Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0632-2011

for

SLE88CFX4001P/m8835b18, SLE88CFX4003/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 all including optional RSA2048 and SHA-2 Library

from

Infineon Technologies AG

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0632-2011

SLE88CFX4001P/m8835b18, SLE88CFX4003/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 all including optional RSA2048 and SHA-2 Library

from	Infineon Technologies AG
PP Conformance:	Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI-PP-0002-2001
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, AVA_MSU.3, AVA_VLA.4

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, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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, 16 December 2011
For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Department

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 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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 (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.

[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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

It includes assurance levels beyond EAL4 resp.E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 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 September 2011 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 website: 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 by the nations listed above.

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 SLE88CFX4001P/m8835b18, SLE88CFX4003/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 all including optional RSA2048 and SHA-2 Library, has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0395-2007. Specific results from the evaluation process BSI-DSZ-CC-0395-2007 were re-used.

The evaluation of the product SLE88CFX4001P/m8835b18, SLE88CFX4003/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 all including optional RSA2048 and SHA-2 Library, was conducted by T-Systems GEI GmbH. The evaluation was completed on 28 October 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

[6] Information Technology Security Evaluation Facility

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 SLE88CFX4001P/m8835b18, SLE88CFX4003/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 all including optional RSA2048 and SHA-2 Library, 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.

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

This page is intentionally left blank.

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) encloses the Infineon SLE88CFX4001P/m8835b18 including optional RSA2048 and SHA-2 Library and the chip derivates SLE88CFX4003P/m8837b18, SLE88CFX3521P/m8857b18, SLE88CFX2921P/m8859b18, all with production line identicator „2“ for Dresden. The hardware and the firmware of the SLE88CFX4001P and the three derivates are identical. The differences between the derivates are the NVM and User ROM size.

The TOE is an integrated circuit (IC) providing a hardware and software platform (Platform Support Layer PSL) to a Smartcard Embedded Software. The TOE is intended to be used in Smart cards for particularly security-relevant applications. That is based on its previous use as developing platform for smart card operating systems according to the lifecycle model defined in [9]. Several security features independently implemented in hardware or controlled by software will be provided to ensure proper operation and integrity and confidentiality of stored data. This includes for example measures for memory protection, leakage protection and sensors to allow operations only under specified conditions.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI-PP-0002-2001 [6].

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, AVA_MSU.3, AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.2.

The TOE Security Functional Requirements are implemented by the following TOE security functions:

TOE Security Function	Addressed issue
SEF1	Operating state checking
SEF2	Phase management with test mode lock-out
SEF3	Protection against snooping
SEF4	Data encryption and data disguising
SEF5	Random number generation
SEF6	TSF self test
SEF7	Notification of physical attack
SEF8	Virtual Memory System (VMS)
SEF9	Cryptographic support
SEF10	NVM tearing save write

Table 1: TOE security functions

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

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6], chapter 6 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the following configurations of the TOE: SLE88CFX4001P/b18 with (Extended) PSL Version 2.00.07 and RSA2048 v1.02.014 (optional) and SHA-2 v1.02.014 (optional), STS Version 00.0F.0F.0F build 585 and TNVM software 09.08. For the evaluation of ADO_IGS the SDK2.9 SP6 was used. For details see chapter 9 of this report.

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:

SLE88CFX4001P/m8835b18, SLE88CFX4003/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 all including optional RSA2048 and SHA-2 Library

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	SLE88CFX4001P/m8835 or SLE88CFX4003/m8837 or SLE88CFX3521P/m8857 or SLE88CFX2921P/m8859 all with production line identicator „2“ for Dresden	b18	Complete modules, in form of plain wafers or in an IC case (e.g. DSO20)
2	SW	IC Dedicated Test Software STS	00.0F.0F.0F build 585	Included in ROM of the HW
3	SW	IC Dedicated Test Software TNVM	09.08	Included in ROM/NVM of the HW
4	SW	IC Dedicated Support Software PSL (Platform Support Layer)	2.00.07	Included in ROM of the HW or Electronic Data.
5	SW	IC Dedicated Support Software Crypto Libraries RSA2048 and SHA-2	1.02.0014	Electronic Data
6	DOC	SLE88 Family - Hardware Reference Manual, Infineon Technologies AG [11]	Edition 2006-07	Electronic Data/Hardcopy

No	Type	Identifier	Release	Form of Delivery
7	DOC	SLE88 Family - SLE88CFXxxxxP PSL & Security Reference Manual, Infineon Technologies AG [12]	Edition 2011-07	Electronic Data/Hardcopy
8	DOC	SLE88CFXxxx1P/3P Errata Sheet, Infineon Technologies AG [13]	25.06.08	Electronic Data/Hardcopy
9	DOC	SLE88 Asymmetric Crypto Library for Crypto@1408 RSA, Infineon Technologies AG [14]	1.02.014, Edition July 06, 2011	Electronic Data/Hardcopy

Table 2: Deliverables of the TOE

The identification of the chip hardware can be done as described in [12], chapter A5 and in [11], chapter 5.4.

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], chapter 11 Appendix. The guidance documentation [12] shows how to tailor the PSL to evaluated variants.

The "mini-operating system" used for embedded software development software has to be disabled by the user as described in [12] and is not a part of any of the evaluated configurations.

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

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE.

The Security Policy of the TOE is to provide basic security functionalities 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 several hardware accelerators and software modules to support the standard cryptographic operations to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols. The TOE will also provide a Random Number Generator.

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 3.2.

5 Architectural Information

A top level block diagram and a list of subsystems can be found within the TOE description of [6], chapter 2.1. The complete hardware description, the complete instruction set and the programmers interfaces to the PSL of the TOE can be found in [11] and [12]. The architecture of the cryptolibrary is provided in [14].

