Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0395-2007

for

Infineon Smart Card IC (Security Controller)
SLE88CFX4001P/m8835b18
SLE88CFX4003P/m8837b18
SLE88CFX3521P/m8857b18
SLE88CFX2921P/m8859b18
each with PSL V2.00.07
and 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

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0395-2007

Infineon Smart Card IC (Security Controller)
SLE88CFX4001P/m8835b18
SLE88CFX4003P/m8837b18
SLE88CFX3521P/m8857b18
SLE88CFX2921P/m8859b18
each with PSL V2.00.07
and specific IC Dedicated Software

from

Infineon Technologies AG

Common Criteria Arrangement
for components up to EAL4

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

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0002-2001**
Functionality:	**BSI-PP-0002-2001 conformant plus product specific extensions** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **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, 27. April 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 7 July 1992, Bundesgesetzblatt I p. 1230

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

5 Proclamation of the Bundesministerium des Innern of 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_IMP.2, 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 product Infineon Smart Card IC (Security Controller) SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 each with PSL V2.00.07 and specific IC Dedicated Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0376-2006 and BSI-DSZ-CC-0269-2006. Specific results from the evaluation process based on BSI-DSZ-CC-0376-2006 and BSI-DSZ-CC-0269-2006 were re-used.

The evaluation of the product Infineon Smart Card IC (Security Controller) SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 each with PSL V2.00.07 and specific IC Dedicated Software was conducted by T-Systems GEI GmbH, Prüfstelle IT-Sicherheit. The T-Systems GEI GmbH, Prüfstelle IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is Infineon Technologies AG.

The certification is concluded with

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

This work was completed by the BSI on 26. April 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 D-1 to D-4.

The product Infineon Smart Card IC (Security Controller) SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 each with PSL V2.00.07 and 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 Technologies AG
Automotive, Industrial & Multimarket,
Chipcard & Security IC´s
Am Campeon 1-12
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 Target of Evaluation (TOE) is the Infineon Smart Card IC (Security Controller) Infineon Smart Card IC (Security Controller) SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18, SLE88CFX3521P/ m8857b18 and SLE88CFX2921P/m8859b18 each with PSL V2.00.07 and specific IC Dedicated Software providing a hardware platform for a smart card to run smart card applications executed by a smart card operating system.

The evaluation was performed as a re-evaluation process based on BSI-DSZ-CC-0269-2006 and BSI-DSZ-CC-0376-2006. The TOE was re-evaluated because of security relevant modifications in hardware and software. The Security Target was updated.

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

The TOE provides a platform for applications requiring non-volatile data storage. The TOE is intended for use in a range of high security applications, including information integrity, access control, mobile telephone, as well as uses in electronic funds transfer and healthcare systems.

The TOE is implemented in the 0,13 µm CMOS technology and manufactured in Infineons IC fabrication in Dresden, Germany, indicated by the production line indicator “2”.

The hardware part of the TOE is the complete chip, composed of a dedicated microprocessor (CPU) with a virtual memory system (VMS), several different memories, security logic, a timer and an interrupt-controlled I/O interface. A Random Number Generator (RNG) is integrated on the chip. The memory comprises RAM, User ROM and NVM (Non Volatile Memory). The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED). The access rights of the application to the memories can be controlled with the Virtual Memory System (VMS).

Four modules for cryptographic operations are implemented on the TOE: (i) The coprocessor Crypto@1408BIT is used for calculation of asymmetric algorithms like RSA, (ii) The Data Encryption Standard (DES) algorithm is computed by the DES module. (iii) The Advanced Encryption Standard (AES) and (iv) Secure Hash Algorithm (SHA-1) are included as software modules in the Platform Support Layer (PSL) software.

As IC Dedicated Software (refer to Protection Profile [8]), the firmware consists of two parts: The one is called Platform Support Layer (PSL). It provides a high level interface to the hardware devices like timers, UART (Universal Asynchronous Receiver Transmitter), Crypto@1408BIT, RNG, NVM, DES and to the cryptographic functions of AES, CRC (Cyclic Redundancy Check) and SHA-1. The PSL provides the user (operating system) with the functionality to load code and data to the memory areas of the TOE in a secured process. The PSL is stored in ROM and NVM of the TOE. As the PSL provides the TOE

security functions interface, the use of the PSL is required to access the security functionality of the TOE. The PSL can be used with a Software development kit (SDK) from Infineon. The SDK itself is not part of the TOE.

