Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0813-2012

for

Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software

from

Infineon Technologies AG

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0813-2012

Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software

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

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

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

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

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

Bonn, 6 June 2012

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski L.S.
Head of Department

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

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

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

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.

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.

---

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

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

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

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

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.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement. This evaluation contains the components ALC_DVS.2, AVA_VAN.5, ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0728-2011. Specific results from the evaluation process BSI-DSZ-CC-0728-2011 were re-used.

The evaluation of the product Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 04 June 2012. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

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

The product was developed by: Infineon Technologies AG.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

[6] 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 smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software 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[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) is Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software. The TOE is a member of the Security Controller family SLE70, provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The TOE consists of a core system, memories, co-processors, peripherals, security modules and analogue peripherals. The major components of the core system are the two CPUs (Central Processing Units), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The co-processor block contains the processors for RSA/EC and DES/AES processing, while the peripheral block contains the random number generation and the external interfaces service. The peripheral block contains also the timers and a watchdog. All data of the memory block is encrypted and all memory types are equipped with an error detection code (EDC), the EEPROM in addition with an error correction code (ECC). The security modules serve for operation within the specified range and manage the alarms.

The dual interface controller is able to communicate using either the contact based or the contactless interface. The implemented dual interface provides a flexibility in using different communication protocols: ISO 7816, ISO 14443 Type A and Type B, FELICA® - ISO/IEC 18092 passive mode, Mifare compatible Interface or the Digital Contactless Bridge (DCLB) mode can be chosen and configured. The DCLB mode is provided by the specific TOE derivatives as listed in Table 4 and enables the use of an external analogue interface or near field communication (NFC) modem via the ISO-pads. Those external analogue modems are typically deemed for applications running in mobile devices and are not part of this TOE. In case of running the DCLB mode, which depends on the customer order and TOE start-up, the part of the contactless interface using the external antenna is out of operation.

The availability of the DCLB mode is configured during TOE production and depends on the customer order. Regarding the DCLB enabled derivates it depends on the operating system of how the pads are used.

The TOE implements a full 16 MByte linear addressable memory space for each privilege level, a simple scalable Memory Management concept and a scalable stack size. The flexible memory concept consists of ROM and Flash-memory as part of the non volatile memory (NVM), respectively EEPROM. The block diagram of the TOE is shown in [6], Figure 1. The TOE comprises as one part the hardware of the smart card security controller in various configurations.

This TOE is intended to be used in smart cards for particularly security relevant applications and for its previous use as developing platform for smart card operating systems according to the life cycle model from [7]. 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.

All products based on the M7820 representing this TOE are identically from hardware perspective and produced with the same masks. The first metal mask (called M1 mask) contains the derivate specific information (e.g. development code, first digit of the design step and i.e. ROM mask data). Depending on the blocking configuration an M7820 product can have different user available memory sizes and can come with or without individual

accessible cryptographic co-processors. For example a product with the M-number M7820 in the field can come in one project with the fully available EEPROM or in another project with equal or any other EEPROM-size below the physical implementation size, depending on the user requirements. The user is has to decide prior to production, whether the symmetric co-processor SCP, or the asymmetric co-processor Crypto2304T, or both, or none of them have to activated. In addition, the user has to select whether the TOE is used with a specific combination of parts of the delivered cryptographic libraries or without any.

The entire configuration is done during the manufacturing process of the TOE according to the choice of the user. All differences between the products of this TOE are realized by means of blocking without changing the hardware. Therefore, all products of this TOE are equal from hardware perspective.

The blocking of the EEPROM is done by setting the according value in the chip configuration page, which is not available to the user. The same means of blocking are also used for switching on and off the accessibility of the cryptographic co-processors SCP and/or Crypto2304T and also for the configuration of the XRAM and ROM sizes.

The memory settings are done during the production process by programming the physical start and end-address of the user available memory areas. The entire configuration page including also the other blocking information can not be changed by the user afterwards and is protected against manipulation. For more details please refer to the Security Target [6], chapter 1.

