Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0732-2011

for

TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P

from

T-Systems International GmbH

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0732-2011

TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P

from	T-Systems International GmbH
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by 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, 21 December 2011

For the Federal Office for Information Security

Bernd Kowalski   L.S.
Head of Department

SOGIS IT SECURITY CERTIFIED

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 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 EAL 1 to EAL 4 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 EAL 4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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

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 component AVA_VAN.5 that is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL 4 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 TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P has undergone the certification procedure at BSI.

The evaluation of the product TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 12 December 2011. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: T-Systems International GmbH.

The product was developed by: T-Systems International GmbH.

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, where specified in the following report and in the Security Target.

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

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

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

5   Publication

The product TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

---

[7]   T-Systems International GmbH
        Untere Industriestraße 20
        57250 Netphen

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 TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P provided by T-Systems International GmbH. The TOE is a smart card with contacts implementing a secure key storage and providing a secure signature creation function for a specific card reader of type Komfort-Chipkartenleser (Cat-K) as required by the Technical Guideline TR-03119 [19]. In the following the TOE is called Signature Module for short.

The intended use of the TOE is restricted to this application in the infrastructure for the electronic identity card ePA (elektronischer Personalausweis).

The TOE provides the following cryptographic algorithms and protocols respective security features:

● Authentication of an external entity based on the PACE protocol [16].

● Encryption and authentication on a secure message channel.

● Secure digital signature creation with the stored secret key bound to the knowledge of authentication data (tSign-PIN).

● Self-protection of the TOE security functionality and the data stored inside.

During operational use phase there is only one user of the TOE, namely the card reader, whereby the Signature Module is integrated during the manufacturing of this card reader. The TOE is never used by an entity outside the terminal (card reader). The signature creation, the secure channel and the authentication based on the PACE protocol is provided to the terminal's software only. The 'Terminal Authentication' procedure requires that the terminal generates a digital signature whereby the terminal makes use of the TOE's signature application. To protect the tSign-PIN and the data to be signed all the communication between the terminal's software and the TOE is encrypted and protected by means of Secure Messaging. This secure channel is established by the well-known and proven as secure PACE protocol executed between the terminal's software and the TOE.

The TOE TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P is composed of the components

● Smart Card Security Controller SLE78CLX480P / M7820 A11 provided by Infineon Technologies AG (with specific IC dedicated software, see BSI-DSZ-CC-0640-2010, but without usage of the Infineon crypto library) and the

● Smart Card Embedded Software comprising the operating system platform TCOS (designed as native implementation) and the dedicated signature application tSign provided by T-Systems International GmbH.

The TOE's operating system platform and application and their technical functionality and inherently integrated security features are designed and developed under consideration of the specifications, standards and requirements as stated in the documents [14] to [19] respective in the Security Target [6], chapters 1.3 and 1.4.

The Security Target [6] is the basis for this certification. It is oriented on and follows the structure of the certified Protection Profiles for Electronic Identity Cards [14] and for Secure Signature Creation Devices [15] but does not claim conformance to these Protection Profiles.

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 4 augmented by AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
Access control to the User Data stored in the TOE	Control of access to user data stored by the TOE during personalisation, administration, configuration and usage of the TOE.
Secure data exchange	Set-up of trusted channels between the TOE and the external world (terminal) with respect to integrity and confidentiality.
Identification and authentication of users and components	Support of identification and authentication of users and components during personalisation, administration, configuration and usage of the TOE.
Audit	Writing of initialisation and personalisation data for audit purposes.
Generation of Random Numbers	Generation and provision of randoms for different purposes, e. g. for session key generation or for the external world (terminal).
Creation of Digital Signatures	Generation of electronic signatures as main security service of the TOE's tSign signature application for the terminal.
Management of and access to TSF and TSF-data	Management and control of the usage of the TOE's TSF and TSF data.
Reliability of the TOE security functionality	Protection of the TSF, the TSF and user data and the reliable functioning of the TSF, e. g. by integrated security mechanisms against physical probing and manipulation as well as integrated selftest functionality.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapters 3.2 to 3.4.

This certification covers the following configurations of the TOE: TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P. For details refer to chapter 8.