The other firmware part is the Self Test Software (STS) which controls the start-up of the chip. The STS configures all necessary parameters like keys for the MED. During the production test at the manufacturer Infineon Technologies AG the STS provides an interface to the test capabilities of the IC chip. The lock out of the test capabilities is also performed by the STS.

The Security Target is written using the Smartcard IC Platform Protection Profile, Version 1.0 (BSI-PP-0002-2001) [8]. With reference to this Protection Profile, the smart card product life cycle is described in 7 phases. The development, production and operational user environment are described and referenced to these phases.

TOE delivery of the IC is defined at the end of phase 3 as wafers or phase 4 as modules. The documentation is delivered from phase 2 to phase 1 in form of data carriers and/or paper documentation.

In addition Embedded Software development tools are delivered from phase 2 to phase 1. These tools are not part of the TOE.

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

The TOE of this Security Target encloses the SLE88CFX4001P and three additional chip derivates. The hardware and the IC Dedicated Software of the SLE88CFX4001P and the three derivates are identical. The differences between the derivates are the NVM and ROM size as shown in the following:

Name of Chip	NVM	ROM	User ROM
SLE88CFX4001P	400 kByte	80 kByte	0 kByte
SLE88CFX4003P	400 kByte	80 kByte	160 kByte
SLE88CFX3521P	352 kByte	80 kByte	0 kByte
SLE88CFX2921P	292 kByte	80 kByte	0 kByte

Table 1: Hardware configurations of the TOE

The firmware versions PSL V2.00.07 can be tailored to remove functionality, which the user decides not to use. The functionality of each version and the process to tailor a PSL version is described in the guidance documentation of the TOE.

The TOE can be delivered to the user with PSL already tailored according to the user choice for the derivate SLE88CFX4003P. This is done in Phase 1 of the life cycle. For the derivates SLE88CFX4001P, SLE88CFX3521P and SLE88CFX2921P the TOE can be tailored based on specific order of the user. This is done during the manufacturing process.

A tailored PSL delivered on the TOE to the user does not include a code implementing functionality, which the user decided not to use. This, for example could be the AES functionality, which is a part of Security Function 9 according to P.Add-Functions. A tailored PSL of the TOE could also for example exclude or deactivate the code implementing some non security enforcing functionality. Therefore this has no impact of any other security policy of the TOE.

The TOE was evaluated against the claims of the Security Target [6].

The development and production environment in terms of the concepts and procedures regarding the CC assurance aspects ACM, ADO and ALC according to the Scheme Interpretation AIS38 [4] were evaluated by the Prüfstelle für IT-Sicherheit of the TÜV Informationstechnik GmbH.

All product specific assurance aspects of the TOE (assurance classes ASE, ADV, AGD, ATE, AVA and the product specific aspects of ACM, ADO and ALC according to Scheme Interpretation AIS38 [4]) were evaluated by the T-Systems GEI GmbH, Prüfstelle IT-Sicherheit. The evaluation was completed on 13. März 2007.

T-Systems GEI GmbH, Prüfstelle IT-Sicherheit as well as the Prüfstelle für IT-Sicherheit of the TÜV Informationstechnik GmbH are evaluation facilities (ITSEF) recognised by BSI.

The sponsor, vendor and distributor is Infineon Technologies AG.

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 EAL 5+ (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 2: Assurance components and EAL-augmentation

1.2 Functionality

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

The following SFRs are taken from CC part 2:

Security Functional Requirement	Identifier	Source from PP or added in ST
FCS	**Cryptographic support**	
FCS_COP.1 [DES]	Cryptographic operation	ST
FCS_COP.1 [3DES]	Cryptographic operation	ST
FCS_COP.1 [RSA]	Cryptographic operation	ST
FCS_COP.1 [AES]	Cryptographic operation	ST
FCS_COP.1 [SHA-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
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 3: 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[8]
FCS	**Cryptographic support**	
FCS_RND.1	Quality metric for random numbers	PP / ST

[8] 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
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 4: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the Security Target [6], chapter 5.1.1 and 7.2.