This TOE is equipped with Flash Loader Software (FL) to allow the download of user software, i.e. the operating system and applications. Various options can be chosen by the user to implement his software during production. For more details please refer to the Security Target [6], chapter 1.

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

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7. 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 Features:

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

TOE Security Features	Addressed issue
SF_CS	Cryptographic Support

Table 1: TOE Security Functionalities

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

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

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

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

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of delivery
1	HW	M7820 Smart Card IC	A11 (produced in Dresden)	Complete modules, with or without inlay antenna mounting, in form of plain wafers, in an IC case or in bare dies.
2	FW	Flash Loader	3.60.009 and FL patch version VP3.60.003 (FWP1) / VP3.61.002 (FWP2) / VP3.61.006 (FWP3)	Stored in reserved area of User ROM on the IC (patch in NVM)
3	FW	STS Self Test Software (the IC Dedicated Test Software)	V78.01.09.09 and STS patch version VP8009 (FWP1) / VP800B (FWP2 + FWP3)	Stored in Test ROM on the IC (patch in NVM)

No	Type	Identifier	Release	Form of delivery
4	FW	RMS Resource Management System (the IC Dedicated Support Software)	V8000 B001B and overall patch 80 0F (FWP1) / 80 14 (FWP2) / 80 47 (FWP3)	Stored in reserved area of User ROM on the IC (patch in NVM)
5	FW	SAM library	V20.22 and overall patch 80 0F (FWP1) / 80 14 (FWP2) / 80 47 (FWP3)	Stored in reserved area of User ROM on the IC (patch in NVM)
6	SW[8]	ROM code (including Embedded Software and crypto libraries)	–	Stored in User ROM on the IC
7	SW[9]	NVM image (including Embedded Software and crypto libraries)	–	Stored in Flash memory on the IC
8	SW	RSA library (optional)	RSA2048 v1.02.008 RSA4096 v1.02.008	Object code in electronic form
9	SW	EC library (optional)	EC v1.02.008	Object code in electronic form
10	SW	SHA-2 library (optional)	SHA-2v1.01	Object code in electronic form
11	SW	Toolbox (optional)	Toolbox v1.02.008	Object code in electronic form
12	DOC	*SLx 70 Family Hardware Reference Manual*	2010-11-18	Hardcopy or pdf-file
13	DOC	*M7801 / M7820 Controller Family for Security Applications Errata Sheet*	2012-03-28	Hardcopy or pdf-file
14	DOC	*M7801/M7820 Controller Security Guidelines User Manual*	2012-05-07	Hardcopy or pdf-file
15	DOC	*SLE 70 Family Programmer's Reference User's Manual*	2012-03-19	Hardcopy and pdf-file
16	DOC	*SLE70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox (1.02.008)*	2010-11-11	Hardcopy and pdf-file
17	DOC	*Crypto@2304T User Manual*	2010-03-23	Hardcopy and pdf-file
18	DOC	*SLx70 Family Secure Hash Algorithm SHA-2 (SHA 256/224, SHA 512/384) Library Version V1.01*	2009-11	Hardcopy and pdf-file
19	DOC	*SLx 70 Family Production and Personalization User's Manual*	2011-10-20	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

[8] Only in case the IC Embedded Software Developer provides Infineon with code for ROM.

[9] Only in case the IC Embedded Software Developer provides Infineon with code for Flash memory.

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. The hardware part of the TOE is identified by M7820 A11 and produced in Dresden/Germany. Another characteristic of the TOE are the chip identification data. In the field, the IC Embedded Software Developer can clearly identify a product in question by the ChipIdent function and the user guidance, whereas an additional RMS function provides the complete chip configuration besides the Flash Loader version. An additional command of the Flash Loader software allows the clear identification of the Flash Loader version. Thereby, the exact and clear identification of any product with its exact configuration of this TOE is given. The chip type byte identifies the different versions of the TOE as listed in chapter 8.

