



## Certification report

<b>Certification file:</b>	<b>TUVIT-DSZ-ITSEC-9130</b>
<b>Product / system:</b>	Smart Card IC SLE 66CX640P version m1422a16 and m1422a17
<b>Product manufacturer:</b>	Infineon Technologies AG St.-Martin-Straße 76 81617 München
<b>Customer:</b>	see above
<b>Evaluation facility:</b>	TÜViT, evaluation body for IT security
<b>Evaluation report:</b>	<i>Version 1.0 of 2001-03-23</i> Document-number: 2046088500010_TÜV_001.01_E Author: Dr. P. Bödeker
<b>Formal process:</b>	completely / properly conducted
<b>Result:</b>	E4 / high
<b>Evaluation stipulations:</b>	two (see section 1.5.1)
<b>Certifier:</b>	Dr. Christoph Sutter
<b>Certification stipulations:</b>	one (see section 1.6.1)

Essen, 2001-03-23

Dr. Ernst-Hermann Gruschwitz

Dr. Christoph Sutter

## Table of contents

<b>1</b>	<b>BASIS AND SUBJECT OF CERTIFICATION</b>	<b>5</b>
1.1	Target of evaluation (TOE) and evaluation criteria	5
1.2	Carrying out of evaluation and evaluation technical report	6
1.3	Results of the re-evaluation	6
1.4	Broadening of the results to other configurations	6
1.5	Stipulations, notes and recommendations of the evaluation	7
1.5.1	Stipulations for the product manufacturer	7
1.5.2	Notes for the product manufacturer	7
1.5.3	Recommendations and notes for the user	7
1.6	Certification stipulations and notes	9
1.6.1	Certification stipulations	9
1.6.2	Notes for the user from the certification	9
1.7	Independence of the certifier	9
<b>2</b>	<b>SUMMARY OF THE SECURITY TARGET</b>	<b>9</b>
2.1	Definition of the TOE and method of use	9
2.1.1	Definition of the TOE	9
2.1.2	Method of use	10
2.1.3	Extent of delivery of the TOE	11
2.2	Intended environment for use	12
2.3	Subjects, objects and access modes / actions	12
2.3.1	Objects worth being protected	12
2.3.2	Subjects	13
2.3.3	Types of access / actions	14
2.4	Assumed threats and security objectives	14
2.4.1	Assumed threats	14
2.4.2	Security objectives and security features	15
2.5	Security enforcing functions	16
2.5.1	SF1: Operating state checking	16
2.5.2	SF2: Data encryption with an on-chip key management and random number generation	16
2.5.3	SF3: Phase management and test mode lock-out	16

2.5.4	SF4: Protection against snooping	16
<b>2.6</b>	<b>Correlation security functions / threats / security objectives</b>	<b>16</b>
2.6.1	Countering security functions / threats	16
2.6.2	Suitability of the functionality	16
<b>2.7</b>	<b>Target evaluation level and strength of mechanism</b>	<b>18</b>
<b>3</b>	<b>RESULTS OF THE EVALUATION</b>	<b>19</b>
<b>3.1</b>	<b>Effectiveness Criteria - Construction</b>	<b>19</b>
3.1.1	Aspect 1: Suitability of Functionality	19
3.1.2	Aspect 2: Binding of Functionality	19
3.1.3	Aspect 3: Strength of Mechanisms	19
3.1.4	Aspect 4: Construction Vulnerability Assessment	20
<b>3.2</b>	<b>Effectiveness Criteria - Operation</b>	<b>21</b>
3.2.1	Aspect 1: Ease of Use	21
3.2.2	Aspect 2: Operational Vulnerability Assessment	22
<b>3.3</b>	<b>Correctness – Construction – The Development Process</b>	<b>23</b>
3.3.1	Phase 1: Requirements (security target)	23
3.3.2	Phase 2: Architectural Design	23
3.3.3	Phase 3: Detailed Design	24
3.3.4	Phase 4: Implementation	24
<b>3.4</b>	<b>Correctness – Construction – The Development Environment</b>	<b>25</b>
3.4.1	Aspect1: Configuration Control	25
3.4.2	Aspect2: Programming Languages and Compilers	26
3.4.3	Aspect3: Developers Security	26
<b>3.5</b>	<b>Correctness – Operation – The Operational Documentation</b>	<b>27</b>
3.5.1	Aspect1: User Documentation	27
3.5.2	Aspect2: Administration Documentation	27
<b>3.6</b>	<b>Correctness – Operation – The Operational Environment</b>	<b>28</b>
3.6.1	Aspect1: Delivery and Configuration	28
3.6.2	Aspect2: Start-up and Operation	28
<b>4</b>	<b>EXCERPTS OF ITSEC AND ITSEM</b>	<b>29</b>
<b>4.1</b>	<b>Assurance - Effectiveness</b>	<b>29</b>
<b>4.2</b>	<b>Assurance - Correctness</b>	<b>29</b>
<b>4.3</b>	<b>Classifying Security Mechanisms</b>	<b>30</b>

---

<b>4.4</b>	<b>Minimum Strength of Security Mechanism</b>	<b>31</b>
<b>5</b>	<b>BIBLIOGRAPHICAL REFERENCES</b>	<b>31</b>
<b>6</b>	<b>ABBREVIATIONS</b>	<b>32</b>

## 1 Basis and subject of certification

The certification was carried out on basis of the certification conditions of the certification body of TÜViT and the certification scheme which is agreed upon with the "Bundesamt für Sicherheit in der Informationstechnik"<sup>1</sup>.

This certification of the chip SLE 66CX640P is a **re-certification** on the basis of the certification TUVIT-DSZ-ITSEC-9115-2000 of the predecessor chip SLE 66CX320P. Functionally the SLE 66CX640P differs from the SLE 66CX320P by:

- doubling of the EEPROM memory size,
- twice implementation of the ROM, i. e. doubling to 2x 64k
- twice implementation of the XRAM, i. e. doubling to 2x 2048k,
- modification of the RNG, and
- implementation of the RNG test routines in the RMS routine.

A re-evaluation has been carried out using the evaluation results from the evaluation of the predecessor chip SLE 66CX320P. Results from the following evaluation aspects have been at least partly reused:

- security model (ITSEC E4.2-E4.4 security model part) and
- testing of the evaluator (ITSEC E4.13, 3.24, 3.28, 3.33, 3.37), and
- developers security (E4.21-E4.23).

### 1.1 Target of evaluation (TOE) and evaluation criteria

Subject of the re-certification is the hardware of the smart card security controller type SLE 66CX640P, version m1422a16 and m1422a17 of the company Infineon Technologies AG, St.-Martin-Straße 76, 81617 München<sup>2</sup> and part of the firmware belonging to it (entry into self test software, version 41.09.09). It is certified that the TOE was evaluated on basis of the "Information Technology Security Evaluation Criteria, Version 1.2 (1991)"<sup>3</sup> and the "Information Technology Security Evaluation Manual, Version 1.0 (1993)"<sup>4</sup>, against the product specific security target by the evaluation body for IT security of TÜV Informationstechnik GmbH<sup>5</sup>.