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:

TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P

The following table outlines the TOE deliverables:

No.	Type	Identifier	Release	Form of Delivery
1	HW/SW	Infineon Secure Smart Card Controller SLE78CLX480P with specific IC dedicated software (BSI-DSZ-CC-0640-2010) Hint: The crypto library from Infineon as covered within the HW certificate BSI-DSZ-CC-0640-2010 (RSA2048/4096 v1.1.18, EC v1.1.18 and SHA-2 v1.1) is not used by the TOE.	Mask Identifier M7820 A11 Package Type M8.4 '05 AF 0B 01 B4 21' (readable by card command FORMAT during initialisation and personalisation phase)	---
2	SW	Card operating system of TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P (implemented in ROM/EEPROM of the IC)		---
3	SW	EEPROM image of TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P including the signature application tSign	File system version '01'	---
The TOE is delivered in form of initialised modules with hardware for contact-based interface, i.e. including the IC, the operating system platform in the ROM resp. EEPROM (for patches) and the EEPROM image.				
4	DOC	TCOS Signature Module 1.0 Release 1, Administrator's Guidance, Guidance Documentation of TCOS Signature Module Version 1.0	Version 1.0.1 / 2011-07-07	Document in electronic form
5	DOC	TCOS Signature Module 1.0 Release 1, Operational Guidance, Guidance Documentation of TCOS Signature Module Version 1.0	Version 1.0.1 / 2011-07-07	Document in electronic form
6	KEY	Password (authentication key): 8 byte key individually chosen for a personalisation agent	---	Key signed and encrypted in electronic form

Table 2: Deliverables of the TOE

Basically the life-cycle of the TOE TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P consists of the development phase and the operational phase. The initialisation of the TOE completely belongs to the development phase and the TOE will be delivered in form of initialised modules to the personaliser for its personalisation. More detailed, the TOE will be delivered as an IC already embedded in a module and containing all software and data structures as defined in the specifications outlined in the Security Target [6], chapters 1.3 and 1.4. In addition, the TOE related guidance documentation as outlined in Table 2 will be provided. No modifications of the TOE by a third party are possible.

For the evaluation process the whole life-cycle of the TOE was considered during the evaluation as far as the developer respective manufacturer of the TOE is directly involved. Any delivery of TOE intermediate or final components is done via a sufficiently secure transport to avoid the delivery of fake chips.

The initialiser and personaliser can identify the TOE by retrieving the following identification data from the TOE:

- IC (chip manufacturer and type)

- Operating system platform (OS version, release number and (pre-) completion code version)

- EEPROM image data (file system version '01')

To get and verify the TOE's identification data, the user executes the card command FORMAT, for details refer to the guidance document [10]. The valid identification data can be taken from Table 2 above.

Within its operational phase, the TOE can be uniquely identified by its serial number.

3   Security Policy

The TOE is the composition of an IC and appropriate Smart Card Embedded Software and will be used as Signature Module within a specific card reader of type Komfort-Chipkartenleser (Cat-K). The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Modification and disclosure of IC assets / Smart Card Embedded Software / application data.

- Compromise, forgery and misuse of confidential user or TSF data including information leakage.

- Physical attacks through the TOE interfaces.

- Tamper detection and resistance.

- Authorisation of the import of the signature creation data (SCD).

- Misuse of the signature creation function of the TOE.

- Storage, copy and release of the SCD.

- Derivation of the SCD.

- Forgery of the DTBS-representation and the electronic signature.

- Life-cycle security.

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:

- Generation of terminal certificates.

- Authentic provision of the Signature Module by the SDSCD Provisioning Service.

- Sending of the data intended to be signed (DTBS).

- Protection of the DTBS.

- Security obligation of the Signatory.

- Personalisation of the Signature Module.

- Authentication of rightful terminals.

- Terminal operation.

The Security Objectives related to the operational environment of the TOE and its dedicated signature application tSIgn can be found in the Security Target [6], chapter 4.2.

5   Architectural Information

The TOE TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P is composed of the already certified Smart Card Security Controller SLE78CLX480P / M7820 A11 with its IC dedicated software from Infineon Technologies AG, the operating system platform and the signature application tSign from T-Systems International GmbH, see also the description of the TOE in the Security Target [6], chapters 1.3 and 1.4.

The TOE is composed of the following subsystems:

- Kernel: Management of the interfaces between all TOE components.

- Crypto-Component: Processing of the cryptographic functions.

- Admin-Component: Processing of the administrative base functions.

- IO-Component: Controlling of the input and output routines and data.

- TCOS-Type Task: APDU processing (system, applications).

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 developer tested all TOE Security Functions either on real cards or with emulator tests. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behavior including error cases. Hereby a representative sample

including all boundary values of the parameter set, e. g. all command APDUs with valid and invalid inputs were tested and all functions were tested with valid and invalid inputs. Repetition of developer tests were performed during the independent evaluator tests.

Since many Security Functions can be tested by TR-03110 [16] APDU command sequences, the evaluators performed these tests with real cards. This is considered to be a reasonable approach because the developer tests include a full coverage of all security functionality. Furthermore, penetration tests were chosen by the evaluators for those Security Functions where internal secrets of the card could maybe be modified or observed during testing. During their independent testing, the evaluators covered

● testing APDU commands related to Access Control,

● testing APDU commands related to Identification and Authentication,

● testing APDU commands related to the Secure Messaging Channel,

● testing APDU commands related to the Creation of Digital Signatures,

● testing related to verify the Reliability of the TOE,

● source code analysis performed by the evaluators,

● testing the commands which are used to execute the PACE protocol,

● testing APDU commands for the initialisation, personalisation and usage phase,

● testing APDU commands for the commands using cryptographic mechanisms.