Different Chip Type codes exist for different design versions (e.g. M7820 A10 and M7820 A11). The chip type, version number and the fabrication facility are coded in the chip identification data as follows [12], chapter 8.16.1.3:

- Byte 04 of the chip identification data contains the identifier byte of the product (compare table 3),
- Byte 05 of the chip identification data contains the identifier of the design step in the format xxyy yyyy where xx = 00 or 01 (for A or B for the Dresden production site) and yyyyyy = 1…63 (e.g. design step A12 is coded as 0000 1100),
- Byte 06 of the chip identification data contains the Fabrication facility (e.g. 0010 for Dresden).

The TOE consists of the hardware part, the firmware parts and the software parts. The software parts are separated into: the cryptographic libraries RSA, EC and SHA-2 and the supporting libraries Toolbox and Base. RSA, EC, SHA-2 and Toolbox provide certain functionality via an API to the Smartcard Embedded Software. The Base Library is only used internally by the RSA, EC and Toolbox libraries and has no user interface. If none the three libraries RSA, EC and Toolbox is delivered, also the Base Library is not on board. The SHA-2 library does not use the Base Library.

The firmware parts are the RMS library, the Service Algorithm Minimal (SAM), the STS firmware for test purpose, providing some functionality via an API to the Smartcard Embedded Software, the Flash Loader for downloading user software to the NVM and the Mifare compatible software interface. The STS is implemented in a separated Test-ROM being part of the TOE.

The Smartcard Embedded Software, i.e. the operating system and applications are not part of the TOE.

The TOE can come with three valid firmware packages (FWP1, FWP2 or FWP3). Table 3 lists all firmware and software packages together with its versions (derived from table 2).

The RSA library is used to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto2304T. The routines are used for the generation of RSA Key Pairs (RsaKeyGen), the RSA signature verification (RsaVerify), the RSA signature generation (RsaSign) and the RSA modulus recalculation (RsaModulus). The hardware Crypto2304T unit provides the basic long number calculations (add, subtract, multiply, square with 1100 bit numbers) with high performance. The RSA library is delivered as object code and in this way integrated in the user software.

Package	FW/SW	Type	Release
FWP1	Firmware	Flash loader Flash loader patch RMS SAM Overall patch (for SAM, RMS and Mifare[10]) STS STS patch	V3.60.009 VP3.60.003 V8000 B001B V20.22 80 0F V78.01.09.09 VP8009
	Software	RSA crypto library (optional)	RSA2048 v1.02.008 RSA4096 v1.02.008
		EC library (optional)	EC v1.02.008
		SHA-2 library (optional)	SHA-2 v1.01
		Toolbox (optional)	Toolbox v1.02.008
FWP2	Firmware	Flash loader Flash loader patch RMS SAM Overall patch (for SAM, RMS and Mifare) STS STS patch	V3.60.009 VP3.61.002 V8000 B001B V20.22 80 14 V78.01.09.09 VP800B
	Software	RSA crypto library (optional)	RSA2048 v1.02.008 RSA4096 v1.02.008
		EC library (optional)	EC v1.02.008
		SHA-2 library (optional)	SHA-2 v1.01
		Toolbox (optional)	Toolbox v1.02.008
FWP3	Firmware	Flash loader Flash loader patch RMS SAM Overall patch (for SAM, RMS and Mifare) STS STS patch	V3.60.009 VP3.61.006 V8000 B001B V20.22 80 47 V78.01.09.09 VP800B
	Software	RSA crypto library (optional)	RSA2048 v1.02.008 RSA4096 v1.02.008
		EC library (optional)	EC v1.02.008
		SHA-2 library (optional)	SHA-2 v1.01
		Toolbox (optional)	Toolbox v1.02.008

Table 3: Firmware and Software packages of the TOE

The EC library is used to provide a high level interface to Elliptic Curve cryptography implemented on the hardware component Crypto2304T. The routines are used for ECDSA signature generation, ECDSA signature verification, ECDSA key generation and Elliptic Curve Diffie-Hellman key agreement. The EC library is delivered as object code and in this way integrated in the user software.