---

<sup>1</sup> Below briefly called BSI

<sup>2</sup> Below briefly called Infineon

<sup>3</sup> Below briefly called ITSEC

<sup>4</sup> Below briefly called ITSEM

<sup>5</sup> Below briefly called TÜViT

An excerpt of ITSEC and ITSEM is in chapter 4.

## 1.2 Carrying out of evaluation and evaluation technical report

The evaluation was carried out from 2001-02-14 until 2001-03-23 by:

- Arnold Abromeit,
- Dr. Patrick Bödeker,
- Wolfgang Peter, and
- Berthold Weghaus

The chairmanship of the evaluation was taken over by Wolfgang Peter and the evaluation technical report, Version 1.0 of 2001-03-23 (Number: 2046088500010\_TÜV\_001.01\_E) was drawn up by Dr. P. Bödeker.

## 1.3 Results of the re-evaluation

The re-evaluation was carried out successfully. The security enforcing functions work according to the security target, which is confirmed by the evaluation results. According to ITSEC the target of evaluation<sup>6</sup> is a product, which shows the following security functionality:

- operating state checking
- data encryption with on-chip key management and random number generation
- phase-management with test mode lock-out
- protection against snooping

The desired evaluation level **E4** was reached and the minimum strength of the checked mechanisms is **high**.

## 1.4 Broadening of the results to other configurations

The TOE is unambiguously marked by the mask specific version number. A configuration of the TOE by the end-user is not possible.

Any change of hardware and/or firmware by the product manufacturer has to be announced to the evaluation facility and to the certification body and may cause a re-evaluation resp. re-certification.

---

<sup>6</sup> Below briefly called TOE

## 1.5 Stipulations, notes and recommendations of the evaluation

### 1.5.1 Stipulations for the product manufacturer

The evaluation technical report contains the following two stipulations:

1. As settled between the evaluator and Infineon, the file workshop 140201 contains all results of the workshop. The file together with the additions resulted in the course of the evaluation has to be archived securely by Infineon. As the evaluation results and the overall evaluation have to be repeatable and reproducible, Infineon is required to be able at any time to present this file to look at.
2. The analysis of the strength of mechanisms bases on an assessment of time and expenses according to state-of-the-art technology. As the analytical techniques with regard to the reverse engineering and the DPA technology respectively will probably develop quickly in the future, a regular review of the analyses is absolutely necessary. Therefore, as soon as new knowledge in this fields exists, **after one year at the latest**, however, the minimum strength of the mechanisms should be re-evaluated and proved to the evaluation body.

### 1.5.2 Notes for the product manufacturer

The evaluation technical report contains no notes for the product manufacturer.

### 1.5.3 Recommendations and notes for the user

The evaluation technical report contains the following 8 recommendations / notes for the user:

1. The development environment of the operating system manufacturer<sup>7</sup> has to be secure, in order to be able to guarantee the security of the TOE on the whole.
2. It is possible to store data in the EEPROM without encryption, which might constitute a risk in case an attacker is given the possibility to read out this data. The operating system manufacturer is responsible for the use of all security functionalities made available by the TOE and controllable by him in a such way, that secure operation is guaranteed. These are the parameters for memory encryption determining areas of the encryption. In the data book [6] it is pointed out to the operating system manufacturer, which effects on the security not proper use of this functionality might have and it is described to him in detail how to use effectively the security mechanisms made available by the TOE.
3. In case an alarm is triggered, the contents of the XRAM are not being deleted. In order to prevent an attacker from reading out this data, the user operating system has to

---

<sup>7</sup> see paragraph 2.1.2 point 1 on page 10 for a description of the "operating system manufacturer"

delete explicitly the XRAM after each reset to the operating system. This fact is pointed out in the data book [6].

4. The delivered MMU is set thus, that SLE66CX640P is compatible with SLE66CX160S, i.e. all ROM areas are mapped. Since the movec blockade of the SLE66CX160S is no longer implemented, in this setting reading out of the ROM by a program in the EEPROM is possible. This is inconsistent with security target SO3. In order to avoid this, the operating system manufacturer has to program the MMU in a way that reading out is impossible. This fact is pointed out in the data book [6].
5. ROM contents of chips, being drawn up with the same mask, are identically encrypted. Therefore, it is recommended to store security critical data (e. g. identification and authentication data) not in the ROM, but in the EEPROM (this is encrypted chip individually). This fact is pointed out to the operating system manufacturer in an application note [7].
6. The TOE shows a power consumption depending on the executed commands and the used data. In principle it is possible to gain from this power consumption information about the data worked on. The TOE has different mechanisms, keeping the overall power consumption as low as possible and disguising a characteristic course of the power consumption. These mechanisms, however, have to be used purposefully by the operating system manufacturer – together with additional software measures – when programming the application in order to protect the TOE against such attacks effectively. In the data book [6] this fact is pointed out to the operating system manufacturer. Furthermore he is delivered application examples. Thus, it is described e. g. how to use these features against DPA attacks together with software measures implemented additionally by the operating system manufacturer. For this, Infineon makes available to the operating system manufacturer a suitable software implementation of the DES algorithm in the form of an application note [8]. The TOE has a hardware DES accelerator. In case the keys necessary for the calculation of the DES are transferred unencrypted into the DES accelerator, these keys can be spied out by means of a SPA/DPA [9]. In order to prevent this, the transfer of the keys have to be protected using the measures described in [8].
7. The TOE contains a random number generator. In order to identify hardware defects or possible manipulation attempts, during operation a test of the noise source of the random number generator has to be performed. In the data book [6] this fact is pointed out to the operating system manufacturer. In the RMS library Infineon makes available routines to the operating system manufacturer, with the help of which such a test can be performed.
8. The TOE has an active shielding for the identification of attacks by means of physical probing. It is possible for the operating system manufacturer to change this current pattern. [10] describes to him how to realise this. Moreover it is recommended to change this current pattern before any security critical operation and to compare the

returned values with the expected values accordingly frequently with regard to the software.

## 1.6 Certification stipulations and notes

### 1.6.1 Certification stipulations

As settled between the evaluator and Infineon, the file workshop 140201 contains all results of the workshop. The file together with the additions resulted in the course of the evaluation has to be archived securely by Infineon. As the evaluation results and the overall evaluation have to be repeatable and reproducible, Infineon is required to be able at any time to present this file to look at.

### 1.6.2 Notes for the user from the certification

The notes for the user of the evaluation report (see 1.5.3) are applicable. There are no additional notes for the user resulting from the certification report.

## 1.7 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 which 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.

## 2 Summary of the security target

### 2.1 Definition of the TOE and method of use

#### 2.1.1 Definition of the TOE

The target of evaluation<sup>8</sup> consists of the hardware of the smart card security controller SLE 66CX640P and a part of its firmware (entry in the self test software, Version 41.09.09)<sup>9</sup>. The purpose of the security controller is the use in smart cards for particularly security relevant applications.

The SLE 66CX640P consists of a dedicated micro processor (CPU) with a memory management unit (MMU), several memory types, a security logic, a timer and an interrupt-controlled I/O-interface. Furthermore a random number generator (RNG) and a checksum module (CRC module) are integrated on the chip.