The security objectives for the TOE environment are outlined only by Non-IT requirements for the TOE environment, i.e. for (i) Design and Implementation of the Smartcard Embedded Software, (ii) Protection during Packaging, Finishing and Personalisation and (iii) Cipher Schemes. For details refer to the Security Target [6], chapter 5.2.2.

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

TOE Security Function	Addressed issue
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	Virtual Memory System (VMS)
SF9	Cryptographic support
SF10	NVM Tearing Save Write

Table 5: TOE Security Functions

SF1: Operating state checking

Correct function of the TOE is only given in the specified range of the environmental operating parameters. 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 operation state is monitored with sensors for the operating voltage, clock signal, frequency, temperature and electromagnetic radiation (e.g. light). The

TOE falls into the defined secure state in case of a specified range violation. The defined secure state causes the chip internal reset process.

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 depending on several phase identifiers. If test mode is the active phase, the TOE requests authentication before any action (test mode lock-out).

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

In addition a chip identification mode exists which is active in all phases. If the chip identification mode is requested the chip identification data stored in a non modifiable NVM area is reported.

During the production phase (phase 3) or after the delivery to the customer (phase 5 or phase 6), the TOE provides the possibility to load a user specific encryption key and user code and data encrypted into the empty (erased) NVM area as specified by the associated control information of the flash loader mode of the loader filter. After finishing the load operation, the flash loader mode is automatically deactivated, so that no second load operation with the flash loader mode is possible.

During the operation of the TOE the PSL provides the possibility to load signed code and data in the NVM and RAM areas as specified by the associated control information of the patch loader mode of the loader filter. The public part of the used signing key is stored in the NVM. This function could be deactivated permanently by the user software.

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 even if it is out of operation (power down).

SF4: Data encryption and data disguising

The memory content of the TOE is encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. Only the key owner has the possibility to read out data. To prevent interpretation of leaked information, randomness is inserted in the information. This function is specifically designed to prevent Differential Power Analysis (DPA) during cryptographic calculations (see chapter 9 and 10 of this report).

SF5: Random number generation

Random data are essential for cryptography as well as for physical security mechanisms. The TOE is equipped with a true random generator based on physical probabilistic effects. The random data can be used

from the user software as well as from the security enforcing functions. The PSL provides tests as required by [4, AIS 31].

SF6: TSF self test

The TOE has a hardware controlled self-test which can be started from the user software or is started directly to test SF5, SF7 and specific parts of SF1. 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: Virtual Memory System (VMS)

The VMS in the TOE controls the address permissions of the so called privileged packages (memory areas) 1 and 2 and of the regular packages 3 to 15 and gives the software the possibility to define different access rights for the regular packages (memory areas) 16 to 255. The address permissions of the privileged package 0 are controlled by the hardware and the VMS. In case of an access violation the VMS will generate a trap. Then a trap service routine can react on the access violation.

The policy of setting up the VMS and specifying the memory ranges for the regular packages 16 to 255 is defined from the user software in the upper layers. The two lower layers are given to the Secure Layer (SL) and the PSL. The Operating system has the layer 2 and the Debug Package has the layer 3. The layer 4 to 15 are not used and reserved for future use.

SF9: Cryptographic Support

Specific cryptographic operations are provided by the TOE. The TOE is equipped with several hardware accelerators and software modules to support the standard cryptographic operation.

The components are a combination of software and hardware unit to support DES encryption, a combination of software and hardware unit to support RSA cryptography and software units to support the AES and the SHA-1. AES availability depends on the selected PSL configuration. Not including the code implementing the AES into the PSL has no impact of any other security policy of the TOE.

SF10: NVM Tearing Save Write

The hardware of the NVM together with the PSL supports the TOE with a function to copy one data block with a defined maximum number of bytes or/and one or a bunch with a maximum number of data blocks of any data size to different NVM locations, under the protection of a data security mechanism. The data security mechanism keeps a backup copy of either the old or the new contents of all addressed NVM pages before

they are overwritten. If the update of the data fails due to an unexpected card tearing, the old or the new contents of all target areas affected by the transaction is recovered at the next power-up.

