Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0706-2011

for

Infineon Technologies AG Smartcard ICs SLE88CNFX6600PM/P, SLE88CNFX6602PM/P, SLE88CNFX5400PM/P, SLE88CNF6600PM/P, SLE88CNF6602PM/P, SLE88CNF5400PM/P, SLE88CFX6600P, SLE88CFX6602P, SLE88CFX5400P, SLE88CF6600P, SLE88CF6602P, SLE88CF5400P all with PSL 3.22.11

from

Infineon Technologies AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0706-2011

Infineon Technologies AG Smartcard ICs SLE88CNFX6600PM/P, SLE88CNFX6602PM/P, SLE88CNFX5400PM/P, SLE88CNF6600PM/P, SLE88CNF6602PM/P, SLE88CNF5400PM/P, SLE88CFX6600P, SLE88CFX6602P, SLE88CFX5400P, SLE88CF6600P, SLE88CF6602P, SLE88CF5400P all with PSL 3.22.11, Version: A13

from	Infineon Technologies AG
PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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.

Bonn, 29 June 2011

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski L.S.
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.1 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition 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 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 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, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3 and AVA_VAN.5 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 Technologies AG Smartcard ICs SLE88CNFX6600PM/P, SLE88CNFX6602PM/P, SLE88CNFX5400PM/P, SLE88CNF6600PM/P, SLE88CNF6602PM/P, SLE88CNF5400PM/P, SLE88CFX6600P, SLE88CFX6602P, SLE88CFX5400P, SLE88CF6600P, SLE88CF6602P, SLE88CF5400P all with PSL 3.22.11 has undergone the certification procedure at BSI.

The evaluation of the product Infineon Technologies AG Smartcard ICs SLE88CNFX6600PM/P, SLE88CNFX6602PM/P, SLE88CNFX5400PM/P,

SLE88CNF6600PM/P, SLE88CNF6602PM/P, SLE88CNF5400PM/P, SLE88CFX6600P, SLE88CFX6602P, SLE88CFX5400P, SLE88CF6600P, SLE88CF6602P, SLE88CF5400P all with PSL 3.22.11 was conducted by T-Systems GEI GmbH. The evaluation was completed on 20 June 2011. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Infineon Technologies AG.

The product was developed by: 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.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. 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 and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Infineon Technologies AG Smartcard ICs SLE88CNFX6600PM/P, SLE88CNFX6602PM/P, SLE88CNFX5400PM/P, SLE88CNF6600PM/P, SLE88CNF6602PM/P, SLE88CNF5400PM/P, SLE88CFX6600P, SLE88CFX6602P, SLE88CFX5400P, SLE88CF6600P, SLE88CF6602P, SLE88CF5400P all with PSL 3.22.11 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

[6] Information Technology Security Evaluation Facility

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Infineon Technologies AG
Am Campeon 1-12
85579 Neubiberg

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.

1 Executive Summary

The Target of Evaluation (TOE), the Infineon Technologies AG Smartcard ICs SLE88CNFX6600PM/P, SLE88CNFX6602PM/P, SLE88CNFX5400PM/P, SLE88CNF6600PM/P, SLE88CNF6602PM/P, SLE88CNF5400PM/P, SLE88CFX6600P, SLE88CFX6602P, SLE88CFX5400P, SLE88CF6600P, SLE88CF6602P, SLE88CF5400P all with PSL 3.22.11 (in the following named SLE88CNFX6600PM), is a smart card IC (Security Controller) with specific IC dedicated software, which is manufactured in a 0,13 µm CMOS technology. The IC is intended to be used in smart cards for particularly security-relevant applications. The term “User Software” is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the user software. The user software itself is not part of the TOE. The SLE88CNFX6600PM, whose block diagram is shown in Figure 2-1 of [6], consists 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, an interface management module, a Single Wire Protocol slave module (SWP) and two co-processors. The firmware, called platform support layer (PSL), provides a high level interface to the hardware devices like timers, UART (Universal Asynchronous Receiver Transmitter), Crypto@1408Bit, TRNG (Random Number Generator), NVM (Non Volatile Memory), DES (Data Encryption Standard) and to the cryptographic functions AES (Advanced Encryption Standard), MD5, CRC (Cyclic Redundancy Check) and SHA (Secure Hash Algorithm). The AES Encryption/Decryption, the MD5 Generator and the CRC Generator are not in the scope of the certification and not part of the security features of the TOE.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7.1 They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionalities:

TOE Security Functionality	Addressed issue
SF1	Operating state checking
SF2	Phase management with test mode lock-out
SF3	Protection against snooping
SF4	TSF self test
SF5	Virtual Memory System (VMS)
SF6	Cryptographic support
SF7	NVM tearing save write

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 8.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 4.1.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 4.3, 4.1.1, 4.2.

