Process for packing IC into the Card
    - The following administrational hints listed in [AGD_CM, 4] have to be taken into consideration from the Card Manufacturer:
    - Deactivation of Card Manufacturer test functionality
- Requirement resulting from AVA_MSU:
    - The Card Manufacturer has to deactivate the Card Manufacturer test functionality before delivering the TOE.

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 [6] 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
DES	Data Encryption Standard; symmetric block cipher algorithm
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EMA	Electro magnetic analysis
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Symmetric block cipher algorithm based on the DES
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification
SC	TSF Scope of Control

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

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

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

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

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

- AIS 25, Version 2, 29 July 2002 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 1.2, July 2002
- AIS 26, Version 2, 6 August 2002 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 1.1, July 2002
- AIS 31, Version 1, 25 Sept. 2001 for: Functionality classes and evaluation methodology of physical random number generators
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 36, Version 1, 29 July 2002 for:
  CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and
  CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2 March 2002

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

[6] MN67S140 Smartcard IC Security Target, 1.2, 02.02.2006, Matsushita Electric Industrial Co., Ltd. (confidential document)

[7] MN67S140 Smartcard IC Security Target (ST-Lite), 1.2, 02.02.2006, Matsushita Electric Industrial Co., Ltd. (sanitized public document)

[8] Evaluation Technical Report (ETR) for MN67S140 Smartcard IC Version RV3, FW12-EAST JAPAN RAILWAY COMPANY SuicaII Contactless Smardcard IC Chip, Version 5, BSI-DSZ-CC-0334, from 03.03.2006, (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] MN67S140 Smartcard IC Administrator Guidance for Card Manufacturer, Version 1.0, 05.12.2005, Matsushita Electric Industrial Co., Ltd.

[11] MN67S140 Smartcard IC Administrator Guidance for Smartcard Embedded Software Developer, Version 1.0, 05.12.2005, Matsushita Electric Industrial Co., Ltd.

[12] MN67S140 Smartcard IC Administrator Guidance for Card Manufacturer, Version 1.0, 05.12.2005, Matsushita Electric Industrial Co., Ltd.

[13] MN67S140 Smartcard IC Administrator Guidance for Smart-cardEmbedded Software Developer, Version 1.0, 05.12.2005, Matsushita Electric Industrial Co., Ltd.

[14] MN101C/MN101E Series Cross Assemblers User's Manual, Version 16, 06.2005, Matsushita Electric Industrial Co., Ltd.

[15] MN101C/MN101E Series C Compiler User's Manual Usage Guide, Version 13, 06.2005, Matsushita Electric Industrial Co., Ltd

[16] MN101C00 Series C Compiler User's Manual Language Description Version 4, 08.1999, Matsushita Electric Industrial Co., Ltd.

[17] MN101C00 Series C Compiler User's Manual Library Reference, Version 2, 08.1999, Matsushita Electric Industrial Co., Ltd.

[18] MN101C/MN101E Series C Source Code Debugger for Windows® User's Manual, Version 3, 05.2004, Matsushita Electric Industrial Co., Ltd.

[19] MN101C/MN101E Series In-stallation Manual, Version 3, 06.2004, Matsushita Electric Industrial Co., Ltd.

[20] MN101C Series Instruction Manual, Version 4, 10.2002, Matsushita Electric Industrial Co., Ltd.

[21] MN101C Series LSI manual, Version 3, 02.1998, Matsushita Electric Industrial Co., Ltd.

[22] PCI/PC Card Installation Manual, Version 7.1, 03.2005, Matsushita Electric Industrial Co., Ltd.

[23] MN67S140 Software Library Specification 2.9, 18.11.2005, Matsushita Electric Industrial Co., Ltd.

[24] ETR-Lite for Composition (ETR-Lite) for MN67S140 Smartcard IC Version RV3, FW12-EAST JAPAN RAILWAY COMPANY SuicaII Contactless Smardcard IC Chip, Version 5, BSI-DSZ-CC-0334, from 03.03.2006

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

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

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

The conformance result consists of one of the following:

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

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

plus one of the following:

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

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

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

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

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

CC Part 3:

Assurance categorisation (chapter 2.5)

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

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

Table 1: Assurance family breakdown and map

Evaluation assurance levels (chapter 6)

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

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

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

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

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

Table 2: Evaluation assurance level summary

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

"Objectives

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

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

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

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

"Objectives

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

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

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

"Objectives

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

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

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

"Objectives

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

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

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

"Objectives

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

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

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

"Objectives

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

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

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

"Objectives

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

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

"Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

"Objectives

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

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

"Application notes

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

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

D Annexes

List of annexes of this certification report

Annex A: Evaluation results regarding development and production environment D-3

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0334-2006

Evaluation results regarding development and production environment

The IT product MN67S140 Smartcard IC, RV3, FV12 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0, extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC15408: 1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

As a result of the TOE certification, dated 16. March 2006, 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) Matsushita Electric Industrial Co., Ltd., Corporate System LSI Development Division, Semiconductor Company, 3-1-1 Yagumo-naka-machi, Moriguchi City, Osaka, 570-8501, Japan (Development)

b) Matsushita Electric Industrial Co., Ltd.,19 Nishi-kujyo Kasugachou, Minami-ku, Kyoto city, Kyoto, 601-8413, Japan (Production: Wafer Fab, Process Definition)

c) Matsushita Electric Industrial Co., Ltd., 271 Higashi-kaihatsu, Tonami City, Toyama 570-8501, Japan (Production: Wafer Fab, Production Testing)

d) Toppan Printing Co., Ltd., 1101-20, Myohoji-cho, Higashi Omi City, Shiga 527-8566 Japan (Mask Center)

e) Matsushita Electric Industrial Co., Ltd., Uozu Factory 800 Higashiyama Uozu City, Toyama 937-8585, Japan (Production: Testing)

f) Matsushita Electric Industrial Co., Ltd., Arai Factory 4-5-1 Kurihara, Myoukou City, Niigata 944-8555, Japan (Production: Mounting, Delivery)

The hardware part of the TOE produced in the semiconductor is labelled by the production line indicator „001“ for Tonami and „010“ for Kyoto (both in Japan).

For all sites listed above, the requirements have been specifically applied for each site and in accordance with the MN67S140 Smartcard IC Security Target, 1.2, 02.02.2006, Matsushita Electric Industrial Co., Ltd. (confidential document) [6]. The evaluators verified, that the threats are countered and the security objectives for the life cycle phases 2, 3 and 4 up to delivery at the end of phase 3 or 4 as stated in the TOE Security Target are fulfilled by the procedures of these sites.