The NVM tearing save write detects errors that happen during the NVM write operation and corrects the errors to provide the correct function of the TOE. If a correction is not possible the TOE is forced into a secure state.

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 [8] were derived from considering the end-usage phase (phase 7 of the life cycle as described in the Security Target) as follows:

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

These high-level security concerns are refined in the Protection Profile [8] and used by the Security Target [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.

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

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

The development and production environment starting with phase 2 up to TOE Delivery are covered by an organisational security policy outlining that the IC developer / manufacturer must apply the policy “Protection during TOE Development and Production (P.Process-TOE)” so that no information is unintentionally made available for the operational phase of the TOE. The Policy ensures confidentiality and integrity of the TOE and its related design information and data. Access to samples, tools and material must be restricted.

A specific additional security functionality for DES, Triple-DES, RSA and AES encryption and decryption as well as the hash algorithm SHA-1 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 test mode is disabled and the operating system software including the PSL IC dedicated SW part of the TOE is already stored in the non-volatile memories of the chip or the loader is configured to be able to load embedded software into the NVM after phase 4.

The derivates of the TOE as outlined in chapter 1 have identical hardware and IC Dedicated Software. The differences between the derivates are the NVM and ROM size. This hardware configuration is done before TOE delivery.

For SLE88CFX4003P the developer of the Embedded Software may tailor the PSL software to remove functionality, which the user decides not to use. The rules to be followed are described in the guidance documentation of the TOE. This is done in phase 1 of the life cycle. For the derivates SLE88CFX4001P, SLE88CFX3521P and SLE88CFX2921P tailoring can be done during the manufacturing process based on specific order of the user.

The TOE can be configured with activated or deactivated Supply Shutdown Mode (SSM). The configuration is done during the manufacturing process of the TOE according to the choice of the user.

Thus, there are no special procedures for generation or installation that are important for a secure use of the TOE after TOE delivery. 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 [8], 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)
SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18,
SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18
each with PSL V2.00.07 and specific IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	Infineon Smart Card ICs SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18, SLE88CFX3521P/m8857b18, SLE88CFX2921P/m8859b18 (Security Controller)	GDS-file-ID: m8830b18_20060310 with production line indicator: “2” (Dresden)		Wafer or packaged module
2	SW	STS Self Test Software *(the IC Dedicated Test Software)*	00.0F.0F.0F build 585 and TNVM code rev.09.08		Stored in Test ROM on the IC
3	SW	Platform Support Layer Software (PSL) *(the IC Dedicated Support Software)* *(optionally tailored by embedded software developer, [see 11])*	*V2.00.07*		precompiled binary files (.obj) integrated into ROM/NVM code by Infineon or via flash loader.
4	DOC	SLE88CFXxxxxP PSL & Security Reference Manual [11]	2006-11	November 2006	Hardcopy and pdf-file
5	DOC	SLE88 Family Microcontrollers Hardware Reference Manual [12]	2006-07	July 2006	Hardcopy and pdf-file
6	DOC	SLE88CFXxxx1P/3P Errata Sheet [13]	2006-11-16	November 16, 2006	Hardcopy and pdf-file

Table 6: Deliverables of the TOE

The tailored variants for PSL Version V2.00.07 as outlined in the Security Reference Manual [11] were part of the evaluation. The “mini-operating system”

used for embedded software development software has to be disabled by the user and is not a part of any of the evaluated configurations.

The parts of the PSL needed to tailor the TOEs variant of the PSL at the user's (i.e. application software developer) site are delivered to the user. These parts of the TOE are identified by a name of the data file and by a hash value. For filenames and corresponding hash values see Security Target [6], section 11 Appendix. The guidance documentation shows how to tailor the PSL to evaluated variants.

In case of delivery with SDK, the SDK itself is not a part of the TOE and beyond its delivery aspect.