The evaluators have tested nearly the same TOE in the certification process BSI-DSZ-CC-0677 systematically against high attack potential during their penetration testing. They have analysed the changes between the two TOEs and found no differences in the source code concerning the security functionality of the TOE.

The achieved test results correspond to the expected test results.

8   Evaluated Configuration

This certification covers the following configurations of the TOE: The TOE as a Signature Module only features one fixed configuration, the composite smart card product TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P consisting of the Infineon chip SLE78CLX480P / M7820 A11, the operating system platform TCOS and the signature application tSign from T-Systems International GmbH. This configuration cannot be altered by the user, and the evaluation is therefore only valid for this configuration of the TOE.

The TOE comprises the parts **TOE_IC**, **TOE_ES**, **TOE_APP, TOE_GD** and **Personalisation Key** as described in the following:

● **TOE_IC**: Consists of the Integrated Circuit of the Signature Module's chip (IC), the SLE78CLX480P / M7820 A11 from Infineon Technologies AG with its IC dedicated test and support software (Certification ID: BSI-DSZ-CC-0640-2010). The TOE_IC firmware contains a crypto library which is <u>not</u> used in this composite TOE.

● **TOE_ES**: The IC Embedded Software, the TCOS operating system platform.

● **TOE_APP**: The tSign signature application, i.e. its data structures and content (not including card individual data like PIN and key values).

● **TOE_GD**: The guidance documentation delivered together with the TOE (refer to [10] and [11]).

● **Personalisation Key:** Individually chosen authentication key (password) for the personalisation agent.

The TOE can be identified in its initialisation and personalisation phase by its ROM data and EEPROM file system identifier. For this case, the FORMAT card command can be used by the initialiser respective personaliser. For the valid identification data as relevant for the present TOE refer to chapter 2 above.

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 EAL 5 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:

● Application of CC to Integrated Circuits,

● Smart Card evaluation guidance,

● Application of Attack Potential to Smart Cards,

● Composite product evaluation for Smart Cards and similar devices,

● Functionality classes and evaluation methodology of physical random number generators.

(See [4], AIS 1, AIS 14, AIS 19, AIS 25, AIS 26, AIS 31, AIS 34, AIS 36, AIS 37, AIS 38.)

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

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [8] 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.

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

● All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report).

● The component AVA_VAN.5 augmented for this TOE evaluation.

As the present TOE TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P can be seen as a derivative of the already certified product TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P, refer to BSI-DSZ-CC-0677-2010 [20], re-use of specific evaluation tasks was possible.

The evaluation has confirmed:

● PP Conformance:　　None

● for the Functionality:　Product specific Security Target
　　　　　　　　　　　　Common Criteria Part 2 extended

● for the Assurance: Common Criteria Part 3 conformant
                            EAL 4 augmented by 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 following cryptographic algorithms are used by the TOE to enforce its security policy:

Algorithms for hash value calculation:

● SHA-1, SHA-224 and SHA-256 according to [18].

Algorithms for encryption and decryption:

● AES (128, 192 and 256 bit) according to [16], Appendix F.2.2.

● CMAC based on AES (128, 192 and 256 bit) according to [16], Appendix F.2.2.

Algorithms for signature generation:

● ECDSA (256, 320, 384 and 512 bit) according to [17].

This holds for the following security functions:

● Generation of digital signatures for Terminal Authentication (ECDSA).

● PACE authentication protocol with key derivation (SHA, RNG, according to [16], chapter 4.2 and Appendix A.3).

● Secure Messaging (AES, CMAC).

Random number generation e. g. for generation of session keys, for authentication protocols and for the external world (terminal) is performed by a physical random number generator provided by the underlying hardware. The rating for the PRNG is P2 with resistance against attack potential 'high' according to AIS 31 (see [4] and the certification report for the hardware BSI-DSZ-CC-0640-2010).

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). According to [16] and [17] the algorithms are suitable for signature generation, authentication protocols as well as for encryption and decryption of data (e. g. exchanged with the TOE) implemented by the TOE. The validity period of each algorithm is mentioned in the official catalogues [16] and [17].

10   Obligations and Notes for the Usage of the TOE

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

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and

techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

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.

In addition, the following aspects need to be fulfilled when using the TOE: Principally, the user has to follow the instructions in the user guidance documents [10] and [11] and has to ensure the fulfilment of the Assumptions about the environment as outlined in the Security Target [6], chapter 3.4.