---

<sup>8</sup> Below briefly called TOE

<sup>9</sup> Below briefly called SLE 66CX640P

The command set of the CPU is compatible to the command set of the standard processor SAB 8051 executing 6 times as fast and offers additional instructions for smart card applications. The memory consists of 256 Byte internal RAM (IRAM), 4 Kbytes extended RAM (XRAM), 136 Kbytes User-ROM, 8 Kbytes Test-ROM and 64 Kbytes EEPROM. With this it meets the requirements of the new generation of operating systems. The access from CPU to memory is carried out via the integrated memory encryption and decryption unit (MED). The access rights to the memories can be controlled with the memory management unit (MMU). Security-, sleep mode- and interrupt logic as well as the RNG are specially designed for smart card applications.

The sleep mode logic (clock stop mode according to ISO/IEC 7816-3 (1997)) serves for the reduction of the total power consumption. The timer allows easy implementation of modern communication protocols like T=1 and all other time critical operations. The interrupt-controlled I/O interface allows the parallel operation of smart card and terminal. The phase locked loop (PLL) unit allows to operate the SLE 66CX640P with a multiplication factor over the external clock signal. The RNG provides no pseudo-random number sequence, but rather produces genuine random numbers under all conditions. The CRC module facilitates the calculation of checksums according to ISO 3309 (16 Bit CRC).

Two modules for cryptographic operation are implemented in the TOE: The advanced crypto engine (ACE) for calculation of asymmetric algorithms like RSA and the DDES module which computes the complete DES algorithm within a few clock cycles. That module is especially designed to counter attacks like DPA.

### 2.1.2 Method of use

Owing to the versatile methods of use of the TOE, it is a product in accordance with ITSEC. There are two different methods of use of the TOE.

1. The operating system manufacturer uses the TOE, to implement the operating system and his specific applications on it. He is responsible for the integration of the TOE into a comprehensive security system using the security functionalities provided by the TOE. The operating system manufacturer integrates the TOE in the smart card and takes over the initialisation and personalisation of the smart card, which is no longer part of the TOE.
2. The end-user uses the TOE which is issued, personalised and initialised by the operating system manufacturer depending on the application like
  - Cashless funds transfer applications,
  - Applications in the field of telecommunications (GSM, PCN, paging- or broadcast-services),
  - Pay-TV applications,
  - Access control applications,

- Applications in the field of healthcare (patients´ cards, health professional cards),
- Signature applications or
- Combinations of the mentioned applications in case of multi-application cards.

The method of use of the product varies markedly depending on the application, which is determined by the software which therefore is beyond the TOE itself. Common features at the level of the TOE are secure data storage and processing, which guarantee confidentiality.

### 2.1.3 Extent of delivery of the TOE

At the TOE on hand two delivery procedures have to be classified.

Delivery of the RMS library and the necessary documentation to the operating system manufacturer for the development of applications for the TOE.

In this connection it is not the delivery of the TOE itself. The delivered RMS library is software containing routines for writing the EEPROM. The operating system manufacturer has to integrate this library in his operating system and deliver both of them back to the product manufacturer. The data book [6], the operational documentation [11], the application notes [7,8,10,12-14], and the security target [15] which are delivered to the operating system manufacturer contain additional information about how to use the security features of the TOE.

No.	description	type
1	RMS-library <sup>10</sup>	software
2	data book	document
3	application notes	document
4	operational documentation	document
5	security target	document

Table 1: Extent of delivery concerning application development

Delivery of the produced chips (including the operating systems) to the customer.

The delivered chips contain the TOE itself and the operating system. Delivery is limited to the preparation of the produced chips at the warehouse on the area of Infineon at Regensburg. There they will be received by the operating system manufacturer or by a haulier ordered by him.

<sup>10</sup> not part of the TOE

No.	description	type
1	SLE66CX640P	hardware/firmware
2	implemented operating system <sup>11</sup>	firmware

Table 2: Extent of delivery of the produced TOE

## 2.2 Intended environment for use

The environment of the TOE is on one hand the development environment of the operating system manufacturer, on the other hand the „final“ environment at the user of the finished product, the smart card. A secured development environment at the operating system manufacturer is essential in order to be able to guarantee the security of the TOE as a whole. Within the „final“ environment the technical measures of the TOE counter the threats described below in order to reach the security objectives. There are no requirements for the environment of the end-user.

## 2.3 Subjects, objects and access modes / actions

### 2.3.1 Objects worth being protected

In this section the objects are listed, which have to be protected against the threats stated in the security target. „Hardware“, not closer specified, means in the following the TOE hardware. The objects are:

#### O1: Hardware design

This is the entirety of all organisational and technical aspects, which lead to the finished mask information starting out from the chip specification. This includes in particular the basic concepts, the implementation of the functionality through the building blocks used (architecture), their electronic circuitry as well as the implementation in layout (chip design) under the constraints of the chip technology used. The implemented security functionality of the hardware requires particular protection.

#### O2: Firmware

The firmware consisting of RMS and STS represents an individual object worth being protected. As it is exclusively the product (hardware) manufacturer, who has influence on this, this object is presented apart from the following object O3 „operating system/application software and -data“.

<sup>11</sup> not part of the TOE

### O3: Operating system/application software and -data

Exclusively the operating system manufacturer has influence on the operating system which is stored in the user ROM. Appropriate implementation must prevent a potential attacker from gaining access to information about protection mechanisms by using the operating system. User specific data is all application relevant information stored in the EEPROM (programs and data).

Especially worth being protected are among others the access rights, authentication information, data protection mechanisms and crypto algorithms, implemented in the operating system and in the application software for the protection of user data, as well as the user data itself. With regard to the use of the TOE for applications subject to the Digital Signature Act [1,2] especially the protection of the private signature key is important.

The RMS routines are part of O3 as they are logically embedded in the application and as they are protected like the application.

### O4: Test routines

These are the routines stored at the test ROM which are only to be used for production testing – they are at the same time part of the firmware and therefore subset of O2 – but as they are protected additionally with the entry to the STS-TM, they are listed separately.

### O5: Product manufacturer specific data for chip identification

This is the data stored in the reserved ROM area and allocated by the product (hardware) manufacturer for the chip ID.

### O6: Product manufacturer specific data for memory encryption

This is the data used for the storage of the basic key for the memory encryption and decryption.

## 2.3.2 Subjects

The two following subjects are defined:

### S1: External users

These are persons who might attack the finished TOE (hardware or firmware). For example the end-user of the smart card has to be seen as potential attacker. Persons making use of the conditions of the development environment respectively the production line and compromising the TOE in the course of the development are therefore excluded.

### S2: Operating system manufacturer

The operating system manufacturer, producing the operating system in a secure development environment is not regarded as attacker. He is not threatening.

### 2.3.3 Types of access / actions

Only the operating system which is implemented securely in the environment of the product manufacturer accesses the TOE. The external user has no access to the TOE.

## 2.4 Assumed threats and security objectives

### 2.4.1 Assumed threats

The threats listed below may be supposed. Against these the TOE has to protect itself by suitable measures. Actions caused by the implemented operating system in a secure development environment are not looked upon as threat.

#### T1: Snooping

This type of threats deals with the risk that an attacker is able to read out information of objects worth being protected without permission.

##### T1.1: Disclosure of the hardware design (O1)

An attacker might try to gain information about the security functionality of the hardware. This includes aspects of chip-specification, -design and -technology.