The TOE has various configurations. The entire configuration is done during the manufacturing process of the TOE according to the choice of the user. All differences between the products of this TOE are realized by means of blocking without changing the hardware. Therefore, all products of this TOE are equal from the hardware perspective. Please refer to chapter 8 for more details about the configurations.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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 Technologies AG Smartcard ICs SLE88CNFX6600PM/P, SLE88CNFX6602PM/P, SLE88CNFX5400PM/P, SLE88CNF6600PM/P, SLE88CNF6602PM/P, SLE88CNF5400PM/P, SLE88CFX6600P, SLE88CFX6602P, SLE88CFX5400P, SLE88CF6600P, SLE88CF6602P, SLE88CF5400P all with PSL 3.22.11

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	SLE88 CNFX 6600PM / M8864XXX or SLE88 CNFX 6602PM / M8867XXX or SLE88 CNFX 5400PM / M8960XXX or SLE88 CNF 6600PM / M8954XXX or SLE88 CNF 6602PM / M8957XXX or SLE88 CNF 5400PM / M8970XXX or SLE88 CNFX 6600P / M8865XXX or SLE88 CNFX 6602P / M8868XXX or SLE88 CNFX 5400P/ M8961XXX or SLE88 CNF 6600P / M8955XXX or SLE88 CNF 6602P / M8958XXX or SLE88 CNF 5400P / M8971XXX or SLE88 CFX 6600P / M8866XXX or SLE88 CFX 6602P / M8869XXX or SLE88 CFX 5400P / M8962XXX or SLE88 CF 6600P / M8956XXX or SLE88 CF 6602P / M8959XXX or SLE88 CF 5400P / M8972XXX	a13	Complete modules, in form of plain wafers or in an IC case (e.g. DSO20)

No	Type	Identifier	Release	Form of Delivery
2	SW	IC Dedicated Test Software STS	06.03.03.03 build 0016	Included in ROM of the HW
3	SW	IC Dedicated Test Software TNVM	0e.31	Included in ROM of the HW
4	SW	IC Dedicated Support Software PSL (Platform Support Layer)	3.22.11	Included in ROM of the HW or Electronic Data.
5	DOC	SLE88CNFX Family Hardware Reference User's Manual, Infineon Technologies AG	Edition 19-12-2009	Electronic Data/Hardcopy
6	DOC	SLE88CNFXxxxxPM PSL & Security Reference Manual, Infineon Technologies AG	Edition May 2011	Electronic Data/Hardcopy
7	DOC	SLE88CNFX Family Errata Sheet, Infineon Technologies AG	02-07-2010	Electronic Data/Hardcopy

Table 2: Deliverables of the TOE

The deliverables and the form of the delivery is outlined in ST [6], section 2.2.5. All parts of the PSL needed for tailoring 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 ([6]). The SLE88CNFXxxxxPM PSL & Security Reference Manual [11] guides how to tailor the PSL to evaluated variants. A guidance on delivery procedures is also given in [11], A5.2. Therein the delivery of user guidance is explained as follows. Infineon Technologies AG provides the user guidance in electronic form encrypted with the PGP tool within an already established PKI. The customer has to:

- decrypt the received documents
- check whether the received documents match the document versions referenced in the accompanying certification report (available at www.bsi.bund.de of the "Bundesamt für Sicherheit in der Informationstechnik".
- optionally, Infineon Technologies AG sends the user guidance in personalized paper form to the customer.

The non-ISO Reset of the chip allows the user to get the chip identification information. The hardware version can be identified by the nameplate on the surface of the die. Details can be found in the SLE88CFXxxxxP PSL & Security Reference Manual [11] and the "SLE88CNFX Family Hardware Reference User's Manual" [10].