The hardware of all derivates listed in table 6, no.1 is identical. The non-ISO Reset of the chip allows the user to get chip identification information. Bytes 4 to 5 are the chip type bytes as described in the SLE88CFXxxxxP PSL & Security Reference Manual [11], appendix A5. The chip type byte identifies the version of the TOE-ICs:

- for SLE88CFX4001P/m8835b18: offset byte 4: 50 hex; offset byte 5: 52 hex
- for SLE88CFX4003P/m8837b18: offset byte 4: 51 hex; offset byte 5: 52 hex
- for SLE88CFX3521P/m8857b18: offset byte 4: 52 hex; offset byte 5: 52 hex
- for SLE88CFX2921P/m8859b18: offset byte 4: 53 hex; offset byte 5: 52 hex

The first nibble of the offset byte 6 (batch number) gives the production line indicator which is „2" for all versions of the TOE, as the evaluated TOE is produced in Dresden.

The code m8830 visible on the chip surface indicates the chip series only.

The PSL-code is embedded into the ROM mask by Infineon or loaded into the NVM as part of the embedded software. It is identified by its unique version number. The Embedded Software has access to the PSL version number for a specific chip by using the PSL command getCompEntry, with parameter VAL_PSL_VERSION = "2.00.07.F4001".

The STS-code is embedded into the ROM mask by Infineon. It is identified by its unique version number. The STS version is stored in the last four bytes of the Chip Identification Number and is "00 0f 0f 0f" which corresponds to "585".

To support Embedded Software development and simulation on bond-out chips, a PSL object file is delivered to the Embedded Software developer. The Embedded Software developer should verify the PSL version.

The delivery process from Infineon to their customers (to phase 5 or phase 6 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 TOE can be delivered in form of complete modules, in form of plain wafers or in an IC case.

To ensure that the customer receives the evaluated version of the chip, either

- he has to personally pick up the TOE at the Infineon Warehouse in Regensburg (VKL-Rgb) or Wuxi to (see part D, annex A of this report) or

- the TOE is sent as a secured transport by specific haulage companies from the Infineon Warehouse in Regensburg (VKL-Rgb) or from Wuxi directly or via one of three distribution centers (DC E for Europe, DC A for Asia and DC U for the United States) to the customer. The sender informs the receiver that a delivery was started; after the delivery was received it has to be checked according to the consignment notes and the sender is to be informed immediately about result of the check.

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

The above mentioned additional PSL object file is delivered as softcopy (encrypted object file) to the Embedded Software developer according to defined mailing procedures.

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

3 Security Policy

The Security Policy of the TOE is defined 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 symmetric cryptographic block cipher algorithms (DES, Triple-DES, AES) to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a Random Number Generator. Additionally the TOE implements RSA cryptography and SHA-1 functionality[9] .

As the TOE is a hardware security platform, the Security Policy of the TOE is also defined to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during DES, Triple-DES and AES cryptographic functions performed by the TOE), protection against physical probing, malfunctions, 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 NVM are not part of the TOE. The code in the Test ROM

[9] The availability of RSA and AES functionality depends on the PSL configuration.

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 test mode is completely disabled.

During the operation of the TOE the PSL provides the possibility to load signed code and data in the NVM and RAM areas as specified by the associated control information (loader function). This function can be deactivated by the user software. (see chapter 10 of this report for secure usage)

In case the PSL software is configured without specific cryptographic functionality drivers, parts of SF9 Cryptographic Support (e.g. AES) are not available to the embedded software. Additional cryptographic functions included in the PSL but not described within SF9 is not part of the evaluated security functionality.

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 chapter 9 of this report.

The full evaluation results are applicable for chips from the semiconductor factory in Dresden, each labelled by the production line indicator „2“.

5 Architectural Information

The Infineon Smart Card IC (Security Controller) SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 each with PSL V2.00.07 and specific IC Dedicated Software is an integrated circuit (IC) providing a hardware and software platform (Platform Support Layer PSL) to a Smartcard Embedded Software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target [6]. The complete hardware description, the complete instruction set and the programmers interfaces to the

PSL of the Infineon SLE88CFX4001P smart card controller can be found in the guidance documentation [11] and [12]

For the implementation of the TOE Security Functions basically the components 32-bit proprietary CPU, (Triple-) DES Co-Processor, numeric coprocessor (ACE), Random Number Generator (RNG), Virtual Memory System, Security Sensors and Filters, Memory Encryption and software drivers within the Platform Support Layer software (PSL) are used. Security measures for physical protection are realized within the layout of the whole circuitry. Logical security measures are implemented in both the circuitry of the hardware and in the software of the PSL.