##### T1.2: Unauthorised reading out of the firmware (O2)

An attacker might try to read out the firmware and thus try to gain information about implemented protection mechanisms.

##### T1.3: Unauthorised reading out of the operating system/application software and data (O3)

An attacker might try to read out operating system, application software or data.

##### T1.4: Unauthorised reading out of the product manufacturer specific data for memory encryption (O6)

An attacker might try to read out the memory area containing the basic key of the memory encryption and decryption.

#### T2: Unauthorised use

This type of threats deals with the risk, that an attacker uses the TOE without permission.

##### T2.1: Unauthorised execution of test routines (O4)

An attacker might try to execute without permission the routines of the STS test mode reserved for the product manufacturer, i. e. initiating the STS test mode entry.

#### T3: Unauthorised modifications

This type of threats deals with the risk, that an attacker modifies the TOE in a way that security functionalities of the TOE are by-passed or changed. The modifications listed are to be taken as representing deliberate action designed to enable unauthorised use of the TOE and the software or data stored in the TOE. Modifications destroying the TOE or making it unusable, are not listed.

T3.1: Unauthorised modification of the hardware (O1)

An attacker might try to modify the hardware and the implemented hardware-protection mechanisms respectively.

T3.2: Unauthorised modification of the firmware (O2)

An attacker might try to modify the firmware (program code and execution) including the protection mechanisms contained therein.

T3.3: Unauthorised modification of operating system/application software and -data (O3)

An attacker might try to modify the operating system (program code and execution), application programs or -data.

T3.4: Unauthorised modification of the test routines (O4)

An attacker might try to modify the routines of the STS test mode (program code and execution) or the STS test mode entry.

T3.5: Unauthorised modification of the product manufacturer specific data for chip identification (O5)

An attacker might try to modify the product manufacturer specific data of the individual chip identification.

T3.6: Unauthorised modification of the product manufacturer specific data for memory encryption. (O6)

An attacker might try to modify the data forming the basic key for memory encryption and decryption.

#### 2.4.2 Security objectives and security features

Starting out from the threats listed above the security objectives listed below may be derived. Modifications are to be taken according to threat T3.

SO1: The hardware must be protected against espionage of the security functionality.

SO2: The hardware must be protected against unauthorised modification of the security functionality.

SO3: The information stored in all memory devices must be protected against unauthorised access.

SO4: The information stored in all memory devices must be protected against unauthorised modification.

SO5: It must not be possible to execute the test routines of the STS test mode without authorisation.

ad SO3,4) Protection against access/modification of the information in the EEPROM must be supported by the operating system.

## 2.5 Security enforcing functions

To reach the security objectives and to counter the threats, the TOE contains the following 4 security enforcing functions (SF):

### 2.5.1 SF1: Operating state checking

The operating state of the TOE is monitored with regard to clock frequency and supply voltage. An alarm is given if the chip leaves the specified area.

### 2.5.2 SF2: Data encryption with an on-chip key management and random number generation

All data in memories is encrypted by the MED unit. Genuine random numbers which are generated from an analog circuit support the key management, but can also be used by an external application.

### 2.5.3 SF3: Phase management and test mode lock-out

During the operation three phases are classified: test mode (TM), user mode (UM) and chip identification mode (CI). Entry in the different modes is controlled by a combination of different flags and a cryptographic function.

### 2.5.4 SF4: Protection against snooping

Various mechanisms protect data against snooping during and outside the operation of the TOE. These are logical as well as topological design measures for covering up.

## 2.6 Correlation security functions / threats / security objectives

### 2.6.1 Countering security functions / threats

The following table shows which security functions counter the respective threats:

	T1.1	T1.2	T1.3	T1.4	T2.1	T3.1	T3.2	T3.3	T3.4	T3.5	T3.6
SF1		X	X	X		X	X	X	X	X	X
SF2		X	X	X				X			X
SF3		X	X	X	X			X	X	X	X
SF4	X	X	X	X		X	X	X	X	X	X

### 2.6.2 Suitability of the functionality

#### Security functions against espionage (T1)

Disclosure of the hardware design (T1.1) is countered by SF4 (protection against snooping), particularly the topological measures for disguising the design.

Thus, for example, the additional upper metal layer (shield) and the arrangement of critical system parts lying in lower levels of the TOE shall serve as visual protection against snooping. Deliberate misleading by more or less random placement and non-standard design of components counter this threat a well.

SF1 (operating state checking), SF2 (encryption), SF3 (test mode lock-out), and SF4 (protection against snooping) counter unauthorised reading out of the firmware, that is the memory contents of the ROM (T1.2). SF1 avoids the TOE getting into states where reading out might be possible. Attacks manipulating the physical parameters like voltage and CLK frequency can be detected and an alarm is generated. SF2 avoids the interpretation of data by attackers, in case they really read them out. The topological protection measures (SF4) described above counter physical espionage of the ROM masks. Moreover, a protection implemented in the hardware prevents data contained by the ROM from being read out by software in the EEPROM and the ROM area containing the test routines is only electrically active in the test mode.

Unauthorised reading out of operating system/application software and -data (T1.3) is countered by SF1, SF2, SF3, and SF4 analogously to T1.2. SF1 prevents the TOE from entering any state where readout could be possible. Attacks manipulating the physical parameter like voltage or CLK frequency can be detected and an alarm is generated. SF2 prevents the memory from selective modification, because the encryption has to be broken first. SF3 ensures that routines contained in the test ROM cannot be used for ROM or EEPROM readout. Covert channels like DPA could be used to reveal application data. This is countered by SF4.

Unauthorised reading out of the product manufacturer specific data for memory encryption (T1.4) is countered by SF1, SF2, SF3, and SF4. SF1 prevents the TOE from entering any state where readout could be possible. Attacks manipulating the physical parameter like voltage or CLK frequency can be detected and an alarm is generated. SF2 stores the key for the memory encryption encrypted with another algorithm. The interpretation is prevented, because the encryption has to be broken first. SF3 ensures that routines contained in the test ROM cannot be used for ROM or EEPROM readout. SF4 prevents the physical read out of the data, because single bits of the information are scrambled in the memory field.

#### Security functions countering unauthorised use (T2)

Unauthorised execution of test routines (T2.1) is countered by SF3. Mechanisms implemented in hard- as well as software prevent the unauthorised entry in the test mode. Also during the operation the different phases (CI, TM, UM) are protected by combined measures of hardware and STS.

#### Security functions countering unauthorised modifications (T3)

Since for modifying the objects worth being protected the knowledge concerning its construction and function is necessary, the security functions which counter espionage are

basically similar to the functions used to counter modifications of the same objects. If any modification has happened it must be detected to ensure security.

Therefore unauthorised modification of the hardware (T3.1) is countered by SF1 and SF4 analogously to countering threat T1.1.

Since firmware as well as operating system are contained in the mask programmed ROM and according to this they are also parts of the hardware, SF4 counters both T3.2 and T3.3, as modification are difficult in the physically hidden ROM and the bits are scrambled in the memory field. That scrambling has to be analysed before a selective modification will succeed. SF1 protects the circuitry of the memories from malfunction induced by external disturbs. T3.3 is countered additionally by SF2 which prevents the memory in the user ROM from selective modification, because the encryption has to be broken first.

