Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0431-2007

for

Infineon Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12, SLE66CL41PE / m1583-e12 with specific IC Dedicated Software

from

Infineon Technologies AG

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

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0431-2007

Infineon Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12, SLE66CL41PE / m1583-e12 with specific IC Dedicated Software

Common Criteria Arrangement for components up to EAL4

from

Infineon Technologies AG

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, version 2.3* (ISO/IEC 15408:2005) extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0002-2001**
Functionality:	**BSI-PP-0002-2001 conformant plus product specific extensions Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant**, **EAL5 augmented by:** 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, 30. August 2007

The Vice President of the Federal Office for Information Security

Hange L.S.

IT Security Certified

SOGIS - MRA

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

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

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

---

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

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

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

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

2 Recognition Agreements

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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 the arrangement has been signed by the national bodies of:

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

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

This evaluation contains the components ACM_SCP.3, ADV_FSP.3, ADV_HLD.3, ADV_INT.1, ADV_RCR.2, ADV_SPM.3, ALC_DVS.2, ALC_LCD.2, ALC_TAT.2, ATE_DPT.2, AVA_CCA.1, 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 products Infineon Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12, SLE66CL41PE / m1583-e12 with specific IC Dedicated Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0399-2007.

The evaluation of the products Infineon Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12, SLE66CL41PE / m1583-e12 with specific IC Dedicated Software was conducted by TÜV Informationstechnik GmbH. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Infineon Technologies AG , Am Campeon 1-12 , D-85579 Neubiberg, Germany

The certification is concluded with

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

This work was completed by the BSI on 30. August 2007.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

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

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-28 and D1 to D-4.

The products Infineon Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12, SLE66CL41PE / m1583-e12 with specific IC Dedicated Software 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] Infineon Technologiel AG
Am Campeon 1-12
D-85579 Neubiberg, Germany

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The product type of the Target of Evaluation (TOE) is the Infineon Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12, SLE66CL41PE / m1583-e12 with specific IC Dedicated Software.

Compared to the product SLE66CLX800PEx / SLE66CLX360PEx (BSI-DSZ-CC-0399) the TOE has different memory sizes for ROM, RAM and EEPROM, and the Advanced Crypto Engine is not implemented. The TOE is implemented with UCP (Unified Channel Programming) technology. This TOE, comprising the group of derivates listed on the title page, is principally based on the same hardware as the first contactless PE-derivate group comprising the derivates with the 80 kByte and 36 kByte EEPROM which have successfully passed the EAL5+ evaluation as well. This was the BSI internal process BSI-DSZ-CC-0399-2007. The security policy of this product is unchanged. The Security Target [6] was updated.

The TOE is manufactured in IC fabrication in Altis, France, indicated by the production line indicator “5” (see part D, Annex A of this report).

The differences in the contactless interface area are responsible for the different naming extensions “M”, “S” or coming without extension. The derivates without extension communicate with the contact-based interface according to ISO 7816/ETSI/EMV and with the contactless interface according to ISO 14443 type A and type B. The extended “M” is used for the Mifare® contactless interface protocol and related memory management (classic 1k emulation), whereas the “S” nominates the derivates with the ISO 18092 passive mode. The TOE will be identified by SLE66CL180PEx if we speak of the three derivates SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12 with an EEPROM of 18 kBytes. The same applies for SLE66CL81PEx (stand for the two derivates SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12 with an EEPROM of 8 kBytes) and the SLE66CL80PEx (stand for the three derivates SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12 with an EEPROM of 8 kBytes). The SLE66CL41PE / m1583-e12 has only one derivate with an EEPROM of 4kByte.

All nine products are identically from hardware perspective and produced with the same masks with the exception of the first metal mask (called M1 mask) which contains the derivate specific information (e. g. development code, design step, memory size).

The hardware part of the TOE is the complete chip, composed of:

- Microcontroller type ECO 2000 (CPU) with the subcomponents memory encryption and decryption unit (MED), memory management unit (MMU) and 256 bytes of internal RAM (IRAM),