The SHA-library provides the calculation of a hash value of freely chosen data input in the CPU. The SHA-library is delivered as object code and is in this way available for the user software. This secure hash-algorithm SHA-2 is intended to be used for signature generation, verification and generic data integrity checks. The use for keyed hash operations like HMAC or similar security critical operations involving keys, is not subject of this TOE and requires specific security improvements and DPA analysis including the operating system, which is not part of this TOE.

[10] Note that Mifare is part of the RMS and mentioned here only for sake of consistency.

The toolbox library does not provide cryptographic support or additional security functionality as it provides only the following basic long integer arithmetic and modular functions in software, supported by the cryptographic coprocessor: Addition, subtraction, division, multiplication, comparison, reduction, modular addition, modular subtraction, modular multiplication, modular inversion and modular exponentiation. No security relevant policy, mechanism or function is supported. The toolbox library is deemed for software developers as support for simplified implementation of long integer and modular arithmetic operations.

The Base Library provides the low level interface to the asymmetric cryptographic coprocessor and has no user available interface. The base library does not provide any security functionality, implements no security mechanism, and does not provide additional specific security functionality.

The cryptographic libraries RSA, EC, SHA-2 and the Toolbox library are delivery options. If one of the libraries RSA, EC and Toolbox or combination hereof are delivered, the Base Lib is automatically part of it. The TOE may come with free combinations of or even without these libraries. In the case of coming without one or any combination of the cryptographic libraries RSA, EC and SHA-2, the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or SHA-2. The Toolbox and Base Library are no cryptographic libraries and provide no additional specific security functionality. For more details please refer to [6], chapter 2.2.2.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

Symmetric cryptographic block cipher algorithms (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 random number generation of appropriate quality.

The RSA library is used to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The EC library is used to provide a high level interface to Elliptic Curve cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. The SHA-library provides the calculation of a hash value of freely chosen data input in the CPU.

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. Details can be found in the Security Target [6], 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 [6], chapter 2.1.

The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The major components of the core system are the two CPUs (Central Processing Units), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The two CPUs control each other in order to detect faults and serve by this for data integrity. The TOE implements a full 16 MByte linear addressable memory space for each privilege level, a simple scalable Memory Management concept and a scalable stack size. The flexible memory concept consists of ROM and Flash-memory as part of the non volatile memory (NVM), respectively EEPROM. For the EEPROM memory the Unified Channel Programming (UCP) memory technology is used.

The two cryptographic co-processors serve the need of modern cryptography: The symmetric coprocessor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Co-processor, called Crypto2304T in the following, is an optimized version of the Crypto@1408 used in the SLE88-family with performance improvements for RSA-2048 bit (4096-bit with CRT) and Elliptic Curve (EC) cryptography.

The software part of the TOE consists of the cryptographic RSA-, EC- and the SHA-2 libraries and the supporting Toolbox and Base libraries. If RSA or EC or Toolbox or combinations hereof are part of the shipment, automatically the Base library is included. The Base library provides the low level interface to the asymmetric cryptographic coprocessor and has no user available interface.

Part of the evaluation are the RSA straight operations with key length from 1024 Bits to 2048 Bits, and the RSA CRT operations with key lengths of 1024 Bits to 4096 Bits. Note that key lengths below 1024 Bits are not included in the certificate. The RSA library is delivered as object code and in this way integrated in the user software. The RSA library can perform RSA operations from 512 to 4096 bits. Depending on the customer’s choice, the TOE can be delivered with the 4096 code portion or with the 2048 code portion only. The 2048 code portion is included in both.

The Flash Loader is a firmware located in the user-ROM and allowing downloading the user software or parts of it to the EEPROM flash memory. After completion of the download the Flash Loader can be permanently deactivated by the user.

For more details please refer to the Security Target [6], chapter 1.2 and 2.2.2.

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 M7820 A11.

Depending on the blocking configuration a M7820 product can have different user available memory sizes and can come with or without individual accessible cryptographic co-processors. For example a product with the M-number M7820 in the field can come in one project with the fully available EEPROM or in another project with equal or any other EEPROM-size below the physical implementation size, depending on the user requirements. The user is has to decide prior to production, whether the symmetric co-processor SCP, or the asymmetric co-processor Crypto2304T, or both, or none of them have to activated. In addition, the user has to select whether the TOE is used with a specific combination of parts of the delivered cryptographic libraries or without any. The user is furthermore free to choose whether he needs the DCLB interface. If not, the TOE comes with a blocked DCLB mode.