Application software and -data (T3.3) stored in EEPROM are protected against modification analogously to T1.3 by SF1, SF2, SF3, and SF4. SF1 prevents unsecured states. SF2 makes it necessary to brake the encryption before selective modification will succeed. SF3 locks out the test mode which could be used for EEPROM programming. SF4 scrambles the bits in the EEPROM.

Modifications of the sequence of TM-routines (T3.4) are countered like the modification of other ROM memories by SF1 and SF4. In addition the test mode routines are protected by SF3.

Unauthorised modification of the product manufacturer specific data (T3.5) is countered by SF1 as the TOE is prevented from malfunction. SF3 protects the test mode which is used to program the EEPROM. SF4 counters external influences on the TOE. In addition to the topological measures scrambling the logical protection mechanism provides read-only or erase-only functionality of the EEPROM memory areas.

Unauthorised modification of the product manufacturer specific data for memory encryption (T3.6) is countered by SF1, SF2, SF3, and SF4. SF1 prevents the TOE from malfunctions. SF2 prevents the memory contents from selective modification because the encryption has to be broken first. SF3 disables the test mode, which could be used to write data. SF4 hinders the assignment bit to byte.

## 2.7 Target evaluation level and strength of mechanism

The target evaluation level striven for by the claimant is **E4**.

The minimum strength of mechanisms striven for by the claimant is **high**.

### 3 Results of the Evaluation

#### 3.1 Effectiveness Criteria - Construction

##### 3.1.1 Aspect 1: Suitability of Functionality

*ITSEC 3.14 The suitability analysis shall link security enforcing functions and mechanisms to the threats, enumerated in the security target, that they are designed to counter.*

*ITSEC 3.15 The suitability analysis shall show how the threats are countered by the security enforcing functions and mechanisms. It shall show that there are no threats that are not adequately countered by one or more of the stated security enforcing functions. The analysis shall be performed using, at minimum, all the information given in figure 4 [5] for the evaluation level in question.*

*ITSEC 3.16 Check that the suitability analysis provided meets all requirements for content and presentation and evidence. Check that the analysis has considered all of the information given in figure 4 [5] for the evaluation level in question.*

**Ascertainment of certification body:** The evaluation facility checked and ascertained that the suitability analysis meets all requirements for content and presentation and evidence (ITSEC 3.14, 3.15) and considered all relevant information. The relation between security functions and threats is shown in section 2.6.

##### 3.1.2 Aspect 2: Binding of Functionality

*ITSEC 3.18 The binding analysis shall provide an analysis of all potential interrelationships between security enforcing functions and mechanisms.*

*ITSEC 3.19 The binding analysis shall show that it is not possible to cause any security enforcing function or mechanism to conflict with or contradict the intent of other security enforcing functions or mechanisms. The analysis shall be performed using, at minimum, all the information given in figure 4 [5] for the evaluation level in question.*

*ITSEC 3.20 Check that the binding analysis provided meets all requirements for content and presentation and evidence. Check that the analysis has considered all of the information given in figure 4 [5] for the evaluation level in question.*

**Ascertainment of certification body:** The evaluation facility checked and ascertained that the binding analysis meets all requirements for content and presentation and evidence (ITSEC 3.18, 3.19) and considered all relevant information.

##### 3.1.3 Aspect 3: Strength of Mechanisms

*ITSEC 3.22 The strength of mechanisms analysis shall list all security enforcing mechanisms that have been identified as critical within the TOE. It shall include or reference analyses of the underlying algorithms, principles and properties of those mechanisms.*

*ITSEC 3.23 The strength of mechanisms analysis shall show that all critical mechanisms satisfy the claimed minimum strength of mechanisms rating, as defined in paragraphs 3.6 to 3.8: in the case of cryptographic mechanisms, this shall take the form of a statement*

*of confirmation from the appropriate national body. Other analyses shall be performed using, at minimum, all the information given in figure 4 [5] for the evaluation level in question.*

*ITSEC 3.24 Check that all mechanisms that are critical have been identified as such. Check that the strength of mechanisms analysis provided meets all requirements for content and presentation and evidence. Check that the analysis has considered all of the information given in figure 4 [5] for the evaluation level in question. Check that the specifications/definitions of all critical mechanisms support the claimed minimum strength rating. Perform **penetration testing** where necessary to confirm or disprove the claimed minimum strength of mechanisms.*

Ascertainment of certification body: Within the TOE all existing mechanisms are identified as critical and categorised in type A and B mechanisms. The evaluation facility checked and ascertained, that all critical mechanisms were identified as such. The submitted strength of mechanisms analysis meets all requirements for content and presentation and evidence (ITSEC 3.22, 3.23) and considers all relevant information. The specifications/definitions of all critical mechanisms support the claimed minimum strength high. The evaluation facility performed penetration tests and ascertained that the respective type A mechanisms support the claimed minimum strength high and that the type B mechanisms cannot be by-passed.

#### 3.1.4 Aspect 4: Construction Vulnerability Assessment

*ITSEC 3.26 The list of known vulnerabilities provided by the sponsor shall identify all vulnerabilities in the construction of the TOE known to him. It shall identify each known vulnerability, provide an analysis of its potential impact, and identify the measures proposed or provided to counter its effect.*

*ITSEC3.27 The analysis of the potential impact of each known vulnerability shall show that the vulnerability in question cannot be exploited in the intended environment for the TOE, because either:*

- *the vulnerability is adequately covered by other, uncompromised, security mechanisms, or*
- *it can be shown that the vulnerability is irrelevant to the security target, will not exist in practice, or can be countered adequately by documented technical, personnel, procedural or physical security measures outside the TOE. These external security measures shall have been defined within (or shall have been added to) the appropriate documentation.*

*The analysis shall be performed using, at minimum, all the information given in figure 4 [5] for the evaluation level in question.*

*ITSEC 3.28 Check that the list of known vulnerabilities in construction meets all requirements for content and presentation and evidence given above. Check that the analysis of the potential impact of each vulnerability has considered all of the information given in figure 4 [5] for the evaluation level in question. Perform an independent vulnerability analysis, taking into account both the listed and any other known construction vulnerabilities found during evaluation. Check that all combinations of known vulnerabilities have been addressed. Check that the analyses of the potential*

*impact of vulnerabilities contain no undocumented or unreasonable assumptions about the intended environment. Check that all assumptions and requirements for external security measures have been appropriately documented. Perform penetration testing to confirm or disprove whether the known vulnerabilities are actually exploitable in practice.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the list of known vulnerabilities in construction meets all requirements for content and presentation and evidence (ITSEC 3.26, 3.27) as described above. It checked and ascertained that the analysis considered all relevant information. The evaluation facility carried out an own vulnerability analysis and detected five further vulnerabilities. This was judged to be a fact which cannot be exploited. The evaluation facility checked and ascertained that all combinations of known vulnerabilities were checked and that no new vulnerabilities result from this. The evaluation facility checked and ascertained that the TOE contains no unreasonable or undocumented assumptions about the intended environment and that all assumptions and requirements for external security measures have been appropriately documented. The evaluation facility performed penetration tests and ascertained that the known vulnerabilities are actually not exploitable in practice.