- External memory comprising 2 kBytes extended RAM (XRAM), 128 Bits PROM, 1728 Bits Map-RAM, 92 kBytes user ROM including the routines for chip management (RMS) (the derivates SLE66CL180PEM, SLE66CL81PEM and SLE66CL80PEM have 88 kBytes), 16 kBytes test ROM containing the test routines (STS) (the derivates SLE66CL180PEM, SLE66CL81PEM and SLE66CL80PEM have 20 kBytes), and a total of 18 kBytes non-volatile memory (EEPROM) for the derivates SLE66CLX180PEx with error detection (EDC) and error correction (ECC), a total of 8 kBytes non-volatile memory (EEPROM) for the derivates SLE66CL81PEx and SLE66CL80PEx with error detection (EDC) and error correction (ECC), a total of 4 kBytes non-volatile memory (EEPROM) for the derivate SLE66CL41PE with error detection (EDC) and error correction (ECC),
- Security logic (SEC), Memory Control Unit (MCU) with FCURSE distributes the data to and from memory components while the FCURSE provides camouflage access operation, true random number generator (RNG), Checksum module (CRC), Interrupt module (INT), Input Logic (INP), Timer (TIM), Dual Key DES (Data encryption according to single-DES and 3DES standard, single DES is out of scope of the evaluation) and Cryptographic Unit (DDC),
- The RF interface (radio frequency power and signal interface) enables contactless communication between a Proximity Integrated Chip Card (PICC) and a reader/writer Proximity Coupling Device (PCD). The power supply and data are received by an antenna which consists of a coil with a few turns directly connected to the IC,
- Address and data bus (ADBUS), SFR bus (SBUS), Memory bus (MBUS),
- Extended configuration (CFG_EXT), extended SFR registers for general purposes and chip configuration.

The firmware part of the TOE consists of the RMS (Resource Management System) routines stored in a reserved area of the normal user ROM for EEPROM programming, security function testing, random number online testing and Mifare protocol (only the derivates SLE66CL180PEM and SLE66CL80PEM) and consists of STS (Self Test Software) stored in the especially protected test ROM consisting of test and initialization routines. The RMS is part of the IC Dedicated Support Software and the STS is part of the IC Dedicated Test Software as defined in Protection Profile [9].

The smart card operating system and the application stored in the User ROM and in the EEPROM are not part of the TOE.

The TOE provides an ideal platform for applications requiring non-volatile data storage. The TOE is intended for use in a range of high security applications, including high speed security authentication, data encryption or electronic signature. 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 is written using the Smart card IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001 [9]. 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 as wafers or phase 4 as modules.

The assumptions, threats and objectives defined in this Protection Profile [9] are used. To address additional security features of the TOE (e.g cryptographic services), the security environment as outlined in the PP [9] is augmented by an additional policy, an assumption and security objectives accordingly.

The IT products the Infineon Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12, SLE66CL41PE / m1583-e12 with specific IC Dedicated Software were evaluated by TÜV Informationstechnik GmbH. The evaluation was completed on 20. July 2007. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Infineon Technologies AG
Am Campeon 1-12
D-85579 Neubiberg, Germany

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 EAL5+ (Evaluation Assurance Level 5 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL5	TOE evaluation: Semiformally designed and tested
+: ALC_DVS.2	Life cycle support – Sufficiency of security measures
+: AVA_MSU.3	Vulnerability assessment - Analysis and testing for insecure states
+: AVA_VLA.4	Vulnerability assessment - Highly resistant

Table 1: Assurance components and EAL-augmentation

[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	Identifier	Source from PP or added in ST
FCS	**Cryptographic support**	
FCS_COP.1	Cryptographic operation	ST
FDP	**User data protection**	
FDP_ACC.1	Subset access control	ST
FDP_ACF.1	Security attribute based access control	ST
FDP_IFC.1	Subset information flow control	PP
FDP_ITT.1	Basic internal transfer protection	PP
FDP_SDI.1	Stored data integrity monitoring	ST
FDP_SDI.2	Stored data integrity monitoring and action	ST
FMT	**Security Management**	
FMT_MSA.1	Management of security attributes	ST
FMT_MSA.3	Static attribute initialisation	ST
FMT_SMF.1	Specification of management functions	ST
FPT	**Protection of the TOE Security Functions**	
FPT_FLS.1	Failure with preservation of secure state	PP
FPT_ITT.1	Basic internal TSF data transfer protection	PP
FPT_PHP.3	Resistance to physical attack	PP
FPT_SEP.1	TSF domain separation	PP
FRU	**Resource utilisation**	
FRU_FLT.2	Limited fault tolerance	PP

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Identifier	Source from PP or added in ST
FAU	**Security Audit**	
FAU_SAS.1	Audit storage	PP / ST[9]

[9] PP/ST: component is described in the PP but operations are performed in the ST.