The API of the Platform Support Layer software (PSL) provide the user interface to all security functions of the TOE where they can be configured or used by the user (i.e. smartcard operating system and/or the smartcard embedded software).

The modular arithmetic functions provided by the PSL are designed to help the user to implement the RSA asymmetric cryptographic algorithm. AES and SHA-1 functionality is provided by PSL software.

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.

6 Documentation

The documentation [11] to [13] is provided with the product by the developer to the customer for secure usage of the TOE in accordance with the Security Target. Additional guidance as outlined in chapter 10 of this report has to be followed.

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.

To support a composite evaluation as defined in AIS 36 [4], the document ETR-lite [10] is provided for the composite evaluator.

7 IT Product Testing

The tests performed by the developer can be divided into following categories:

1) technology development tests as the earliest tests to check the technology against the specification and to get the technology parameters used in simulations of the circuitry (this testing is not strictly related to Security Functions);

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

3) regression tests which are performed for the IC Dedicated Test Software (PSL) and for the IC Dedicated Support Software (STS) on emulator versions of the TOE or within the simulation of chip in special hardware;

4) qualification tests to release the TOE to production:

   - used to determine the behaviour of the chip with respect to different operating conditions and varied process parameters (often also referred to as characterisation tests)

   - special verification tests for Security Functions which were done with samples of the TOE (referred also as developers security evaluation) and which include also layout tests by automatic means and optical control, in order to verify statements concerning the layout;

5) functional production tests, which are done for every chip to check its correct functionality as a last step of the production process (phase 3 or phase 4 depending on the TOE delivery form).

The developer tests cover all Security Functions and all security mechanisms as identified in the Functional Specification, and in the High and Low Level Designs.

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developers sites. They performed independent tests to supplement, augment and to verify the tests performed by the developer by sampling or by complete repetition of regression tests especially for the software. Besides repeating exactly the developers tests, test parameters and test equipment are varied and additional analysis was done. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

The evaluators supplied evidence that the actual versions of the TOE provides the Security Functions as specified by the developer. The test results confirm the correct implementation of the TOE Security Functions.

For penetration testing the evaluators took all Security Functions into consideration. Intensive penetration testing was planed based on the analysis results and performed for the underlying mechanisms of Security Functions using bespoke equipment and expert know how. The penetration tests considered both the physical tampering of the TOE and attacks which do not modify the TOE physically (i.e. DPA/SPA testing).

Several samples of the TOE were used for the evaluator’s tests in the evaluators laboratory and at the developer’s site. The samples used to perform the tests are provided by the wafer fab Dresden. Since the characterisation tests are an important part of the initial tests that are requested for the release of the production of a wafer fab the results are only valid for the fab Dresden (see part D, annex A of this report).

The test results are valid for all hardware derivates of the TOE containing the same software (PSL, STS and TNVM), as the only difference is the configured

(by software means) size of the available NVM to the user, the size of ROM made available to the user. These configuration options have no impact on evaluation test results.

Testing included different PSL configurations. The test results are valid for the PSL configurations as outlined in the guidance documentation (Security Reference Manual [11]).

8 Evaluated Configuration

The TOE is identified by the version Infineon Smart Card IC (Security Controller) SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 each with PSL V2.00.07 and specific IC Dedicated Software with production line indicator “2” (Dresden). The embedded software developer decides on configuration of the PSL software as described above. The TOE has only one fixed evaluated configuration at the time of delivery to phase 4 resp. 5.

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

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. Thus, the evaluation was mainly performed in the user mode. For all evaluation activities performed in test mode, there was a rationale why the results are valid for the user mode, too.

The evaluated derivate of the TOE is SLE88CFX4001P/b18 with PSL Version 2.00.07, STS Version 00.0F.0F.0F build 585 and TNVM software 09.08. For the evaluation of ADO_IGS the SDK 2.9 SP6 was used.