The new workspace based on one of the certified PSLs can be downloaded to the target chip via the Flash or the Patch Loader. In order to start the Loader driver on the target chip, a 'mini-operating system' is stored by Infineon's factory, which becomes active after each reset. The 'mini-operating system' is not part of the PSL and not certified. If the download of the new workspace is executed, the user has to ensure that the 'mini-operating system' is overwritten or disabled as described in [11].

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) 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 SHA-1and SHA-256 functionality.

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 and Triple-DES 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 Assumptions defined in the Security Target and some aspects of Threats and organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Usage of Hardware Platform
- Treatment of User Data
- Protection during Packaging, Finishing and Personalisation
- Usage of Key-dependent Functions

Details can be found in the Security Target [6] chapter 4.3.

5 Architectural Information

The Infineon SLE800CNFX6600PM smart card IC (Security Controller) 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 “SLE88CNFX6600PM/m8864 Security Target”. The complete hardware description, the complete instruction set and the programmers interfaces to the PSL of the Infineon SLE800CNFX6600PM smart card controller can be found in the “SLE88CNFX Family Hardware Reference User’s Manual” [10] and “SLE88CNFXxxxxPM PSL & Security Reference Manual” [11].

For the implementation of the TOE Security Functions basically the components 32-bit proprietary CPU, (Triple-) DES Co-Processor, numeric coprocessor, 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).

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

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 developer's 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 developer's 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 developer has tested the TOE. In cases that different configurations were tested, the evaluators assessed the validity of test results for the TOE.

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

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The evaluated derivative of the TOE is SLE88CNFX6600PM/M8864XXX a13 with PSL Version 3.22.11, STS Version 06.03.03.03 build 0016 and TNVM software rev. 0e.31.

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

The evaluation results including also results of tests performed by the developer are valid for all hardware derivatives of the TOE containing the same software (PSL, STS and NVM), 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 including also results of tests performed by the developer are valid for all tailoring options (see [11], section 7.1) for PSL variants on all derivatives. 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.

In order to start the Loader driver on the target chip, a ’mini-operating system’ is stored by Infineon’s factory, which becomes active after each reset. The ’mini-operating system’ is not part of the PSL and not certified. If the download of the new workspace is executed, the user has to ensure that the 'mini-operating system' is overwritten or disabled as described in [11].

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

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

Supporting Document – Mandatory Technical Document, The Application of CC to Integrated Circuits

- Supporting Document – Mandatory Technical Document, Application of Attack Potential to Smartcards
- Supporting Document - Guidance, Smartcard Evaluation

(see [4], AIS 25, AIS 26, AIS 37).

For RNG assessment the scheme interpretations AIS 31 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [9] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7]
- for the Functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

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

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for the TOE Security functionality SF6 (Cryptographic Support).

The following cryptographic algorithms are used by the TOE to enforce its security policy:

Algorithm	Bit Length	Application	Portion of the TSF	Standard of Implementation	Standard of Application	Validity Period
DES	56	General service for the user, encryption and decryption	SF6	NIST Special Publication 800-67, Version 1.1 , NIST Special Publication 800-38A, Edition 2001	-	-

Algorithm	Bit Length	Application	Portion of the TSF	Standard of Implementation	Standard of Application	Validity Period
3DES	112, 168	General service for the user, encryption and decryption	SF6	NIST Special Publication 800-67, Version 1.1, NIST Special Publication 800-38A, Edition 2001	-	-
SHA	160, 256	General service for the user. The secure hash algorithm SHA is intended to be used for signature generation, verification and generic data integrity checks. The use for keyed hash operations like HMAC or similar, is not subject of the TOE	SF6	FIPS PUB 180-3	-	-

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 4, Para. 3, Clause 2). But Cryptographic Functionalities with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for this functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The Cryptographic Functionality DES, 2-key Triple DES (2TDES), SHA1 (used as collision-resistant hash function) provided by the TOE achieves a security level of maximum 80 Bits (in general context).

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation (see table 2) which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [9].