Security Functional Requirement	Identifier	Source from PP or added in ST
FCS	**Cryptographic support**	
FCS_RND.1	Quality metric for random numbers	PP / ST
FMT	**Security management**	
FMT_LIM.1	Limited capabilities	PP
FMT_LIM.2	Limited availability	PP
FPT	**Protection of the TOE Security Functions**	
FPT_TST.2	Subset TOE testing	ST

Table 3: SFRs CC part 2 extended

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target [6], chapter 5.1 and 7.2.

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

TOE Security Functions	Description
SF1	Operating state checking
SF2	Phase management with test mode lock-out
SF3	Protection against snooping
SF4	Data encryption and data disguising
SF5	Random number generation
SF6	TSF self test
SF7	Notification of physical attack
SF8	Memory Management Unit (MMU)
SF9	Cryptographic support

Table 4: TOE Security Functions

SF1: Operating state checking

Correct function of the TOE is only given in the specified range. To prevent an attack exploiting that circumstance, it is necessary to detect if the specified range is left.

All operating signals are filtered to prevent malfunction and the operating state is monitored with sensors for the operating voltage, clock signal, frequency, temperature and electromagnetic radiation including light. This function includes also mechanisms to detect and correct specific EEPROM memory errors. In order to prevent accidental bit faults during production in the ROM, over the data stored in ROM a CRC-Checksum is calculated.

SF2: Phase management with test mode lock-out

During start-up of the TOE the decision for the user mode or the test mode is taken dependent on several phase identifiers. In addition a chip identification mode exists which is active in all phases. If test mode is the active phase, the TOE requests authentication before any action (test mode lock-out). If the chip identification mode is requested the chip identification data stored in a non modifiable EEPROM area is reported.

The phase management is used to provide the separation between the security enforcing functions and the user software. The TOE is set to user mode before TOE delivery.

SF3: Protection against snooping

Several mechanisms, like topological design measures for disguise, protect the TOE against snooping the design or the user data during operation and even it is out of operation (power down).

SF4: Data encryption and data disguising

The memory contents of the TOE are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. In addition the data transferred over the bus to and from the special SFRs (CRC, RNG, DDES) is encrypted automatically with a dynamic key change. Important parts of the CPU and the complete DES component are especially designed to counter leakage attacks like DPA or EMA.

SF5: Random number generation

Random data is essential for cryptography as well as for physical security mechanisms. The TOE is equipped with a true random generator based on physical probabilistic controlled effects. The random data can be used from the user software as well as from the security enforcing functions.

SF6: TSF self test

As part of the TSF, a hardware controlled self-test can be started from the user software or can be started directly to test SF1, SF5 and SF7. Any attempt to modify the sensor devices will be detected from the test.

SF7: Notification of physical attack

The entire surface of the TOE is protected with the active shield. Attacks over the surface are detected when the shield lines are cut or get contacted.

SF8: Memory Management Unit (MMU)

The MMU in the TOE gives the user software the possibility to define different access rights for memory areas and components. In case of an access violation the MMU will generate a non maskable interrupt (NMI). Then an interrupt service routine can react on the access violation. The policy of setting up the MMU and specifying the memory ranges is defined by the user software.

If the TOE supports the Mifare® protocol, a special area of the EEPROM is reserved and can only be accessed by the Mifare® Operating System.

SF9: Cryptographic Support

Cryptographic operations are provided by the TOE. The TOE is equipped with a hardware accelerator to support the standard cryptographic operations. The DES is supported completely in hardware.

As the final transition from test mode to user mode is performed before TOE delivery, all TOE Security Functions are applicable from TOE delivery at the end of phase 3 or 4 (depending on when TOE delivery takes place in a specific case) to phase 7.

For more details please refer to the Security Target [6], 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 [6], 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 [6] 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 [6] 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-encryption and -decryption 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 *test mode*. 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) or at the end of IC Packaging (Phase 4). At this point in time the operating system including the RMS routines for the SLE66CLxxxPEM derivatives which support the Mifare® protocol is already stored in the non-volatile memories of the chip and the *test mode* is disabled.

The SLE66CL180PEx, the SLE66CL81PEx, the SLE66CL80PEx and the SLE66CL41PE are identically from hardware perspective and produced with the same masks with the exception of the first metal mask which contains the derivate specific information. The difference is that in the SLE66CL81PEx, the SLE66CL80PEx and the SLE66CL41PE the memory is blocked to smaller size. This configuration is done before TOE delivery.