## 3.2 Effectiveness Criteria - Operation

### 3.2.1 Aspect 1: Ease of Use

*ITSEC 3.31 The ease of use analysis shall identify possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation.*

*ITSEC 3.32 The ease of use analysis shall show that any human or other error in operation that deactivates or disables security enforcing functions or mechanisms will be easily detectable. It shall show that if it is possible to configure or cause the TOE to be used in a way which is insecure (i.e. the security enforcing functions and mechanisms of the TOE do not satisfy the security target), when an end-user or administrator of the TOE would reasonably believe it to be secure, then this fact will also be detectable. The analysis shall be performed using, at minimum, all the information given in figure 4 [5] for the evaluation level in question.*

*ITSEC 3.33 Check that the ease of use analysis provided meets all requirements for content and presentation and evidence. Check that the analysis has considered all of the information given in figure 4 for the evaluation level in question. Check the analysis for undocumented or unreasonable assumptions about the intended environment. Check that all assumptions and requirements for external security measures (such as external procedural, physical and personnel controls) have been appropriately documented. Repeat any configuration and installation procedure to check that the TOE can be configured and used securely, using only the user and administration documentation for guidance. Perform other testing where necessary to confirm or disprove the ease of use analysis.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the ease of use analysis submitted meets all requirements for content and presentation and

evidence (ITSEC 3.31, 3.32) and that the analysis considered all relevant information. It furthermore checked and ascertained that the analysis contains no undocumented or unreasonable assumptions about the intended environment. The evaluation facility checked and ascertained that all assumptions and requirements for external security measures have been appropriately documented. The TOE is only available in one single configuration which cannot be changed by the end-user. Therefore the repeating of the configuration and installation procedures is inapplicable. Additional tests were performed by the evaluation facility confirming the ease of use analysis.

### 3.2.2 Aspect 2: Operational Vulnerability Assessment

*ITSEC 3.35 The list of known vulnerabilities provided by the sponsor shall identify all vulnerabilities in operation of the TOE known to him. It shall identify each known vulnerability, provide an analysis of its potential impact, and identify the measures proposed or provided to counter its effect.*

*ITSEC 3.36 The analysis of the potential impact of each known vulnerability shall show that the vulnerability in question cannot be exploited in the intended environment for the TOE, because either:*

- *the vulnerability is adequately covered by other, uncompromised, external security measures, or*
- *It can be shown that the vulnerability is irrelevant to the security target or will not be exploitable in practice.*

*The analysis shall be performed using, at minimum, all the information given in figure 4 [5] for the evaluation level in question. Any required external security measures shall have been defined within (or shall have been added to) the appropriate documentation.*

*ITSEC 3.37 Check that the list of known vulnerabilities in operation meets all requirements for content and presentation and evidence given above. Check that the analysis of the potential impact of each vulnerability has considered all of the information given in figure 4 for the evaluation level in question. Perform an independent vulnerability analysis, taking into account both the listed and any other known operational vulnerabilities found during evaluation. Check that all combinations of known vulnerabilities have been addressed. Check that the analyses of the potential impact of vulnerabilities contain no undocumented or unreasonable assumptions about the intended environment. Check that all assumptions and requirements for external security measures have been appropriately documented. Perform penetration testing to confirm or disprove whether the known vulnerabilities are actually exploitable in practice.*

**Ascertainment of certification body:** There are no operational vulnerabilities known to the product manufacturer. The evaluation facility performed an own vulnerability analysis and ascertained no operational vulnerabilities. Therefore a list of the known operational vulnerabilities is inapplicable. The evaluation facility checked and ascertained that the analysis considered all relevant information. As no operational vulnerabilities have been ascertained the analysis of all potential combinations of vulnerabilities as well as the analysis of potential impacts are inapplicable. Furthermore there are no additional assumptions or

requirements for external security measures which have to be documented and no penetration tests had to be performed by the evaluation facility.

### 3.3 Correctness – Construction – The Development Process

#### 3.3.1 Phase 1: Requirements (security target)

*ITSEC E4.2 The security target shall describe the security enforcing functions to be provided by the TOE. In the case of a system, in addition the security target shall include a System Security Policy (SSP) identifying the security objectives and the threats to the system. In the case of a product, in addition the security target shall include a rationale, identifying the method of use for the product, the intended environment and the assumed threats within that environment. A **formal model of security policy shall be provided or referenced to define the underlying security policy to be enforced by the TOE. An informal interpretation of this model in terms of the security target shall be provided.** The security enforcing functions within the security target shall be specified using **both an informal and semiformal style as categorised in Chapter 2.***

*ITSEC E4.3 In the case of a system the security target shall describe how the proposed functionality fulfils the security objectives and is adequate to counter the identified threats. In the case of a product the security target shall describe how the functionality is appropriate for that method of use and is adequate to counter the assumed threats. **The informal interpretation of the formal security policy model shall describe how the security target satisfies the underlying security policy.***

*ITSEC E4.4 Check that the information provided meets all requirements for content and presentation and evidence. Check that there are no inconsistencies in the security target. **Check that there are no security features in the security target that conflict with the underlying security policy.***

Ascertainment of certification body: In the security target the TOE is defined as product according to ITSEC. The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.2, E4.3) for a product and that there are no inconsistencies in the security target<sup>12</sup>. The evaluation facility checked and ascertained that there are no security measures that conflict with the underlying security policy.

#### 3.3.2 Phase 2: Architectural Design

*ITSEC E4.5 A **semiformal notation shall be used in the architectural design to produce a semiformal description.** It shall describe the general structure of the TOE. It shall describe the external interfaces of the TOE. It shall describe any hardware and firmware required by the TOE with a statement of the functionality of supporting protection mechanisms implemented in that hardware or firmware. It shall describe the separation of the TOE into security enforcing and other components.*

---

<sup>12</sup> For a summary of the security target see chapter 2.

*ITSEC E4.6 The description of the architecture shall describe how the security enforcing functions of the security target will be provided. It shall describe how the separation into security enforcing and other components is achieved. **It shall describe how the chosen structure provides for largely independent security enforcing components.***

*ITSEC E4.7 Check that the information provided meets all requirements for content and presentation and evidence. Check that the separation of security enforcing and other components is valid.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.5, E4.6). The evaluation facility checked and ascertained that the separation of security enforcing and other components is valid.

### 3.3.3 Phase 3: Detailed Design

*ITSEC E4.8 A semiformal notation shall be used to develop a semiformal detailed design. The detailed design shall specify all basic components. **It shall describe, through all levels of the design hierarchy, the realisation of all security enforcing and security relevant functions. It shall describe the separation of the TOE into security enforcing, security relevant and other components. It shall be structured into well-defined, largely independent basic components that facilitate testing and minimise the potential for violations of security.** It shall identify all security mechanisms. It shall map security enforcing functions to mechanisms and components. All interfaces of security enforcing and security relevant components shall be documented stating their purpose and parameters. Specifications/definitions for mechanisms shall be provided. These specifications shall be suitable for the analysis of interrelationships between the mechanisms employed. Specifications need not be provided for components that are neither security enforcing nor security relevant. Where more than one level of specification is provided, there shall be a clear and hierarchical relationship between levels.*

*ITSEC E4.9 The detailed design shall describe how the security mechanisms provide the security enforcing functions specified in the security target. It shall describe why components for which no design information is provided cannot be either security enforcing or security relevant.*

*ITSEC E4.10 Check that the information provided meets all requirements for content and presentation and evidence.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.8, E4.9).