Chip Type	Sales Name	NVM kByte[11]	ROM kByte[11]	XRAM kByte[11]	ISO 7816[12]	ISO 14443	Mifare[13] comp. Interface	FELICA®/ ISO/IEC 18092 Passive mode	DCLB
A0h	SLE78CLX1440P	144	280	8	Yes	Yes	No	No	No
A2h	SLE78CLX1440PM	144	280	8	Yes	Yes	Yes	No	No
A3h	SLE78CLX1440PS	144	280	8	Yes	Yes	No	Yes	No
A4h	SLE78CLX1600P	160	280	8	Yes	Yes	No	No	No
A5h	SLE78CLX1600PM	160	280	8	Yes	Yes	Yes	No	No
A6h	SLE78CLX1600PS	160	280	8	Yes	Yes	No	Yes	No
A7h	SLE78CLX1280P	128	280	8	Yes	Yes	No	No	No
A8h	SLE78CLX1000P	100	280	8	Yes	Yes	No	No	No
A9h	SLE78CLX800P	80	280	8	Yes	Yes	No	No	No
AAh	SLE78CLX800PS	80	280	8	Yes	Yes	No	Yes	No
ABh	SLE78CLX800PM	80	280	8	Yes	Yes	Yes	No	No
ACh	SLE78CLX802P	80	216	8	Yes	Yes	No	No	No
ADh	SLE78CLX802PM	80	216	8	Yes	Yes	Yes	No	No
AEh	SLE78CLX780P	78	280	8	Yes	Yes	No	No	No
AFh	SLE78CLX480P	48	280	8	Yes	Yes	No	No	No
B0h	SLE78CLX480PM	48	280	8	Yes	Yes	Yes	No	No
B1h	SLE78CLX360P	36	280	8	Yes	Yes	No	No	No

[11] Depicts the size of user available memory which is defined by blocking.

[12] Availability depends on procurement order: If the DCLB mode is chosen, contactless communication using the antenna and ISO7816 communication are out of operation. If the CL-interface is chosen, the DCLB mode communication is out of operation.

[13] Mifare is only used as an indicator of product compatibility to the respective technology. This holds for the entire document, whenever the term Mifare is used.

Chip Type	Sales Name	NVM kByte	ROM kByte[11]	XRAM kByte[11]	ISO 7816	ISO 14443	Mifare comp. Interface	FELICA®/ ISO/IEC 18092 Passive mode	DCLB
B2h	SLE78CLX360PM	36	280	8	Yes	Yes	Yes	No	No
B3h	SLE78CLX360PS	36	280	8	Yes	Yes	No	Yes	No
9Bh	SLE78CDX1440PMS	144	280	8	No / Yes[12]	No / Yes[12]	No / Yes[12]	No / Yes[12]	No / Yes[12]
9Ch	SLE97144SE	144	280	8	No	No	Yes	No	Yes
95h	SLE97080SE	80	280	8	No	No	Yes	No	Yes
96h	SLE97144SD	144	280	8	Yes	Yes	Yes	Yes	No
97h	SLE97080SD	80	280	8	Yes	Yes	Yes	Yes	No
98h	SLE78CLFX1600P	160	0	8	Yes	Yes	No	No	No
99h	SLE78CLFX1600PM	160	0	8	Yes	Yes	Yes	No	No
9Ah	SLE78CLFX1600PSM	160	0	8	Yes	Yes	Yes	Yes	No

Table 4: TOE Identification (Product identifiers)

The entire configuration is done during the manufacturing process of the TOE according to the choice of the user. All differences between the products of this TOE are realized by means of blocking without changing the hardware. Therefore, all products of this TOE are equal from hardware perspective.