Thus, there are no special procedures for generation or installation that are important for a secure use of the TOE. The further production and delivery processes, like the Smart Card Finishing Process, Personalisation and the delivery of the smart card to an end user, 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 smart card operating system and the smart card application software 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).

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:

Infineon Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12, SLE66CL41PE / m1583-e12 with specific IC Dedicated Software

The following tables outline the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	SLE66CL180PE Smart Card IC	GDS-file-ID: m1585-e12 with production line indicator: “5” (Altis)		Wafer or packaged module
		SLE66CL180PEM Smart Card IC	GDS-file-ID: m1584-e12 with production line indicator: “5” (Altis)		Wafer or packaged module
		SLE66CL180PES Smart Card IC	GDS-file-ID: m1586-e12 with production line indicator: “5” (Altis)		Wafer or packaged module
		SLE66CL81PE Smart Card IC	GDS-file-ID: m1594-e12 with production line indicator: “5” (Altis)		Wafer or packaged module
		SLE66CL81PEM Smart Card IC	GDS-file-ID: m1595-e12 with production line indicator: “5” (Altis)		Wafer or packaged module
		SLE66CL80PE Smart Card IC	GDS-file-ID: m1591-e12 with production line indicator: “5” (Altis)		Wafer or packaged module
		SLE66CL80PEM Smart Card IC	GDS-file-ID: m1592-e12 with production line indicator: “5” (Altis)		Wafer or packaged module
		SLE66CL80PES Smart Card IC	GDS-file-ID: m1593-e12 with production line indicator: “5” (Altis)		Wafer or packaged module
		SLE66CL41PE Smart Card IC	GDS-file-ID: m1583-e12 with production line indicator: “5” (Altis)		Wafer or packaged module

No	Type	Identifier	Release	Date	Form of Delivery
2	FW	STS Self Test Software *(the IC Dedicated Test Software)*	V57.08.07		Stored in Test ROM on the IC
3	FW	RMS-E Resource Management System *(the IC Dedicated Support Software)*	RMS_E V06		Stored in reserved area of User ROM on the IC

Table 5: Delivered hardware and software of the TOE

No	Type	Identifier	Release	Date	Form of Delivery
4	DOC	Data Book - SLE66CL(X)xxxPE(M/S) Security Controller Family incl. the errata & delta Sheet [36]	10.06	October 2006	Hardcopy and pdf-file
5	DOC	Errarta & delta Sheet - SLE66CL(X)xxxPE(M/S) Controllers- Products and Boundout [37]	03.07	March 2007	Hardcopy and pdf-file
6	DOC	Security Programmers' Manual - SLE66C(L)xxxP(E) Controllers [33]	12.06	December 2006	Hardcopy and pdf-file
7	DOC	Security & Chip Card ICs – SLE66CxxxPE – Instruction Set [34]	07.04	July 2004	Hardcopy and pdf-file
8	DOC	Chip Card & Security ICs -SLE66CL(X)xxxPE(M/S) – Instruction Set and Special Function Registers – Quick Reference [35]	11.06	November 2006	Hardcopy and pdf-file
9	DOC	Application Notes [10] – [32]	See chapter 14 below		Hardcopy and pdf-file

Table 6: Delivered documents of the TOE

The hardware part of the TOE is identified by SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12 and SLE66CL41PE / m1583-e12. For identification of a specific chip, the Chip Identification Number stored in the EEPROM can be used (see [36], chapter 7.9).

The chip type byte identifies the different versions in the following manner:

- B3 hex for version m1585e1(x),
- B4 hex for version m1584e1(x),
- B5 hex for version m1586e1(x),
- B1 hex for version m1594e1(x),
- B2 hex for version m1595e1(x),
- A7 hex for version m1591e1(x),
- A3 hex for version m1592e1(x),
- B0 hex for version m1593e1(x),
- AF hex for version m1583e1(x).

Using the additional detailed production parameter bytes, one can reconstruct the last character (x) of the version number of a specific chip via a database system at Infineon Logistic Department.

The first nibble of the batch number (see [36], chapter 7) gives the production line indicator which is "5" for both chip versions manufactured in Infineons IC fabrication in Corbeil Essonnes (Altis), France.

The STS is identified by its unique version number which is stored in three additional control bytes of the Chip Identification Number.

The delivery process from the TOE Manufacturer to the Card Manufacturer (to Phase 4 or Phase 5 of the life cycle) guarantees, that the customer is aware of the exact versions of the different parts of the TOE as outlined above.