For the implementation of the TOE security functions basically the components 32-bit proprietary CPU, (Triple-) DES Co-Processor, numeric coprocessor (Crypto@1408Bit), 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. The cryptolibraray provides services related to AES, RSA, SHA1 and SHA2. 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 API of cryptolibrary is available via PSL I/O-driver API.

The modular arithmetic functions provided by the PSL are designed to help the user to implement different asymmetric cryptographic algorithms.

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 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. 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).

8 Evaluated Configuration

The evaluated derivate of the TOE is SLE88CFX4001P/b18 with (Extended) PSL Version 2.00.07 and RSA2048 v1.02.014 (optional) and SHA-2 v1.02.014 (optional), STS Version 00.0F.0F.0F build 585 and TNVM software 09.08 with production line identicator „2“ for Dresden.

9 Results of the Evaluation

9.1 CC specific results

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 up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- The Application of CC to Integrated Circuits
- Application of Attack Potential to Smartcards
- Functionality classes and evaluation methodology for physical random number generators and
- ETR-lite – for Composition and ETR-lite – for composition: Annex A Composite smartcard evaluation: Recommended best practice

(see [4, AIS 25, AIS 26, AIS 31 and AIS 36]) were used.

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] 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 class ASE

- All components of the EAL 5 package as defined in the CC (see also part C of this report)
- The components ALC_DVS.2, AVA_MSU.3, AVA_VLA.4 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0395-2007, results of the previous certification were taken into account. All work units were re-performed.

The evaluation has confirmed:

- PP Conformance: Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI-PP-0002-2001 [9]
- 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, AVA_MSU.3, AVA_VLA.4
- The following TOE security functions fulfil the claimed Strength of Function : high

SEF2	Phase management with test mode lock-out
SEF3	Protection against snooping
SEF4	Data encryption and data disguising
SEF5	Random number generation
SEF9 (partly)	RSA key generation, SHA-1 and SHA2

In order to assess the Strength of Function the scheme interpretations AIS 31 (see [4]) were used.

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 rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for:

- the TOE Security Function SEF9 (DES, 3DES, RSA, AES, RSA 2048, SHA1 and SHA 2) and
- for other usage of encryption and decryption within the TOE.

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 these functions 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 Functionalities SHA1 used as collision-resistent hash function, 2-key Triple DES (2TDES) and RSA 512-1024 bit 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 operational 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.

The limited validity for the usage of cryptograhic algortithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

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 [10].

In addition, the following aspects need to be fulfilled when using the TOE:

See chapter 7.2 of [10]. The developer has to provide chapter 7.2 of [10] as part of the guidance documentation to the user.

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

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
DES	Digital Encryption Standart, symmetric block cipher algorithm
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NVM	Non Volatile Memory
PP	Protection Profile
PSL	Platform Support Layer
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman, asymmetric block cipher algorithm
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SPA	Simple Power Analysis
SSM	Supply Shutdown Mode
ST	Security Target
STS	Self Test Software
TDES	Tripple-DES
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE security functions
TSP	TOE Security Policy

12.2 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.

13 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.[8]

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

[6] Security Target BSI-DSZ-CC-0632-2011, Version 2.0, 26 October 2011, SSLE88CFX4001P / m8835 includung optional RSA2048 and SHA-2 Library Security Target, Infineon Technologies AG

[7] Evaluation Technical Report, Version 2.02, 26 October 2011, Evaluation Technical Report – Summary for Infineon Smart Card IC SLE88CFX4001P/m8835, T-Systems GEI GmbH (confidential document)

[8] Configuration list for the TOE, Version 1.6, 6 July 2011, SLE88CFX4001P / m8835 Configuration Management Scope (confidential document)

[9] Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI-PP-0002-2001

[10] ETR for composite evaluation according to AIS 36 for the Product Infineon Smart Card IC SLE88CFX4001P/m8835, Version 2.02, 6 October 2011, T-Systems GEI GmbH (confidential document)

[11] Guidance documentation for the TOE, Edition 2006-07, SLE88 Family - Hardware Reference Manual, Infineon Technologies AG

[12] Guidance documentation for the TOE, Edition 2011-07, SLE88 Family - SLE88CFXxxxxP PSL & Security Reference Manual, Infineon Technologies AG

[8] specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- 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 September 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 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[13] Guidance documentation for the TOE, 25 June 2008, SLE88CFXxxx1P/3P Errata Sheet, Infineon Technologies AG

[14] Guidance documentation for the TOE, Version 1.02.014, 6 July 2011, SLE88 Asymmetric Crypto Library for Crypto@1408 RSA, Infineon Technologies AG

[15] FIPS PUB 180-1 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SECURE HASH STANDARD, National Institute of Standards and Technology, April 17, 1995

[16] FIPS PUB 180-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SECURE HASH STANDARD (SHS), National Institute of Standards and Technology, Oct08

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:

- **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.
- **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:

- **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.
- **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:

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

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

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

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 B of Certification Report BSI-DSZ-CC-0632-2011

Evaluation results regarding development and production environment

The IT product SLE88CFX4001P/m8835b18, SLE88CFX4003/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 all including optional RSA2048 and SHA-2 Library (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 16 December 2011, the following results regarding the development and production environment apply. The Common Criteria Security 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:

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

Site	Address	Function
Dresden-Toppan	Toppan Photomask, Inc. Rähnitzer Allee 9 01109 Dresden Germany	Mask Center
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	Production, Initialisation 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

Site	Address	Function
Singapore	Exel Singapore Pte Ltd DHL Exel Supply Chian 81, ALPS Avenue Singapore 498803	Distribution Center
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.