9 Results of the Evaluation

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 and

(iii) ETR-lite – for Composition and ETR-lite – for composition: Annex A Composite smartcard evaluation: Recommended best practice

(see [4, AIS 25, AIS 26 and AIS 36]) 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 evaluation results of the development and production environment in terms of the concepts and procedures regarding the CC assurance aspects ACM, ADO and ALC according to the Scheme Interpretation AIS38 [4] were provided by the ITSEF of TÜV Informationstechnik GmbH.

The verdicts for the CC, Part 3 assurance components (according to EAL 5 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

Assurance classes and components		Verdict
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
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

As changes to the TOE were in hardware as well as in software, all assurance aspects were reviewed in the couse of this re-evaluation.

The evaluation has shown that:

- the TOE is conform to the Smartcard IC Platform Protection Profile, BSI-PP-0002-2001 [8]
- 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) including resistance of the DES and AES against Differential Power Analysis (DPA), SF 5 (Random number generation) and SHA-1 of SF9 (Cryptographic support). Therefore the scheme interpretations AIS 26 and AIS31 (see [4]) were used.

SPA/DPA analysis for RSA-Functionality is not fully part of this certification (please refer to chapter 10 of this report).

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

a) DES and Triple-DES encryption and decryption and

b) RSA encryption and decryption

c) AES encryption and decryption -- 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 6, produced in the semiconductor factory in Dresden, labelled by the production line indicator „2“ within the chip identification number in the NVM, and the firmware and software versions as indicated in table 6 and the documentation listed in table 6, too.

The test results of light penetration attacks apply only to TOE which thickness is not below 180µm.

The evaluation results including also results of tests performed by the developer are valid for all hardware derivates of the TOE containing the same software (PSL, STS and TNVM), as the only differences are the configured (by software means) size of the available NVM to the user and the size of ROM made available to the user during mask manufacturing. All those configuration options have no impact on evaluation results.

The evaluation results hold for the TOE with disabled and enalbled SSM.

The evaluation results including also results of tests performed by the developer are valid for all tailoring options (see [11], section 5.2) for PSL variants on all derivates. This statement must be understood as follows. A PSL driver provides a tested functionality on its interfaces only when it is enabled and included. There are no security flaws related to disabling or not including PSL drivers. There is no difference in terms of the rating the overall security to the situation when the user decides not to use a specified PSL driver at all.

The evaluation results cannot be extended to further versions/derivates of the TOE and/or another production sites without any extra investigations.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

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 [10] 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 operational documents [11] - [13] contain necessary information about the usage of the TOE and all security hints therein have to be considered by the smart card Embedded Software developer.

In the following, specific items are listed:

The document [11] guides on tailoring of the PSL variant during development (by the user) of the application software and on removing the “mini-operating system” which is not a part of a certified configuration. Infineon will also provide the Security Target to customers. This includes the assumptions about the environment and usage of the TOE and the security functions provided by the TOE.

Besides the requirements to follow the instructions in the user guidance documents (especially section 4, [11] and the corresponding delta information in [13]) and to ensure fulfilment of the assumptions about the environment in the Security Target, the following items have to be followed:

1. The Virtual Memory System must be properly initialised and managed in order to fulfil the security policy defined by application developer. The security and the PSL layer maintain their own Security Policy. The application software (i.e. operating system) is responsible for using the virtual memory system with respect to this policy, i.e. not to change these protections by any means. It is further responsible for using only the VMS API from PSL in a manner that is sufficient to fulfil its own Security Policies. Note that the PSL driver ensures that the logical scrambling (through random mapping of virtual to physical address on memory allocation) is realised.

2. The user should check for the sufficient physical address randomisation of data areas (RAM, NVM) when the user decides to use the fixed mapping features offered by the development tools.

3. The user must also take care about DPA/SPA security when using the SHA-1 with secret key data (i.e. keyed hash) as the SHA-1 implementation is not claimed to be DPA/SPA resistant and therefore its respective resistance was not tested.

4. Requirements for Embedded Software development are addressed by the IC user guidance [11] to [13]. The concrete measures being applied by the developer of the Smartcard Embedded Software must be evaluated during the composite evaluation. In particular the effectiveness of DPA/SPA countermeasures in the usage of the SEF9, RSA (ModPow API) and ModInv API must be evaluated as the TOE implements by itself only basic functionality. Further detailed information on composite evaluation is provided according to AIS36 [4] in ETR-lite [10].