The delivery of the TOE to the customer (card manufacturer) is done in the following ways:

1. The customer picks up the TOE directly in Großostheim (DC-E), Singapore (DC-A), Wuxi (DC-C), Tokyo (DC-J) or Hayward (DC-U),
2. The production sites send the TOE to one of the distribution centers Großostheim (DC-E), Singapore (DC-A), Wuxi (DC-C), Tokyo (DC-J) and Hayward (DC-U). The distribution centers send the TOE to the customer.

TOE documentation is delivered either as hardcopy or as softcopy (encrypted) according to defined mailing procedures.

Defined procedures at the development and production sites guarantee that the right versions of the RMS and STS are implemented into a specific ROM mask for a TOE IC.

3 Security Policy

The Security Policy of the TOE is to provide basic Security Functions to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a random number 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 cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE shall

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

4 Assumptions and Clarification of Scope

The smart card operating system and the application software stored in the User ROM and in the EEPROM are not part of the TOE. 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 TOE is delivered as a hardware unit at the end of the chip manufacturing process (phase 3 of the life cycle defined) or at the end of the IC packaging into modules (phase 4 of the life cycle defined). At these specific points in time the operating system software is already stored in the non-volatile memories of the chip and the test mode is completely disabled.

The smart card applications need the Security Functions of the smart card operating system based on the security features of the TOE. With respect to security the composition of this TOE, the operating system, and the smart card application is important. Within this composition the security functionality is only partly provided by the TOE and causes dependencies between the TOE Security Functions and the functions provided by the operating system or the smart card application on top. These dependencies are expressed by environmental and secure usage assumptions as outlined in the user documentation.

Within this evaluation of the TOE several aspects were specifically considered to support a composite evaluation of the TOE together with an embedded smart card application software (i.e. smart card operating system and application). This was necessary as Infineon Technologies AG 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 Altis, labelled by the production line indicator „5“.

5 Architectural Information

The Infineon Smart Card IC (Security Controller) by SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12 and SLE66CL41PE / m1583-e12 with the specific 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. The complete hardware description and the complete instruction set of the TOE is to be found in the Data Book [36] and other guidance documents delivered to the customer, see table 6.

For the implementation of the TOE Security Functions basically the components processing unit (CPU) with memory management unit (MMU), RAM, ROM, EEPROM, security logic, interrupt module, bus system, Random Number Generator (RNG) and the two modules for cryptographic operations of the chip are used. Security measures for physical protection are realised within the layout of the whole circuitry.

The Special Function Registers, the CPU instructions and the various on-chip memories provide the interface to the software using the Security Functions of the TOE.

The TOE IC Dedicated Test Software (STS), 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 (RMS), stored on the chip, is used for EEPROM programming and Security Function testing. It is stored by the TOE manufacturer in a reserved area of the normal user ROM and can be used by the users embedded software.

6 Documentation

The documentations [10] – [35] are 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 operating system and/or application software which will use the TOE as hardware computing platform to implement the software (operating system / application software) which will use the TOE.

7 IT Product Testing

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

(i) Simulation tests: These tests are performed before starting the production to develop the technology for the production and to define the process parameters.

(ii) Qualification tests: These tests are performed after the first production of chips with a new mask. The tests are performed in test mode.

(iii) Verification tests: These tests are performed in user mode and check the functionality in the end user environment. The results of the qualification and verification tests are the basis on which it is decided, whether the TOE is released to production.

(iv) Security evaluation tests: These tests are performed in user mode and check the security mechanisms aiming on the security functionality and the effectivness of the mechanisms. The random numbers are tested as required by AIS 31 and fulfil the criteria.

(v) Production tests: These tests are performed at each TOE before delivery. The test program stored in the test ROM is carried out for every chip. The aim of the production tests is to check whether each chip is functioning correctly.

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 Altis (see part D, annex A of this report) were used for tests.

The evaluators testing effort can be summarised into the following classes of tests: Module tests, Simulation tests, Emulation tests, Tests in user mode, Tests in test mode and Hardware tests. The evaluators performed independent tests to supplement, augment and to verify the tests performed by the developer by sampling. Besides repeating exactly the developers tests, test parameters were varied and additional analysis was done. With these kind of tests performed in the developer's testing environment the entire security functionality of the TOE was verified. Overall the evaluators have tested the TSF systematically against the functional specification, the high-level design and the low-level design.

The evaluators supplied evidence that the actual version of the TOE with production line indicator "5" (Altis) provides the Security Functions as specified.

