

# Certification Report

**BSI-DSZ-CC-0854-2013**

for

**Infineon smartcard IC (Security Controller) M7791  
B12 with optional SCL library version 1.01.009 and  
with specific IC-dedicated firmware**

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



# Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

## BSI-DSZ-CC-0854-2013

**Infineon smartcard IC (Security Controller) M7791 B12 with optional SCL library version 1.01.009 and with specific IC-dedicated firmware**

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



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, 28 August 2013

For the Federal Office for Information Security

Bernd Kowalski  
Head of Department

L.S.



SOGIS Recognition  
Agreement

This page is intentionally left blank.

## Preliminary Remarks

Under the BSIG<sup>1</sup> 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.

---

<sup>1</sup> Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

## Contents

|    |   |    |
|----|---|----|
| A  | Certification.....                                  | 7  |
| 1  | Specifications of the Certification Procedure.....  | 7  |
| 2  | Recognition Agreements.....                         | 7  |
| 3  | Performance of Evaluation and Certification.....    | 8  |
| 4  | Validity of the Certification Result.....           | 9  |
| 5  | Publication.....                                    | 9  |
| B  | Certification Results.....                          | 11 |
| 1  | Executive Summary.....                              | 12 |
| 2  | Identification of the TOE.....                      | 14 |
| 3  | Security Policy.....                                | 15 |
| 4  | Assumptions and Clarification of Scope.....         | 16 |
| 5  | Architectural Information.....                      | 16 |
| 6  | Documentation.....                                  | 17 |
| 7  | IT Product Testing.....                             | 17 |
| 8  | Evaluated Configuration.....                        | 18 |
| 9  | Results of the Evaluation.....                      | 18 |
| 10 | Obligations and Notes for the Usage of the TOE..... | 20 |
| 11 | Security Target.....                                | 21 |
| 12 | Definitions.....                                    | 21 |
| 13 | Bibliography.....                                   | 25 |
| C  | Excerpts from the Criteria.....                     | 27 |
|    | CC Part 1:.....                                     | 27 |
|    | CC Part 3:.....                                     | 28 |
| D  | Annexes.....  | 37 |

## A Certification

### 1 Specifications of the Certification Procedure

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

- BSIG<sup>2</sup>
- BSI Certification Ordinance<sup>3</sup>
- BSI Schedule of Costs<sup>4</sup>
- 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<sup>5</sup> [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.

#### 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. 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.

---

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

<sup>3</sup> 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

<sup>4</sup> 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

<sup>5</sup> Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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 ALC\_DVS.2, ALC\_TAT.2, ALC\_CMS.5 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 smartcard IC (Security Controller) M7791 B12 with optional SCL library version 1.01.009 and with specific IC-dedicated firmware has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0814-2012. Specific results from the evaluation process BSI-DSZ-CC-0814-2012 were re-used.

The evaluation of the product Infineon smartcard IC (Security Controller) M7791 B12 with optional SCL library version 1.01.009 and with specific IC-dedicated firmware was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 22 August 2013. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)<sup>6</sup> 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.

---

<sup>6</sup> Information Technology Security Evaluation Facility

## 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, as 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 smartcard IC (Security Controller) M7791 B12 with optional SCL library version 1.01.009 and with specific IC-dedicated firmware, has been included in the BSI list of 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<sup>7</sup> of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

<sup>7</sup> 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) is the **Infineon smartcard IC (Security Controller) M7791 B12 with optional SCL library version 1.01.009 and with specific IC-dedicated firmware**. The TOE consists of a core system, memories, coprocessor, peripherals, security modules and analog peripherals. The major components of the core system are the CPU, the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The  $\mu$ SCP co-processor supports 3DES and AES processing, while the peripheral block contains the random number generation and the external interfaces service. The peripheral block also contains timers and a watchdog. All data of the memory block is encrypted, RAM and ROM are equipped with an error detection code and the NVM is equipped with an error correction code (ECC). Security modules manage the alarms. Alarms may be triggered when the environmental conditions are outside the specified operational range. The block diagram of the TOE is shown in [6] and [8], Figure 1. The TOE comprises as one part the hardware of the smart card security controller in various configurations.

The TOE is able to communicate using its contactless interface. The interface provides the flexibility to use different communication protocols: e.g. ISO 14443 Type A and Type B, ISO/IEC 18092 passive mode can be chosen and configured.