Beside the hardware there are three firmware configurations available. The differences are listed in table 3:

9 Results of the Evaluation

9.1 CC specific results

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

The Evaluation Methodology CEM [2] was used for those components up to 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
- The Application of Attack Potential to Smartcards
- 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 [9] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

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

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

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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0728-2011, re-use of specific evaluation tasks was possible. The changes are related to improvements of the firmware.

The evaluation has confirmed:

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

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

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

9.2 Results of cryptographic assessment

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for: SF_CS (Cryptographic Support). The following cryptographic algorithms are used by the TOE to enforce its security policy:

- hash functions: SHA-2
- algorithms for encryption and decryption: 3DES (key sizes of 2 x 56 bit or 3 x 56 bit), AES (key sizes of 128 bit or 192 bit or 256 bit), RSA (key sizes of 1024 - 4096 bit) and ECDSA (key sizes of 1024 - 4096 bit) and specific key generation algorithms as well as ECDH for key sizes of 192 - 521 bits (see [6, chapter 7.1.49])

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).

The Cryptographic Functionalities 2-key Triple DES (3DES), RSA 1024 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 [11] to [18] 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 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 [9].

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 [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

AIS31	“Anwendungshinweise und Interpretationen zu ITSEC und CC Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren”
APB™	Advanced Peripheral Bus
API	Application Programming Interface
AXI™	Advanced eXtensible Interface Bus Protocol
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
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CI	Chip Identification Mode (STS-CI)
CIM	Chip Identification Mode (STS-CI), same as CI
CPU	Central Processing Unit
CCRA	Common Criteria Recognition Arrangement
Crypto2304T	Asymmetric Cryptographic Processor
CRC	Cyclic Redundancy Check
CRT	Chinese Reminder Theorem
DCLB	Digital Contactless Bridge
DES	Data Encryption Standard; symmetric block cipher algorithm
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
EAL	Evaluation Assurance Level
EC	Elliptic Curve Cryptography
ECC	Error Correction Code
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EDU	Error Detection Unit
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMA	Electro Magnetic Analysis
FW	Firmware
Flash EEPROM	Flash Memory
HW	Hardware
IC	Integrated Circuit
ICO	Internal Clock Oscillator

ID	Identification
IMM	Interface Management Module
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
ITP	Interrupt and Peripheral Event Channel Controller
I/O	Input/Output
IRAM	Internal Random Access Memory
MED	Memory Encryption and Decryption
MMU	Memory Management Unit
NVM	Non-Volatile Memory
OS	Operating system
ST	Security Target
PEC	Peripheral Event Channel
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rives-Shamir-Adleman Algorithm
SAM	Service Algorithm Minimal
SCP	Symmetric Cryptographic Processor
SF	Security Feature
SFR	Special Function Register, as well as Security Functional Requirement, the specific meaning is given in the context
SPA	Simple Power Analysis
STS	Self Test Software
SW	Software
SO	Security Objective
TOE	Target of Evaluation
TM	Test Mode (STS)
TSF	TOE Security Functions
TRNG	True Random Number Generator
TSC	TOE Security Functions Control
TSF	TOE Security Functionality

UART	Universal Asynchronous Receiver/Transmitter
UM	User Mode (STS)
UmSLC	User Mode Security Life Control
WDT	Watch Dog Timer
XRAM	eXtended Random Access Memory
3DES	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 - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

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

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

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

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

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

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

13 Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[14].

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

[6] Security Target M7820 A11 including optional Software Libraries RSA – EC – SHA-2 – Toolbox, Version 1.5, 2012-05-07, Infineon Technologies AG

[7] Security IC Platform Protection Profile, Version 1.0, 15.06.2007, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under reference BSI-CC-PP-0035-2007

[8] Evaluation Technical Report, M7820 A11, Version 1, 2012-06-01, TÜV Informationstechnik GmbH – Evaluation Body for IT Security (confidential document)

[9] ETR for composite evaluation according to AIS 36 for the Product M7820 A11, Version 1, 2012-06-01, TÜV Informationstechnik GmbH, Evaluation Body for IT Security (confidential document)