For this re-evaluation the evaluators re-assessed the penetration testing and confirmed the results from the previous certification procedure BSI-DSZ-CC-0399-2007 where they took all Security Functions into consideration. 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 Infineon Smart Card IC (Security Controller) by SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12 and SLE66CL41PE / m1583-e12 with the specific IC Dedicated Software and with production line indicator “5” (Altis). After delivery the TOE only features one fixed configuration (user mode), which cannot be altered by the user. The TOE was tested in this configuration. All the evaluation and certification results therefore are only effective for this version of the TOE. For all evaluation activities performed in test mode, there was a rationale why the results are valid for the user mode, too.

Every information of how to use the TOE and its Security Functions by the software is provided within the user documentation.

9 Results of the Evaluation

9.1 Evaluation of the TOE

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4], AIS 34). For smart card IC specific methodology the CC supporting documents

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards

(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 EAL5 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		Verdict
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Development tools CM coverage	ACM_SCP.3	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.3	PASS
Semiformal high-level design	ADV_HLD.3	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Modularity	ADV_INT.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Semiformal correspondence demonstration	ADV_RCR.2	PASS
Formal TOE Security Policy model	ADV_SPM.3	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.2	PASS
Compliance with implementation standards	ALC_TAT.2	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: low-level design	ATE_DPT.2	PASS
Functional testing	ATE_FUN.1	PASS

Assurance classes and components		**Verdict**
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Covert channel analysis	AVA_CCA.1	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, EAL5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function:
  SF 2 (Phase management with test mode lock-out),
  SF 3 (Protection against snooping),
  SF 4 (Data encryption and data disguising) and
  SF 5 (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 SF9 which is the Triple DES encryption and decryption by the hardware co-processor 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 Altis, labelled by the production line indicator „5“ within the chip identification number in the EEPROM, and the firmware and software versions as indicated in table 5 and the documentation listed in table 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 [8] 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 the Smartcard Embedded Software Developer and the Card Manufacturer. The actual end user obtains the TOE from the Card Manufacturer 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 application notes.

- All security hints described in [33], [36] and the delivered application notes [10] – [32] have to be considered.
- Especially the recommendation in [33], chapter 4 should be followed.

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 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.

  The Smartcard Embedded Software Developer should not accept deliverables from Infineon he had not requested. All confidential information sent in electronic form has to be accepted only in encrypted form.

- Requirement resulting from AGD_ADM and AGD_USR:
  In the environment the following assumption has to be fulfilled:

  - "Protection during packaging, finishing and personalisation" resulting from A.Process-Card (It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery are assumed to be protected appropriately).
  - In addition the development environment of the operating system developer has to be protected adequately, in order to be able to guarantee the security of the TOE on the whole.

- Requirement resulting from AGD_ADM and AGD_USR:
  The following requirements of the environment defined in [6] has to be taken into consideration from the Smartcard Embedded Software Developer:

  - "Cryptographic key generation" resulting from FCS_CKM.1 (for 3DES), or "Import of user data without security attributes" resulting from FDP_ITC.1 (for 3DES), or "Import of user data with security attributes" resulting from FDP_ITC.2 (for 3DES),
  - "Cryptographic key destruction" resulting from FCS_CKM.4 (for 3DES), and
  - "Secure security attributes" resulting from FMT_MSA.2 (for 3DES).
  - RE.Phase-1: Design and Implementation of the Smartcard Embedded Software
  - RE.Process-Card: Protection during Packaging, Finishing and Personalisation
  - RE.Cipher: Cipher Schemas

- Requirement resulting from AVA_MSU:
  During development of the Smartcard Embedded Software the correct configuration of the following parameters has to be checked:

- Wait states functionality is activated for all operations of the Embedded Software critical for side channel attacks (e.g. SPA/DPA),
- FCURSE functionality is activated for all operations of the Embedded Software critical for side channel attacks (e.g. SPA/DPA),
- parameters for memory encryption E0ADR, E2ADR and E2ENC (XKEY) which configure the ranges of encryption,
- if the SW comparison of random numbers to/with regard to the active shielding is correctly implemented [28],
- MMU is configured correct,
- calls of the self test of the TSF implemented in the RMS routines to detect failures of the sensors are implemented. Depending on the application (e.g. time between possible resets) the developer of the Smartcard Embedded Software has to decide how often this function has to be executed during normal operation. The self test shall be executed at least once during security relevant operation (e.g. key generation).
- call of the test of the random number generation to detect failures of the RNG is implemented.
- Application of the security advices given in [36], chapter 19.9, [33], and [27].