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

AES Advanced Encryption Standard

AIS Application Notes and Interpretations of the Scheme

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

CPU Central Processing Unit

DES Data Encryption Standard

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

HW Hardware

IC Integrated Circuit

IT Information Technology

ITSEC Information Technology Security Evaluation Criteria

ITSEF Information Technology Security Evaluation Facility

NVM Non Volatile Memory

PP Protection Profile

PSL Platform Support Layer

RAM Random Access Memory

RNG Random Number Generator

ROM Read-Only Memory

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

SHA	Secure Hash Algorithm
ST	Security Target
STS	Self Test Software
SW	Software
SWP	Single Wire Protocol
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionalities
UART	Universal Asynchronous Receiver Transmitter
VMS	Virtual Memory System

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0706-2011, Version 0.3, 30.05.2011, SLE88CNFX6600PM/m8864 Security Target, Infineon Technologies AG

[7] Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

[8] Evaluation Technical Report, Version 1.02, 09.06.2011, T-Systems GEI GmbH, (confidential document)

[9] ETR for composite evaluation according to AIS 36 for the Product Infineon Smart Card IC SLE88CNFX6600PM/m8864, Version 1.02, 09.06.2011, T-Systems GEI GmbH (confidential document)

[10] SLE88CNFX Family Hardware Reference User's Manual, Edition 19-12-2009, Infineon Technologies AG

[11] SLE88CNFXxxxxPM PSL & Security Reference Manual, Edition May 2011, Infineon Technologies AG

[12] SLE88CNFX Family Errata Sheet, Infineon Technologies AG, 02-07-2010

[8] specifically

- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 7, 3 August 2010, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 36, Version 3, 19 October 2010, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, 17.05.2010, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

C Excerpts from the Criteria

CC Part1:

Conformance Claim (Release 3 = chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

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

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”**Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)**

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0706-2011

Evaluation results regarding development and production environment

The IT product Infineon Technologies AG Smartcard ICs SLE88CNFX6600PM/P, SLE88CNFX6602PM/P, SLE88CNFX5400PM/P, SLE88CNF6600PM/P, SLE88CNF6602PM/P, SLE88CNF5400PM/P, SLE88CFX6600P, SLE88CFX6602P, SLE88CFX5400P, SLE88CF6600P, SLE88CF6602P, SLE88CF5400P all with PSL 3.22.11 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 29 June 2011, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2) are fulfilled for the development and production sites of the TOE listed below:

Site	Address	Function
Amkor	Amkor Technology Philippines Km. 22 East Service Rd South Superhighway Muntinlupa City 1702 Philipines Amkor Technology Philippines 119 North Science Avenue Laguna Technopark, Binan Laguna 4024 Philipines	Module Mounting
Augsburg	Infineon Technologies AG Alter Postweg 101 86159 Augsburg Germany	Development
Dresden	Infineon Technologies Dresden GmbH & Co. OHG Königsbrücker Str. 180 01099 Dresden Germany	Production, Initialisation Pre-personalisation
Dresden-Toppan	Toppan Photomask, Inc. Rähnitzer Allee 9	Mask Center

Site	Address	Function
	01109 Dresden Germany	
Graz / Villach / Klagenfurt	Infineon Technologies Austria AG Development Center Graz Babenbergerstr. 10 8020 Graz Austria Infineon Technologies Austria AG Siemensstr. 2 9500 Villach Austria Infineon Technologies Austria AG Lakeside B05 9020 Klagenfurt Austria	Development
Großostheim	Infineon Technology AG DCE Kühne & Nagel Stockstädter Strasse 10 - Building 8A 63762 Großostheim Germany	Distribution Center
Hayward	Kuehne & Nagel 30805 Santana Street Hayward, CA 94544 U.S.A.	Distribution Center
Kulim	Infineon Technologies (Kulim) Sdn. Bhd Lot 10 &11, Julan Hi-Tech 7 Industrial Zone Phase II Kulim Hi-Tech Park 09000 Kulim, Kedah Darul Aman Malaysia	Initialisation and Pre-personalisation
Munich	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg Germany	Development
Regensburg-West	Infineon Technologies AG Wernerwerkstraße 2 93049 Regensburg Germany	Module Mounting, inlay antenna mounting, Distribution Center
Singapore	Exel Singapore Pte Ltd DHL Exel Supply Chian 81, ALPS Avenue Singapore 498803	Distribution Center

Site	Address	Function
Singapore Kallang	Infineon Technologies AG 168 Kallang Way Singapore 349253	Module Mounting
Wuxi	Infineon Technologies (Wuxi) Co. Ltd. No. 118, Xing Chuang San Lu Wuxi-Singapore Industrial Park Wuxi 214028, Jiangsu P.R. China	Module Mounting, Distribution Center

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.