[10] Configuration Management Scope M7820 A11 including optional Software Libraries RSA – EC – SHA-2 – Toolbox, Version 2.0, 2012-05-03, Infineon Technologies AG (confidential document)

[11] SLE70 Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface, Version 1.02.008, 2010-11-11, Infineon Technologies AG

[14] specifically

- AIS 20, Version 2.1. 02 December 2011, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 7, 30 June 2011, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 8, 08 June 20101 Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 2.1, 02 December. 2012 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, 08 June 2011, 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

[12] Crypto@2304T User Manual, 2010-03-23, Infineon Technologies AG

[13] SLE 70 Family Programmer's Reference User's Manual, 2012-03-19, Infineon Technologies AG

[14] M7801 / M7820 Controller Family for Security Applications Errata Sheet, 2012-03-28, Infineon Technologies AG

[15] SLx 70 Family Hardware Reference Manual, 2010-11-18, Infineon Technologies AG

[16] SLx70 Family Secure Hash Algorithm SHA-2 (SHA 256/224, SHA 512/384) Library Version V1.01, 2009-11, Infineon Technologies AG

[17] M7801/M7820 Controller Security Guidelines, 2012-05-07, Infineon Technologies AG

[18] SLx 70 Family Production and Personalization, 2011-10-20, Infineon Technologies AG

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

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

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

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

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

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

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

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

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

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

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

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

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

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

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

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

Table 4: 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 41

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0813-2012

Evaluation results regarding development and production environment

The IT product Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software (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 6 June 2012, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2)

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

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

Site	Address	Function
Chanhassen	Smartrac Technology US Inc. 1546 Lake Drive West Chanhassen, MN 55317 USA	Inlay Mounting
Corbeil Essones - Toppan	Toppan Photomask, Inc. European Technology Center Boulevard John Kennedy 224 91105 Corbeil Essonnes France	Mask Production
Dresden	Infineon Technologies Dresden GmbH & Co. OHG Königsbrücker Str. 180 01099 Dresden Germany	Wafer Production, Initialization and Pre-personalizaiton
Dresden-Toppan	Toppan Photomask, Inc Rähnitzer Allee 9 01109 Dresden Germany	Mask Production
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, IT
Großostheim – K&N	Infineon Technology AG DCE Kühne & Nagel Stockstädter Strasse 10 – Building 8A 63762 Großostheim Germany	Distribution Center
Hayward – K&N	Kuehne & Nagel 30805 Santana Street Hayward, CA 94544 U.S.A.	Distribution Center
Hsinchu - ARDT	Ardentec Corporation No. 3, Gungye 3rd Rd., Hsin-Chu Industrial Park, Hu-Kou, Hsin-Chu Hsien, Taiwan 30351, R.O.C. Taiwan 30351, R.O.C.	Wafer Test

Site	Address	Function
Manila - 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
Munich	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg	Development
Munich - G&D	Giesecke & Devrient GmbH Distribution Center DLC Prinzregentenstraße 159 81677 Munich Germany	Distribution Center
Ranzan - Toppan	Toppan Printing Co., Ltd. 6-2, Hanami-Dai, Ranzan-Machi, Hiki-Gun Saitama 355-0204 Japan	Inlay Mounting
Regensburg-West	Infineon Technologies AG Wernerwerkstraße 2 93049 Regensburg Germany	Module Mounting, Inlay Mounting, Distribution Center
Reichshof - SmarTrac	Smartrac Technology Germany Building RW2 Gewerbeparkstr. 10 51580 Reichshof-Wehnrath Germany	Inlay Mounting, Delivery
Round Rock - Toppan	Toppan Printing Company America, Inc. Round Rock Site 2175 Greenhill Drive Round Rock, Texas 78664	Inlay Mounting
Singapore - DHL	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, Electrical module testing
Tainan - TSMC	Taiwan Semiconductor Manufacturing Company Ltd. 1, Nan-Ke North Rd. Tainan Science Park Tainan 741-44 Taiwan	Mask & Wafer Production, Initialization and Pre-personalization

Site	Address	Function
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.