This TOE is intended to be used in smartcards and for its previous use as a development platform for smartcard operating systems according to the lifecycle model from [8] The term Smartcard Embedded 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 Smartcard Embedded Software. The Smartcard Embedded Software itself is not part of the TOE.

This TOE is represented by various configurations called products. The degree of freedom for configuring the TOE is predefined by Infineon Technologies AG. For more details please refer to the Security Target [6] and [8], chapter 2.2.7.

The micro Symmetric Cryptographic Processor ( $\mu$ SCP) supports calculation of dual-key or triple-key triple-DES and AES. The  $\mu$ SCP in combination with the optional SCL library compute the complete 3DES and AES algorithm. The SCL library is used to provide a high level interface to the 3DES and AES cryptography, which is partly implemented on the hardware component  $\mu$ SCP and includes countermeasures against SPA, DPA and DFA attacks. The SCL library is delivered as object code and in this way integrated into the user software.

Note that the  $\mu$ SCP can be blocked. The blocking depends on the user's choice prior to the production of the hardware.

The entire firmware of the TOE consists of different parts. One part comprises the RMS and SAM routines for NVM programming, security functional test, and random number online testing . The RMS and SAM routines are stored by Infineon Technologies in ROM. The second part is the STS, consisting of test and initialization routines. The STS routines are stored in a specially protected test ROM and are not accessible by user software. The third part is the Flash Loader, a piece of software located in ROM and NVM. It supports download of user software or parts of it to NVM. After completion of the download the Flash Loader can be deactivated permanently by the user. The fourth part is the Mifare compatible software interface, accessible via RMS routines, if the Mifare compatible interface option is active. Note that the Mifare compatible Interface portion is always

present but deactivated in case of non-Mifare compatible Interface derivatives. The optional software part of the TOE is the SCL library.

The SCL library is used to provide a high level interface to the 3DES and AES cryptography, which is partly implemented on the hardware component  $\mu$ SCP and includes countermeasures against SPA, DPA and DFA attacks. The SCL library is delivered as object code and in this way integrated into the user software. The TOE can be delivered with or without the SCL library. If the user decides not to use the SCL library, the accompanying “Additional Specific Security Functionality (O.Add-Functions)” Triple Data-Encryption-Standard (3DES) and Advanced Encryption Standard AES are not provided by 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] and [8], chapter 7. 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 Functionality:

| TOE Security Features | Addressed issue                         |
|-----------------------|---|
| SF_DPM                | Device Phase Management                 |
| SF_PS                 | Protection against Snooping             |
| SF_PMA                | Protection against Modification Attacks |
| SF_PLA                | Protection against Logical Attacks      |
| SF_CS                 | Cryptographic Support                   |

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6] and [8], 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] and [8], chapter 4.2.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and 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:

### **Infinion smartcard IC (Security Controller) M7791 B12 with optional SCL library version 1.01.009 and with specific IC-dedicated firmware**

The following table outlines the TOE deliverables:

| No | Type | Identifier   | Release                   | Form of delivery  |
|----|------|--|---------------------------|---|
| 1  | HW   | M7791 Smart Card IC  | B12 (produced in Dresden) | Complete modules, as plain wafers in an IC case or in bare dies |
| 2  | FW   | Flash Loader   | FW Identifier 77.014.11.2 | Stored in reserved area of ROM on the IC (patch in NVM)         |
| 3  | FW   | STS Self Test Software (the IC Dedicated Test Software)  | FW Identifier 77.014.11.2 | Stored in Test ROM on the IC (patch in NVM)                     |
| 4  | FW   | RMS Resource Management System (the IC Dedicated Support Software)   | FW Identifier 77.014.11.2 | Stored in reserved area of ROM on the IC (patch in NVM)         |
| 5  | FW   | SAM library  | FW Identifier 77.014.11.2 | Stored in reserved area of ROM on the IC (patch in NVM)         |
| 6  | SW   | NVM image (including Embedded Software and crypto libraries)   | –                         | Stored in Flash memory on the IC                                |
| 7  | SW   | SCL (optional)   | 1.01.009                  | Object code in electronic form                                  |
| 8  | DOC  | <i>SLx 70 Family Production and Personalization User's Manual</i>  | 2012-06-27                | Hardcopy and pdf-file   |
| 9  | DOC  | <i>AMM Advanced Mode for Mifare-Compatible Technology Addendum to M7791 Hardware Reference Manual</i>                      | 2012-03-26                | Hardcopy or pdf-file  |
| 10 | DOC  | <i>M7791 SOLID FLASH Controller for Contactless Transport, Payment and Basic ID Applications Hardware Reference Manual</i> | 2012-05-03                | Hardcopy or pdf-file  |
| 11 | DOC  | <i>M7790, M7791, M7793, M7794 Controller Family for Security Applications Errata Sheet</i>                                 | 2013-07-08                | Hardcopy or pdf-file  |
| 12 | DOC  | <i>M7791 Security Guidelines User's Manual</i>   | 2013-08-06                | Hardcopy or pdf-file  |
| 13 | DOC  | <i>SLE 70 Family Programmer's Reference User Manual</i>  | 2013-03-15                | Hardcopy and pdf-file   |
| 14 | DOC  | <i>SLE77P Symmetric Crypto Library for <math>\mu</math>SCP version 2 DES / AES (1.01.009)</i>                              | 2013-03-19                | Hardcopy and pdf-file   |

Table 2: Deliverables of the TOE

A processing step during production testing incorporates the chip-individual features into the hardware of the TOE. The individual TOE hardware is uniquely identified by its serial number. The serial number comprises the lot number, the wafer number and the coordinates of the chip on the wafer. Each individual TOE can therefore be traced unambiguously and thus assigned to the entire development and production process.

As the TOE is under control of the user software, the TOE Manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the Composite Product Manufacturer to include mechanisms in the implemented software (developed by the IC Embedded Software Developer) which allows detection of modifications after the delivery.

The hardware part of the TOE is identified by M7791. Another characteristic of the TOE are the chip identification data. These chip identification data is accessible via the Generic Chip Identification Mode (GCIM). This GCIM outputs amongst others a chip identifier byte, design step, firmware identifier, metal configuration identifier, temperature range and system frequency. Additionally, dedicated RMS functions [14, chapter 8.16] allow a customer to extract the present hardware configuration.

The SCL (optional) as separate software part of the TOE is identified by its unique version number. The user can identify this version by calculating the hash signatures of the provided library files. The mapping of these hash signatures to the version numbers is provided in [8, chapter 10]. The TOE can be delivered with or without the SCL library.

### 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 a symmetric cryptographic block cipher algorithm (Triple-DES and AES) to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a True Random Number Generator (TRNG).

SCL library (optional) is used to providing a high level interface to the 3DES and AES cryptography, which is partly implemented on the hardware component  $\mu$ SCP and includes countermeasures against SPA, DPA and DFA attacks.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during AES and Triple-DES functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of security functionalities (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: protection during packaging, finishing and personalization, usage of hardware platform and treatment of user data. The augmented organizational security policy P.Add-Functions, derived from the additional security functionality of the cryptographic libraries, the augmented assumption A.Key-Function, related to the usage of key-depending functions, and the threat of memory access violation T.Mem-Access, due to specific TOE memory access control functionality, have been added. Details can be found in the Security Target [6] and [8], chapter 4.3.

## 5 Architectural Information

The TOE is an integrated circuits (IC) providing a platform to a smart card operating system and smart card application software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target Lite [8], chapter 2.1. The TOE is manufactured by Infineon Technologies in a 90 nm CMOS technology. The term Smartcard Embedded 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 Smartcard Embedded Software. The Smartcard Embedded Software itself is not part of the TOE.

The TOE consists of a core system, memories, coprocessor, peripherals, security modules and analog peripherals. The major components of the core system are the CPU, the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The  $\mu$ SCP co-processor supports 3DES and AES processing, while the peripheral block contains the random number generation and the external interfaces service. The peripheral block also contains timers and a watchdog. All data of the memory block is encrypted, RAM and ROM are equipped with an error detection code and the NVM is equipped with an error correction code (ECC). Security modules manage the alarms. Alarms may be triggered when the environmental conditions are outside the specified operational range.