- Recomendation resulting from AVA_VLA [33,chapter 4]

11 Annexes

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

12 Security Target

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

13 Definitions

13.1 Acronyms

3DES Symmetric block cipher algorithm based on the DES

API Application Programming Interface

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
ECB	Electrical Code Block
EEPROM	Electrically Erasable Programmable Read Only Memory
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
RSA	Rivest, Shamir, Adelmann – a public key encryption algorithm
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
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

13.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005

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

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

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

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

[6] Security Target, Infineon Technologies AG, Security and Chipcard ICs, SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12 and SLE66CL41PE / m1583-e12, 20. February 2007, Version 1.2, (confidential document)

[7] Evaluation Technical Report, Version 3, 13. July 2007, for the Product Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12 and SLE66CL41PE / m1583-e12, (confidential document)

[8] ETR-lite for composition, according to AIS 36, Version 3, 13. July 2007, for the Product Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12 and SLE66CL41PE / m1583-e12 (confidential document)

[9] Smart card 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] SLE66CLxxxP - Anticollision Type A, Version 03.03, March 2003, Infineon Technologies AG

[11] SLE66CLxxxP - Anticollision Type B, Version 03.03, March 2003 Infineon Technologies AG

[12] SLE66CLxxxP - Card Coil Design Guide, Version 10.05, October 2005, Infineon Technologies AG

[13] SLE66CLXxxxPE – Implementation of Transmission Protocol according to ISO/IEC 14443 Part 3 and 4, Version 02.06, February 2006, Infineon Technologies AG

[14] SLE66CLxxxP - Implementation of Transmission Protocol according to ISO/IEC 14443 Part 4, Version 03.03, March 2003, Infineon Technologies AG

[15] Application Note, SLE66CXxxS Using CRC (PDF+SW), Version 03.01, March 2001, Infineon Technologies AG

[16] Application Note, SLE66CXxxP, Infineon Chipcard Crypto API (PDF+SW), Version 05.02, May 2002, Infineon Technologies AG

[17] Application Note, SLE66CxxxP, DDES - EC2 confidential, Version 02.04, February 2004, Infineon Technologies AG

[18] Complementary Application Note SLE66CxxxPE, DDES – EC2 confidential, Version 07.05, July 2005, Infineon Technologies AG

[19] Application Note, SLE66CxxxPE, Using MicroSlim NVM (cLib), confidential, Version 05.05, May 2005, Infineon Technologies AG

[20] Application Note, SLE66CxxxP/PE, Memory Encryption Decryption confidential, Version 11.04, November 2004, Infineon Technologies AG

[21] Application Note, SLE66CxxxPE, MMU-Memory Management Unit (PDF+SW) confidential, Version 12.04, December 2004, Infineon Technologies AG

[22] Application Note, SLE66CxxxP, MMU Security Issues (PDF) confidential, Version 01.02, January 2002, Infineon Technologies AG

[23] SLE66CLxxxP - Optimized Contactless Energy performance, Version 01.07, January 2007, Infineon Technologies AG

[24] SLE66C(L)xxxPE - Optimized Usage of Data NVM Above 64k, Version 08.05, August 2005, Infineon Technologies AG

[25] Application Note, SLE66CxxxP/PE, Testing the RNG, confidential, Version 11.04, November 2004, Infineon Technologies AG

[26] Application Note, SLE66CxxxP/PE, Using RNG a.t. FIPS140 (PDF+SW), confidential, Version 02.04, February 2004, Infineon Technologies AG

[27] Application Note, SLE66CxxxPE, Security Advice 05.04 (PDF+SW) confidential, Version 05.04, May 2004, Infineon Technologies AG

[28] Application Note, SLE66CxxxPE, Using the active shield, confidential, Version 12.04, December 2004 Infineon Technologies AG

[29] Application Note, DES – software version (PDF+SW), confidential, Version 09.97, September 1997, Infineon Technologies AG

[30] Application Note, SLE66CxxxP, UART (PDF+SW), confidential, Version 10.03, October 2003, Infineon Technologies AG

[31] Application Note, SLE66CxxxPE - UART basic (PDF), Version 02.07, February 2007

[32] Application Note, SLE66CxxxPE - UART static (PDF), Version 01.07, January 2007

[33] Security Programmers' Manual - SLE66C(L)xxxP(E) Controllers, Version 12.06, December 2006