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 full Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SSM	Supply Shutdown Mode
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Bibliography

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

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

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

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

- AIS 25, Version 2, 29 July 2002 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 1.2, July 2002
- AIS 26, Version 2, 6 August 2002 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 1.1, July 2002
- AIS 31, Version 1, 25 Sept. 2001 for: Functionality classes and evaluation methodology of physical random number generators
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 36, Version 1, 29 July 2002 for: CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2 March 2002
- AIS 38, Version 1.1, 7 January 2004, Reuse of evaluation results

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

[6] Security Target BSI-DSZ-CC-0395, SLE88CFX4001P/m8835, Version 1.6, Infineon Technologies AG, 29 November 2006

[7] Evaluation Technical Report, BSI-DSZ-CC-0395, Product Infineon Smart Card IC SLE88CFX4001P/m8835, Version 1.41, 13 March 2006, T-Systems (confidential document)

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

[9] Infineon Technologies AG, Chip Card & Security ICs, Evaluation Documentation, SLE88CFX4001P/m8835 Configuration Management Scope (ACM_SCP), Version 1.5, Infineon Technologies AG, 13 March 2007 (i.e. TOE Configuration List, confidential document)

[10] ETR-lite for composition according to AIS 36 for the Product Infineon Smart Card IC SLE88CFX4001P/m8835, Version 1.40, T-Systems GEI GmbH, 12 December 2006 (confidential document)

[11] SLE88CFXxxxxP PSL & Security Reference Manual, Edition 2006-11, Infineon Technologies AG, November'06 (confidential document)

[12] SLE88 Family Microcontrollers Hardware Reference Manual, Edition 2006-07, Infineon Technologies AG, July'06 (confidential document)

[13] SLE88CFXxxx1P/3P Errata Sheet, Edition November 16, 2006, Infineon Technologies AG, 16.11.06 (confidential document)

This page is intentionally left blank.

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-0395-2007

Evaluation results regarding development and production environment

The IT product Infineon Smart Card IC (Security Controller) SLE88CFX4001P/m8835b18, SLE88CFX4003P/m8837b18, SLE88CFX3521P/ m8857b18 and SLE88CFX2921P/m8859b18 each with PSL V2.00.07 and 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 27. April 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 TechnologiesAG, Infineon Technologies AG, Am Campeon 1-12, 85579 Neubiberg, Germany (development center)

b) Infineon Technologies AG, Development Center Graz, Babenbergerstr. 10, A-8020 Graz, Austria (development center)

c) Infineon Technologies AG, Alter Postweg 101, D-86159 Augsburg (development center)

d) Infineon Technologies AG, Königsbrücker Str. 180, 01099 Dresden, Germany (semiconductor factory)

e) DuPont Photomasks Germany GmbH (DPI), Rähnitzer Allee 9, 01109 Dresden

f) Du Pont Photomasks France S.A., 224, bd John Kennedy, F-91105 Corbeil Essonnes, France (mask shop)

g) Infineon Technologies AG, Leibnizstraße 6, D-93055 Regensburg, Germany (IC packaging into modules, warehouse and delivery center)

h) Infineon Technologies Asian Pacific, Exel Singapure Pte. Ltd., 81 ALPS Avenue, Exel Supply Chain Hub, Singapore 498803 (warehouse and delivery center)

i) Infineon Technologies (Wuxi) Co. Ltd., No. 118, Xing Chuang San Lu, Wuxi-Singapore Industrial Park, Wuxi 214028, Jiangsu P.R. China (IC packaging into modules, warehouse and delivery center)

The hardware part of the TOE produced in the semiconductor factory in Dresden is labelled by the production line indicator „2“.

For all sites listed above, the requirements have been specifically applied for each site and in accordance with the Security Target BSI-DSZ-CC-0395, SLE88CFX4001P/m8835, Version 1.6, Infineon Technologies AG, 29 November 2006 [6]. The evaluators verified, that the threats are countered and the security objectives for the life cycle phases 2, 3 and 4 up to delivery at the end of phase 3 or 4 as stated in the TOE Security Target are fulfilled by the procedures of these sites.