The CPU accesses memory via the integrated Memory Encryption and Decryption unit (MED). The access rights of the application to the memories can be controlled with the memory management unit (MMU). Errors in RAM and ROM are automatically detected (EDC, Error Detection Code) in terms of the NVM 1-Bit-errors are also corrected (ECC, Error Correction Code).

The controller of this TOE stores both code and data in a linear 16-Mbyte memory space, allowing direct access without the need to swap memory segments in and out of memory using a memory management unit.

The cache is a high-speed memory buffer located between the CPU and (external) main memories holding a copy of some of the memory contents to enable access.

The TRNG (True Random Number Generator) is specially designed for smartcard applications. The TRNG fulfils the requirements of the functionality class PTG.2 and produces genuine random numbers which then can be used directly or as seed for the PRNG (Pseudo Random Number generator). The PRNG is not in the scope of the evaluation.

The low-power HALT mode is used to reduce the overall power consumption during data transfer between peripherals and volatile memories. The timer can be used to implement

timing critical communication protocols. The RF interface is a contactless interface compliant to ISO14443.

The Clock Unit (CLKU) supplies the clocks for all components of the TOE. The Clock Unit can work in an internal and external clock mode.

## 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 were divided into six 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 Functionalities);
2. Tests which are performed in a simulation environment with different tools for the analogue circuitries and for the digital parts of the TOE;
3. Regression tests of the hardware within a simulation environment based on special software dedicated only for the regression tests;
4. Regression tests which are performed for the IC Dedicated Test Software and for the IC Dedicated Support Software on emulator versions of the TOE and within a software simulation of chip in special hardware;
5. Characterisation and verification tests to release the TOE to production:
  - a) 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);
  - b) special verification tests for Security Functionalities 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;
6. Functional production tests, which are done for every chip to check its correct functionality as a last step of the production process (phase 3).

The developer tests cover all security functionalities and all security mechanisms as identified in the functional specification.

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developers site. They performed independent tests to supplement, augment and to verify the tests performed by the developer. The tests of the developer were repeated by sampling, by repetition of complete regression tests and by software routines developed by the evaluators and computed on samples with an evaluation operating system. For the developer tests repeated by the evaluators other test parameters were used and the test

equipment was varied. 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 evaluation has shown that the actual version of the TOE provides the security functionalities as specified by the developer. The test results confirm the correct implementation of the TOE security functionalities.

For penetration testing the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities 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. The penetration tests results confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

## 8 Evaluated Configuration

This certification covers the following configurations of the TOE:

- Smartcard IC M7791 B12.

Depending on the blocking configuration a M7791 product can have different user available configurations listed below:

| Blocking object    | Blocking options      |
|--------------------|-----------------------|
| Solid Flash        | Up to 100 kByte       |
| RAM                | Up to 4 kByte         |
| µSCP               | Available/unavailable |
| System Frequency   | 33MHz to maximum      |
| RFI input capacity | 27pF, 56pF, 78pF      |

Table 3: Blocking Configurations

The Bill-Per-Use (BPU) method enables a customer to use tailored products of the TOE within the TOE’s configuration options (see Table 3). BPU allows a customer to block chips on demand at the customer’s premises. Customers, who intend to use this feature receive the TOEs in a predefined configuration. The blocking information is part of a chip configuration area. Dedicated blocking information can be modified by customers using specific APDUs. Once final blocking is done, further modifications are disabled. the user is free to choice prior to production, whether he needs the symmetric co-processor µSCP or not. In addition, the user is also free to choice whether the TOE comes with a delivered cryptographic library SCL or without. Details can be found in the Security Target [6] and [8], chapter 2.2.7.

## 9 Results of the Evaluation

### 9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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).

The following guidance specific for the technology was used:

- The Application of CC to Integrated Circuits
- The Application of Attack Potential to Smartcards
- Guidance, Smartcard Evaluation
- Functionality classes and evaluation methodology of physical random number generators

(see [4], AIS 25, AIS 26, AIS 31).

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 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.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0814-2012, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on several minor/major hardware changes.

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 / extended  
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: SF\_CS (Cryptographic Support).

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

- algorithms for the encryption and decryption: 3DES, AES

The strength of the cryptographic algorithms was not rated in the course of the product certification (see BSIG Section 9, Para. 4, 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' ([www.bsi.bund.de](http://www.bsi.bund.de)).