### 3.3.4 Phase 4: Implementation

*ITSEC E4.11 The description of correspondence shall describe the correspondence between source code or hardware drawings and basic components of the detailed design. The test documentation shall contain plan, purpose, procedures and results of the tests **and a justification why the extent of test coverage is sufficient.** The library of test programs shall contain test programs and tools to enable all tests covered by the test documentation to be repeated.*

*ITSEC E4.12 The test documentation shall describe the correspondence between tests and the security enforcing functions defined in the security target. It shall describe the correspondence between tests and the security enforcing and security relevant functions defined in the detailed design. It shall describe the correspondence between tests and the security mechanisms as represented in the source code or hardware drawings. Evidence of retests after the discovery and correction of errors relevant to security is obligatory to demonstrate that the errors have been eliminated and no new errors have been introduced.*

*ITSEC E4.13 Check that the information provided meets all requirements for content and presentation and evidence. Use the library of test programs to check by sampling the results of tests. Check that tests cover all security enforcing functions identified in the security target. Check that the tests cover all security enforcing and security relevant functions identified in the detailed design and all security mechanisms identifiable in the source code or hardware drawings. Check all retesting following the correction of errors. Perform additional tests to search for errors.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.11, E4.12). The library of test programs had been used to check by sampling the results of tests. The evaluation facility checked and ascertained that tests cover all security enforcing functions identified in the security target. The evaluation facility checked and ascertained that the tests cover all security enforcing and security relevant functions identified in the detailed design and all security mechanisms identifiable in the source code or hardware drawings. The check of all retesting following the correction of errors is inapplicable since no such tests were performed. Additionally the evaluation facility performed tests to search for errors. In this connection no errors were found.

### **3.4 Correctness – Construction – The Development Environment**

#### **3.4.1 Aspect1: Configuration Control**

*ITSEC E4.15 The development process shall be supported by a **tool based** configuration control system and an acceptance procedure. The configuration list provided shall enumerate all basic components out of which the TOE is built. The TOE, its basic components and all documents provided including the manuals and the source code or hardware drawings shall possess a unique identifier. The use of this unique identifier is obligatory in references. The configuration control system shall ensure that the TOE under evaluation matches the documentation provided and that only authorised changes by **authorised persons** are possible. **The configuration control tools shall be able to control and audit changes between different versions of objects subject to configuration control.***

*ITSEC E4.16 The information on the configuration control system shall describe how it is used in practice and applied in the manufacturing process in accordance with the developer's quality management procedures.*

*ITSEC E4.17 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and*

*evidence. Use the developers tools to rebuild selected parts of the TOE and compare with the submitted version of the TOE.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the documented procedures are being applied and that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.15, E4.16). The evaluation facility rebuilt selected parts of the TOE and ascertained no differences with the submitted version of the TOE.

#### 3.4.2 Aspect2: Programming Languages and Compilers

*ITSEC E4.18 Any programming languages used for implementation shall be well-defined, e.g. as in an ISO standard. Any implementation dependent options of the programming language shall be documented. For all compilers used, the implementation options selected shall be documented.*

*ITSEC E4.19 The definition of the programming languages shall define unambiguously the meaning of all statements used in the source code.*

*ITSEC E4.20 Check that the information provided meets all requirements for content and presentation and evidence.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.18, E4.19).

#### 3.4.3 Aspect3: Developers Security

*ITSEC E4.21 The document on the security of the development environment shall describe the intended protection for the integrity of the TOE and the confidentiality of the associated documents. Physical, procedural, personnel and other security measures used by the developer shall be described.*

*ITSEC E4.22 The information on the security of the development environment shall describe how the integrity of the TOE and the confidentiality of the associated documentation are maintained.*

*ITSEC E4.23 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence. Search for errors in the procedures.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the documented procedures are being applied. The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.21, E4.22). The evaluation facility searched for errors in the documented procedures and ascertained that they are errorless.

### 3.5 Correctness – Operation – The Operational Documentation

#### 3.5.1 Aspect1: User Documentation

*ITSEC E4.25 The user documentation shall describe the security enforcing functions relevant to the end-user. It shall also give guidelines covering their secure operation. The user documentation e.g. Reference Manuals, User Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level.*

*ITSEC E4.26 The user documentation shall describe how an end-user uses the TOE in a secure manner.*

*ITSEC E4.27 Check that the information provided meets all requirements for content and presentation and evidence.*

Ascertainment of certification body: The TOE is delivered exclusively to the operating system manufacturer. He corresponds to the system administrator of ITSEC. The actual end-user receives the TOE from the operating system manufacturer together with the application running on the TOE. Therefore no user documentation on the part of the chip manufacturer is necessary for the TOE. For this reason only one operational documentation exists dealing with both aspects of ITSEC together (user and administration documentation).

The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.25, E4.26).

#### 3.5.2 Aspect2: Administration Documentation

*ITSEC E4.28 The administration documentation shall describe the security enforcing functions relevant to an administrator. It shall distinguish two types of functions: those which allow an administrator to control security parameters, and those which only allow him to obtain information. If an administrator is required, it shall describe all security parameters which are under his control. It shall describe each type of security-relevant event, relevant to the administrative functions. It shall describe details, sufficient for use, of procedures relevant to the administration of security. It shall give guidelines on the consistent and effective use of the security features of the TOE and how those features interact. It shall describe instructions on how the system/product shall be installed and how, if appropriate, it shall be configured. The administration documentation, e.g. Reference Manuals, Administrator Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level.*

*ITSEC E4.29 The administration documentation shall describe how the TOE is administered in a secure manner.*

*ITSEC E4.30 Check that the information provided meets all requirements for content and presentation and evidence.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.28, E4.29)<sup>13</sup>.

### 3.6 Correctness – Operation – The Operational Environment

#### 3.6.1 Aspect1: Delivery and Configuration

*ITSEC E4.32 If different configurations are possible, the impact of the configurations on security shall be described. The procedures for delivery and system generation shall be described. A procedure approved by the national certification body for this evaluation level shall be followed, which guarantees the authenticity of the delivered TOE. While generating the TOE, any generation options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how and when the TOE was generated.*

*ITSEC E4.33 The information supplied shall describe how the procedures maintain security.*

*ITSEC E4.34 Check that the information provided meets all requirements for content and presentation and evidence. Check the correct application of the delivery procedures. Search for errors in the system generation procedures.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.32, E4.33). The TOE is delivered with only one single configuration determined unambiguously by the mask version. Therefore there is no impact of different configurations on the security. The correct application of the delivery procedures was checked. The TOE has to be collected directly from the product manufacturer which is the delivery procedure<sup>14</sup> admitted by BSI for evaluation level E4.