[34] Security & Chip Card ICs – SLE66CxxxPE – Instruction Set, Version 07.04, July 2004, Infineon Technologies AG

[35] Chip Card & Security ICs - SLE66CL(X)xxxPE(M/S) – Instruction Set and Special Function Registers – Quick Reference, Version 11.06, November 2006, Infineon Technologies AG

[36] Data Book – SLE66CL(X)xxxPE(M/S) Security Controller, Version 10.06, 31 October 2006, Infineon Technologies AG

[37] Errarta & delta Sheet – SLE66CL(X)xxxPE(M/S) Controllers – Products and Boundout, Version 03.07, March 2007, Infineon Technologies AG

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

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

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

plus one of the following:

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

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

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

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

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

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

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

CC Part 3:

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0431-2007

Evaluation results regarding development and production environment

The IT product Infineon Smart Card IC (Security Controller) SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12, SLE66CL41PE / m1583-e12 with specific IC Dedicated Software (Target of Evaluation, TOE) has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, version 2.3 (ISO/IEC 15408:2005), extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, version 2.3 (ISO/IEC15408: 2005).

As a result of the TOE certification, dated 08. August 2007, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

- **ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.3),**
- **ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and**
- **ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.2, ALC_TAT.2),**

are fulfilled for the development and production sites of the TOE listed below:

a) **Infineon Technologies AG, Secure Mobile Solutions, Alter Postweg 101, 86159 Augsburg, Germany (Development)**

b) **Altis Semiconductor S.N.C., Boulevard John Kennedy 224, 91105 Corbeil Essonnes, France (Production)**

c) **Altis Toppan (former DuPont), Toppan Photomask, Inc, European Technology Center, Boulevard John Kennedy 224, 91105 Corbeil-Essonnes Cedex, France (Mask Center)**

d) **Amkor Technology Philippines, Km. 22 East Service Rd., South Superhighway, Muntinlupa City 1702, Philipines, and Amkor Technology Philippines, 119 North Science Avenue, Laguna Technopark, Binan, Laguna 4024, Philipines (Module Mounting)**

e) **Infineon Technologies Austria AG, Development Center Graz, Babenbergerstr. 10, 8020 Graz, Austria, and Infineon Technologies Austria AG, Siemensstr. 2, 9500 Villach, Austria (Development)**

f) **Infineon Technologies Dresden GmbH & Co. OHG, Königsbrücker Str. 180, 01099 Dresden, Germany (Production)**

g) **Toppan Photomask Inc., Rähnitzer Allee 9, 01109 Dresden, Germany (Mask Center)**

h) **Assa Abloy Identification Technologies GmbH (former Sokymat GmbH), In den Weiden 4b, 99099 Erfurt, Germany (Antenna inlay mounting)**

i) **Kuehne & Nagel, 30805 Santana Street, Hayward, CA 94544 U.S.A. (Distribution Center)**

j) **Infineon Technologies AG, Am Campeon 1-12, 85579 Neubiberg, and Infineon Technologies AG, Otto-Hahn-Ring 6, 81739 München (Perlach), Germany (Development)**

k) **Infineon Technologies AG, Leibnizstrasse 6, 93055 Regensburg (Burgweinting), Germany (Module Mounting (with inlay antenna mounting), warehouse)**

l) **Exel Singapore Pte Ltd, Exel Supply Chian Hub, 81, ALPS Avenue, Singapore (Distribution Center)**

m) **Kintetsu World Express, Inc., Tokyo Import Logistics Center, Narita Terminal, Tokyo, Japan (Distribution Center)**

n) **Infineon Technologies (Wuxi) Co. Ltd., No. 118, Xing Chuang San Lu, Wuxi-Singapore Industrial Park, Wuxi 214028, Jiangsu, P.R. China (Module Mounting, Delivery)**

The hardware part of the TOE produced in the semiconductor factory in Altis, France, is labelled by the production line indicator „5“.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target, BSI-DSZ-0431-2007, Version 1.2, 20. February 2007, Security and Chipcard ICs, SLE66CL180PE / m1585-e12, SLE66CL180PEM / m1584-e12, SLE66CL180PES / m1586-e12, SLE66CL81PE / m1594-e12, SLE66CL81PEM / m1595-e12, SLE66CL80PE / m1591-e12, SLE66CL80PEM / m1592-e12, SLE66CL80PES / m1593-e12 and SLE66CL41PE / m1583-e12, Infineon Technologies AG [6].

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