The Cryptographic Functionalities 2-key Triple DES (3DES) 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 OSPs 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 cryptographic algorithms 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:

- All security hints described in the delivered documents [13] to [18] have to be considered.

The Composite Product Manufacturer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

- All security hints described in [12] have to be considered.

In addition the following hint resulting from the evaluation of the ALC evaluation aspect has to be considered:

- The IC Embedded Software Developer can deliver his software either to Infineon to let them implement it in the TOE (in Flash memory) or to the Composite Product Manufacturer to let him download the software in the Flash memory.
- The delivery procedure from the IC Embedded Software Developer to the Composite Product Manufacturer is not part of this evaluation and a secure delivery is required.

## 11 Security Target

For the purpose of publishing, the Security Target [8] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

## 12 Definitions

### 12.1 Acronyms

|                    |   |
|--------------------|---|
| <b>AES</b>         | Advanced Encryption Standard  |
| <b>AIS31</b>       | “Anwendungshinweise und Interpretationen zu ITSEC und CC Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren” |
| <b>APB™</b>        | Advanced Peripheral Bus   |
| <b>APDU</b>        | Application Protocol Data Unit  |
| <b>API</b>         | Application Programming Interface   |
| <b>AXI™</b>        | Advanced eXtensible Interface Bus Protocol  |
| <b>BPU</b>         | Bill Per Use  |
| <b>BSI</b>         | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany  |
| <b>BSIG</b>        | BSI-Gesetz / Act on the Federal Office for Information Security   |
| <b>CC</b>          | Common Criteria for IT Security Evaluation  |
| <b>CEM</b>         | Common Methodology for Information Technology Security Evaluation   |
| <b>CI</b>          | Chip Identification Mode (STS-CI)   |
| <b>CIM</b>         | Chip Identification Mode (STS-CI), same as CI   |
| <b>CPU</b>         | Central Processing Unit   |
| <b>CCRA</b>        | Common Criteria Recognition Arrangement   |
| <b>Crypto2304T</b> | Asymmetric Cryptographic Processor  |
| <b>CRC</b>         | Cyclic Redundancy Check   |
| <b>CRT</b>         | Chinese Remainder Theorem   |
| <b>DCLB</b>        | Digital Contactless Bridge  |
| <b>DES</b>         | Data Encryption Standard; symmetric block cipher algorithm  |
| <b>DPA</b>         | Differential Power Analysis   |

|                     |   |
|---------------------|---|
| <b>DFA</b>          | Differential Failure Analysis                           |
| <b>EAL</b>          | Evaluation Assurance Level                              |
| <b>EC</b>           | Elliptic Curve Cryptography                             |
| <b>ECC</b>          | Error Correction Code                                   |
| <b>ECDH</b>         | Elliptic Curve Diffie–Hellman                           |
| <b>ECDSA</b>        | Elliptic Curve Digital Signature Algorithm              |
| <b>EDC</b>          | Error Detection Code                                    |
| <b>EDU</b>          | Error Detection Unit                                    |
| <b>EEPROM</b>       | Electrically Erasable and Programmable Read Only Memory |
| <b>EMA</b>          | Electro Magnetic Analysis                               |
| <b>Flash EEPROM</b> | Flash Memory  |
| <b>FL</b>           | Flash Loader software                                   |
| <b>FW</b>           | Firmware  |
| <b>GCIM</b>         | Generic Chip Identification Mode                        |
| <b>HW</b>           | Hardware  |
| <b>IC</b>           | Integrated Circuit                                      |
| <b>ICO</b>          | Internal Clock Oscillator                               |
| <b>ID</b>           | Identification  |
| <b>IMM</b>          | Interface Management Module                             |
| <b>IT</b>           | Information Technology                                  |
| <b>ITP</b>          | Interrupt and Peripheral Event Channel Controller       |
| <b>I/O</b>          | Input/Output  |
| <b>IRAM</b>         | Internal Random Access Memory                           |
| <b>MED</b>          | Memory Encryption and Decryption                        |
| <b>MMU</b>          | Memory Management Unit                                  |
| <b>NVM</b>          | Non-Volatile Memory                                     |
| <b>OS</b>           | Operating system  |
| <b>ST</b>           | Security Target   |
| <b>PEC</b>          | Peripheral Event Channel                                |
| <b>PP</b>           | Protection Profile                                      |
| <b>PRNG</b>         | Pseudo Random Number Generator                          |
| <b>PROM</b>         | Programmable Read Only Memory                           |
| <b>RAM</b>          | Random Access Memory                                    |
| <b>RMS</b>          | Resource Management System                              |
| <b>RNG</b>          | Random Number Generator                                 |