#### 3.6.2 Aspect2: Start-up and Operation

*ITSEC E4.35 The procedures for secure start-up and operation shall be described. If any security enforcing functions can be deactivated or modified during start-up, normal operation or maintenance, this shall be described. **Procedures shall exist which can restore the TOE to a secure state after a failure, or a hardware or software error.** If the TOE contains hardware which contains security enforcing hardware components, then administrator, end-user, or self initiated diagnostic tests shall exist that can be performed on the TOE in its operational environment.*

*ITSEC E4.36 The information supplied shall describe how the procedures maintain security. The sponsor shall provide example results from all diagnostic test procedures for security enforcing hardware components. The sponsor shall provide examples of any audit trail output created during start-up and operation.*

---

<sup>13</sup> See also the remarks of section 3.5.1

<sup>14</sup> See AIS 10, version 2 as of 96-12-18

*ITSEC E4.37 Check that the information provided meets all requirements for content and presentation and evidence. Check the example evidence required for start-up and operation. Search for errors in the procedures.*

Ascertainment of certification body: The evaluation facility checked and ascertained that the information provided meets all requirements for content and presentation and evidence (ITSEC E4.35, E4.36). Since no result protocols of hardware diagnoses and no protocol information are created during start-up and operation, no check is necessary. Production tests performed before delivery of the TOE to the customer were checked. As a result of the production tests follows either a correctly working TOE or a not functioning TOE. Not functioning chips are being destroyed. The evaluation facility searched for errors in the procedures and ascertained no errors.

## 4 Excerpts of ITSEC and ITSEM

### 4.1 Assurance - Effectiveness

*ITSEC 3.2:*

Assessment of effectiveness involves consideration of the following aspects of the TOE:

- a) the suitability of the TOE's security enforcing functions to counter the threats to the security of the TOE identified in the security target;
- b) the ability of the TOE's security enforcing functions and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;
- c) the ability of the TOE's security mechanisms to withstand direct attack;
- d) whether known security vulnerabilities in the *construction* of the TOE could in practice compromise the security of the TOE;
- e) that the TOE cannot be configured or used in a manner which is insecure but which an administrator or end-user of the TOE would reasonably believe to be secure;
- f) whether known security vulnerabilities in the *operation* of the TOE could in practice compromise the security of the TOE.

### 4.2 Assurance - Correctness

*ITSEC 4.2-4.10:*

Seven evaluation levels are defined in respect of the confidence in the correctness of a TOE. E0 designates the lowest level and E6 the highest. The seven evaluation levels can be *characterised* as follows:

#### Level E0

This level represents inadequate assurance.

### Level E1

At this level there shall be a security target and an informal description of the architectural design of the TOE. Functional testing shall indicate that the TOE satisfies its security target.

### Level E2

In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.

### Level E3

In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.

### Level E4

In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.

### Level E5

In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.

### Level E6

In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.

## **4.3 Classifying Security Mechanisms**

### *ITSEM 6.C.4-6.C.7*

A type A mechanism is a security mechanism with a potential vulnerability in its algorithm, principles or properties, whereby the mechanism can be overcome by the use of sufficient resources, expertise and opportunity in the form of a direct attack. An example of a type A mechanism would be an authentication program using a password: if the passwords can be guessed by attempting all possible passwords in succession, the authentication mechanism is of type A. type A mechanism often involve the use of a „secret“ such as a password or cryptographic key.

All type A mechanisms on a TOE have a strength, which corresponds to the level of resources, expertise and opportunity required to compromise security by directly attacking the mechanism.

When assessing the strength of a mechanism, the context in which the mechanism operates should be taken into account. See the Example subsection below.

A type B mechanism is a security mechanism which, if perfectly conceived and implemented, will have no weaknesses. A type B mechanism can be considered to be impregnable to direct attack regardless of the level of resources, expertise and opportunity deployed. A potential example of a type B mechanism would be access control based on access control lists: if perfectly conceived and implemented, this type B mechanism cannot be defeated by direct attack. However, these type B mechanisms can be defeated by indirect attacks which are the subject of other effectiveness analyses.

#### 4.4 Minimum Strength of Security Mechanism

##### *ITSEC 3.5-3.8*

All critical security mechanisms (i.e. those mechanisms whose failure would create a security weakness) are assessed for their ability to withstand direct attack. The minimum strength of each critical mechanism shall be rated either *basic*, *medium* or *high*.

For the minimum strength of a critical mechanism to be rated **basic** it shall be evident that it provides protection against random accidental subversion, although it may be capable of being defeated by knowledgeable attackers.

For the minimum strength of a critical mechanism to be rated **medium** it shall be evident that it provides protection against attackers with limited opportunities or resources.

For the minimum strength of a critical mechanism to be rated **high** it shall be evident that it could only be defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicality.

## 5 Bibliographical references

- [1] ITSEC: *Information Technology Security Evaluation Criteria*, version 1.2 (1991)
- [2] ITSEM: *Information Technology Security Evaluation Manual*, version 1.0 (1993)
- [3] *Digital Signature Act (Signaturgesetz – SigG)* as of 1997-10-22
- [4] *Digital Signature Ordinance (Signaturverordnung – SigV)* as of 1997-10-22
- [5] According to figure 4 of the ITSEC criteria for level E4 at least the following information resp. documents for carrying out of the vulnerability analysis are to be used:
  - a) the security target,
  - b) a formal model of security policy,
  - c) an informal description of functions,
  - d) a semiformal description of functions,
  - e) a semiformal description of the architectural design,
  - f) a semiformal description of the detailed design,

- g) the hardware drawings and the source code, and
- h) the complete operational documentation.
- [6] Preliminary Confidential Data Book, Security and Chip Cards ICs, SLE 66CxxxP, version 12.00.
- [7] Confidential Application Note, SLE 66CxxxP, Memory Encryption Decryption, version 5.00.
- [8] Confidential Application Note, SLE 66CxxxP, DES / EC2 Accelerator, version 5.00.
- [9] Security Check of the Smart Card Processor SLE66CX320P STS version 40.09.09 2000-04-19.
- [10] Confidential Application Note, Using the Active Shield Feature, version 3.00.
- [11] Operational Documentation SLE66CX640P, version 1.0, 2001-02-16
- [12] Confidential Application Note, SLE 66CxxxP, Testing the Random Number Generator, version 5.00.
- [13] Confidential Application Note, SLE 66CxxxP, Transfer of a ROM Mask from SLE 66CxxS to SLE66CX320P, version 11.99.
- [14] Confidential Application Note, SLE 66CxxxP, UART, version 3.00.
- [15] Security Target SLE66CX640P, Version 1.0, 2001-03-01

## 6 Abbreviations

ACE	advanced crypto engine
AIS	application notes and interpretations concerning the scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik (federal bureau for information technology security)
CI	chip identification mode (STS)
CPU	central processing unit
EEPROM	electrical erasable and programmable read only memory
ID	identification
IRAM	internal random access memory
ITSEC	Information Technology Security Evaluation Criteria, version 1.2 (1991)
ITSEM	Information Technology Security Evaluation Manual, version 1.0 (1993)
MED	memory encryption and decryption unit
MMU	memory management unit

---

PLL	phase locked loop
PROM	programmable read only memory
RMS	resource management system
RNG	random number generator
ROM	read only memory
STS	self test software
TM	test mode
TOE	target of evaluation
UM	user mode
XRAM	extended random access memory