|                     |   |
|---------------------|---|
| <b>ROM</b>          | Read Only Memory  |
| <b>RSA</b>          | Rives-Shamir-Adleman Algorithm  |
| <b>SAM</b>          | Service Algorithm Minimal   |
| <b>SCP</b>          | Symmetric Cryptographic Processor   |
| <b>SF</b>           | Security Feature  |
| <b>SFR</b>          | Special Function Register, as well as Security Functional Requirement, the specific meaning is given in the context |
| <b>SOLID FLASH™</b> | An Infineon Trade Mark and Stands for Flash EEPROM Technology   |
| <b>SPA</b>          | Simple Power Analysis   |
| <b>STS</b>          | Self Test Software  |
| <b>SW</b>           | Software  |
| <b>SO</b>           | Security Objective  |
| <b>TOE</b>          | Target of Evaluation  |
| <b>TM</b>           | Test Mode (STS)   |
| <b>TSF</b>          | TOE Security Functions  |
| <b>TRNG</b>         | True Random Number Generator  |
| <b>TSC</b>          | TOE Security Functions Control  |
| <b>TSF</b>          | TOE Security Functionality  |
| <b>UART</b>         | Universal Asynchronous Receiver/Transmitter   |
| <b>UM</b>           | User Mode (STS)   |
| <b>UmSLC</b>        | User Mode Security Life Control   |
| <b>WDT</b>          | Watch Dog Timer   |
| <b>XRAM</b>         | eXtended Random Access Memory   |
| <b>3DES</b>         | Triple DES Encryption Standards   |

## 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** - A 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 4, September 2012  
Part 2: Security functional components, Revision 4, September 2012  
Part 3: Security assurance components, Revision 4, September 2012
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012
- [3] BSI certification: Procedural Description (BSI 7125)
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE<sup>8</sup>.
- [5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website
- [6] Security Target M7791 B12 including the optional Software Library SCL BSI-DSZ-CC-0854-2013, Version 3.3, 2013-08-06, Infineon Technologies AG (confidential document)
- [7] Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007
- [8] Security Target Lite M7791 B12 BSI-DSZ-CC-0854-2013, Version 3.3, 2013-08-06, Infineon Technologies AG (sanitised public document)
- [9] Evaluation Technical Report (ETR Summary) for the M7791 B12, BSI-DSZ-CC-0854, Version 2, 2013-08-23, TÜV Informationstechnik GmbH (confidential document)
- [10] ETR for composite evaluation according to AIS 36 for the Product M7791 B12, Version 2, 2013-08-23, TÜV Informationstechnik GmbH (confidential document)
- [11] Configuration Management Scope M7791 B12 including optional Software Library SCL, Version 2.0, 2013-04-03, Infineon Technologies AG (confidential document)
- [12] SLx 70 Family Production and Personalization User's Manual, 2012-06-27, Infineon Technologies AG
- [13] SLE77P Symmetric Crypto Library for µSCP version 2 DES / AES User Interface (1.01.009), 2013-03-09, Infineon Technologies AG

<sup>8</sup>specifically

- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 1, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

- [14] SLE 70 Family Programmer's Reference User Manual, 2013-03-15, Infineon Technologies AG
- [15] M7790, M7791, M7793, M7794 Controller Family for Security Applications Errata Sheet, Version 2.0, 2013-07-08, Infineon Technologies AG
- [16] M7791 SOLID FLASH Controller for Contactless Transport Payment and Basic ID Applications Hardware Reference Manual, Version 1.0, 2012-05-03, Infineon Technologies AG
- [17] AMM Advanced Mode for Mifare-Compatible Technology Addendum to M7791 Hardware Reference Manual, Rev.1.0, Version 1.0, 2012-03-26, Infineon Technologies AG
- [18] M7791 Security Guidelines User's Manual, 2013-08-06, Infineon Technologies AG

## C Excerpts from the Criteria

CC Part 1:

### Conformance Claim (Release Release 4 = 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<br>APE_OBJ.2 Security objectives |
|  | APE_ECD.1 Extended components definition   |
|  | APE_REQ.1 Stated security requirements<br>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<br>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<br>ASE_OBJ.2 Security objectives                  |
|  | ASE_ECD.1 Extended components definition  |
|  | ASE_REQ.1 Stated security requirements<br>ASE_REQ.2 Derived security requirements                               |
|  | ASE_TSS.1 TOE summary specification<br>ASE_TSS.2 TOE summary specification with architectural design<br>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<br>ADV_FSP.2 Security-enforcing functional specification<br>ADV_FSP.3 Functional specification with complete summary<br>ADV_FSP.4 Complete functional specification<br>ADV_FSP.5 Complete semi-formal functional specification with<br>additional error information<br>ADV_FSP.6 Complete semi-formal functional specification with<br>additional formal specification |
|                  | ADV_IMP.1 Implementation representation of the TSF<br>ADV_IMP.2 Implementation of the TSF   |
|                  | ADV_INT.1 Well-structured subset of TSF internals<br>ADV_INT.2 Well-structured internals<br>ADV_INT.3 Minimally complex internals   |
|                  | ADV_SPM.1 Formal TOE security policy model  |
|                  | ADV_TDS.1 Basic design<br>ADV_TDS.2 Architectural design<br>ADV_TDS.3 Basic modular design<br>ADV_TDS.4 Semiformal modular design<br>ADV_TDS.5 Complete semiformal modular design<br>ADV_TDS.6 Complete semiformal modular design with formal<br>high-level design presentation   |

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

38

## Annex B of Certification Report BSI-DSZ-CC-0854-2013

### Evaluation results regarding development and production environment



The IT product Infineon smartcard IC (Security Controller) M7791 B12 with optional SCL library version 1.01.009 and with specific IC-dedicated firmware (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 28 August 2013, 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 and ALC\_TAT.2))

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

| Site   | Address  | Function                   |
|--|--|----------------------------|
| Agrate - DNP   | DNP Photomask Europe S.p.A.<br>Via C. Olivetti 2/A<br>20041 Agrate Brianza<br>Italy  | Mask Production            |
| Augsburg   | Infineon Technologies AG<br>Alter Postweg 101<br>86159 Augsburg<br>Germany   | Development                |
| Bangalore  | Infineon Technologies India Pvt. Ltd.<br>13 <sup>th</sup> Floor, Discoverer Building<br>International Technology Park<br>Whitefield Road<br>Bangalore,<br>India – 560066 | SW Development and Testing |
| Bangkok - SmarTrac covered by [AIS47]<br>Site certification from 2011-10-25 (cert ID BSI-DSZ-CC-S-0007-2011) | Smartrac Technology Ltd.<br>142/121/115 Moo<br>Hi-Tech Industrial Estate<br>Tambon Ban Laean<br>Amphor Bang-Pa-In<br>13160 Ayutthaya<br>Thailand                         | Inlay Mounting             |
| Bukarest   | Infineon Technologies Romania<br>Blvd. Dimitrie Pompeiu Nr. 6<br>Sector 2<br>020335 Bucharest<br>Romania   | Development                |

| Site   | Address   | Function  |
|--|---|---|
| Burlington - ASK   | ASK-intTag, LLC<br>Building 966<br>1000 River St., Essex Junction,<br>Vermont 05452<br>USA  | Inlay Mounting  |
| Chanhassen   | Smartrac Technology US Inc.<br>1546 Lake Drive West<br>Chanhassen, MN 55317<br>USA  | Inlay Mounting  |
| Corbeil Essones - Toppan   | Toppan Photomask, Inc.<br>European Technology Center<br>Boulevard John Kennedy 224<br>91105 Corbeil Essones<br>France   | Mask Production   |
| Dresden  | Infineon Technologies Dresden GmbH<br>& Co. OHG<br>Königsbrücker Str. 180<br>01099 Dresden<br>Germany   | Wafer Production, Initialization<br>and Pre-personalization |
| Dresden - Toppan   | Toppan Photomask, Inc<br>Rähnitzer Allee 9<br>01109 Dresden<br>Germany  | Mask Production   |
| Galway - HID covered by [AIS47]<br>Site certification from 2012-09-19<br>(cert ID<br>BSI-DSZ-CC-S-0015-2012) | HID Global Ireland Teoranta<br>Pairc Tionscail na Tulaigh<br>Baile na hAbhann<br>Co. Galway<br>Ireland  | Inlay Mounting  |
| Graz / Villach / Klagenfurt  | Infineon Technologies Austria AG<br>Development Center Graz<br>Babenbergerstr. 10<br>8020 Graz<br>Austria<br><br>Infineon Technologies Austria AG<br>Siemensstr. 2<br>9500 Villach<br>Austria<br><br>Infineon Technologies Austria AG<br>Lakeside B05<br>9020 Klagenfurt<br>Austria | Development, IT   |
| Großostheim - K&N  | Infineon Technology AG<br>DCE<br>Kühne & Nagel<br>Stockstädter Strasse 10 – Building 8A<br>63762 Großostheim<br>Germany   | Distribution Center   |
| Hayward - K&N  | Kuehne & Nagel<br>30805 Santana Street<br>Hayward, CA 94544<br>USA  | Distribution Center   |

| Site                 | Address  | Function                                |
|----------------------|--|---|
| Hsin-Chu - ARDT      | Ardentec Corporation<br>No. 3, Gungye 3 <sup>rd</sup> Rd.,<br>Hsin-Chu Industrial Park, Hu-Kou,<br>Hsin-Chu Hsien, Taiwan 30351, R.O.C.<br>Taiwan 30351, R.O.C.  | Wafer Test                              |
| Manila - Amkor       | Amkor Technology Philippines<br>Km. 22 East Service Rd.<br>South Superhighway<br>Muntinlupa City 1702<br>Philippines<br><br>Amkor Technology Philippines<br>119 North Science Avenue<br>Laguna Technopark, Binan<br>Laguna 4024<br>Philippines | Module Mounting                         |
| Morgan Hill          | Infineon Technologies North America<br>Corp.<br>18275 Serene Drive<br>Morgan Hill, CA 95037<br>USA   | Inlay Testing, Distribution<br>Center   |
| Munich               | Infineon Technologies AG<br>Am Campeon 1-12<br>85579 Neubiberg<br>Germany  | Development                             |
| Munich - G&D         | Giesecke & Devrient GmbH<br>Distribution Center DLC<br>Prinzregentenstraße 159<br>81677 Munich<br>Germany  | Distribution Center                     |
| Ranzan - Toppan      | Toppan Printing Co., Ltd.<br>6-2, Hanami-Dai, Ranzan-Machi,<br>Hiki-Gun<br>Saitama 355-0204<br>Japan   | Inlay Mounting                          |
| Regensburg-West      | Infineon Technologies AG<br>Wernerwerkstraße 2<br>93049 Regensburg<br>Germany  | Module Mounting, Distribution<br>Center |
| Reichshof - SmarTrac | Smartrac Technology Germany<br>Building RW2<br>Gewerbeparkstr. 10<br>51580 Reichshof-Wehnrath<br>Germany   | Inlay Mounting, Delivery                |
| Round Rock - Toppan  | Toppan Printing Company America,<br>Inc.<br>Round Rock Site<br>2175 Greenhill Drive<br>Round Rock, Texas 78664<br>USA  | Inlay Mounting                          |
| Singapore - DHL      | DHL Exel Supply Chain<br>Richland Business Centre<br>11 Bedok North Ave 4, Level 3,<br>Singapore 489949  | Distribution Center                     |

| Site              | Address  | Function  |
|-------------------|--|---|
| Singapore Kallang | Infineon Technologies Asia Pacific PTE Ltd.<br>168 Kallang Way<br>Singapore 349253   | Module Mounting, Electrical module testing                      |
| Tainan - TSMC     | Taiwan Semiconductor Manufacturing Company Ltd.<br>1, Nan-Ke North Rd.<br>Tainan Science Park<br>Tainan 741-44<br>Taiwan                     | Mask & Wafer Production, Initialization and Pre-personalization |
| Wuxi              | Infineon Technologies (Wuxi) Co. Ltd.<br>No. 118, Xing Chuang San Lu<br>Wuxi-Singapore Industrial Park<br>Wuxi 214028, Jiangsu<br>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] and [8]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.