Particular constraints derive from security requirements in the guidance documents [10] and [11]. The guidance documents for TOE users are separated in guidance documents for users in different roles. For preparative and personalisation procedures, the guidance document [10] was set up, for the operational phase of the TOE the guidance [11] is intended.

11 Security Target

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

12 Definitions

12.1 Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DEMA	Differential Electromagnetic Analysis
DPA	Differential Power Analysis
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital SIgnature Algorithm
ePA	elektronischer Personalausweis
ES	Embedded Software
ETR	Evaluation Technical Report
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria

ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
nPA	neuer Personalausweis
PP	Protection Profile
PRNG	Physical Random Number Generator
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Algorithm
SAR	Security Assurance Requirement
SCD	Signature Creation Data
SDSCD	Secure Digital Signature Creation Device (refer to [6], Acronyms)
SEMA	Simple Electromagnetic Analysis
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionalities

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 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

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

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

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

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

[6] Security Target BSI-DSZ-CC-0732-2011, Specification of the Security Target TCOS
Signature Module Version 1.0 Release 1/SLE78CLX480P, Version 1.0.1,
28.11.2011, T-Systems International GmbH (public document)

[7] Evaluation Technical Report TCOS Signature Module Version 1.0 Release
1/SLE78CLX480P, Version 1.0, 12 December 2011, SRC Security Research &
Consulting GmbH (confidential document)

[8] ETR for composition according to AIS36, BSI-DSZ-CC-0640-2010,
SLE78CLXxxxP/M/PS / M7820 A11, Version 4, July 2010, TÜV Informationstechnik
GmbH (confidential document)

[9] Configuration list for the TOE, Konfigurationsliste von TCOS Signature Module
Version 1.0 Release 1/SLE78CLX480P, Version 1.02, 09.12.2011, T-Systems
International GmbH (confidential document)

---

[8]specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren

- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document

- AIS 26, Version 8, 8 June 2011, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document

- AIS 31, Version 1, 25 September 2001, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren

- AIS 32, Version 7, 8 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 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

- AIS 36, Version 3, 19 October 2010, Kompositionsevaluierung including JIL Document and CC Supporting Document

- AIS 38, Version 2.9, 8 June 2011, Reuse of evaluation results

[10] TCOS Signature Module 1.0 Release 1, Administrator's Guidance, Guidance Documentation of TCOS Signature Module Version 1.0, Version 1.01, 07.07.2011, T-Systems International GmbH

[11] TCOS Signature Module 1.0 Release 1, Operational Guidance, Guidance Documentation of TCOS Signature Module Version 1.0, Version 1.01, 07.07.2011, T-Systems International GmbH

[12] Certification Report, BSI-DSZ-CC-0640-2010 for Infineon Technologies Smart Card IC (Security Controller) M7820 A11 with optional RSA2048/4096v1.1.18, EC v1.1.18 and SHA-2 v1.1 libraries and with specific IC dedicated software from Infineon Technologies AG, 28 July 2010, BSI

[13] Smartcard IC Platform Protection Profile, Version 1.0, 15.06.2007, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under BSI-CC-PP-0035-2007, 23 August 2007

[14] Common Criteria Protection Profile Electronic Identity Card (ID_Card PP), Version 1.03, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under BSI-CC-PP-0061-2009, 16 December 2009

[15] Protection Profiles for Secure Signature Creation Device - Part 2: Device with Key Generation, Version 1.03, 2009-12, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under BSI-CC-PP-0059-2009, 11 December 2009

[16] Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connec-tion Establishment (PACE), and Restricted Identification (RI), Version 2.02, Bundesamt für Sicherheit in der Informationstechnik (BSI), 09.11.2009

[17] Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 1.11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 17.04.2009

[18] Federal Information Processing Standards Publication FIPS PUB 180-2, Specifications for the Secure Hash Standard (SHS), February 2004

[19] Technische Richtlinie TR-03119: Anforderungen an Chipkartenleser mit ePA Unterstützung Version 1.1, Bundesamt für Sicherheit in der Informationstechnik (BSI), 15.12.2009

[20] Certification Report, BSI-DSZ-CC-0677-2010 for TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P from T-Systems International GmbH, 11 November 2010, BSI

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 1: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

"Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation."

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

"Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited."

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

"Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Class AVA: Vulnerability assessment (chapter 16)

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

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

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

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

This page is intentionally left blank

D   Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development
             and production environment.

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0732-2011

Evaluation results regarding development and production environment

The IT product TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P (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 21 December 2011, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1) are fulfilled for the development and production sites <u>of the TOE</u> listed below:

a)   T-Systems International GmbH, Untere Industriestraße 20, 57250 Netphen-Dreis-Tiefenbach, Germany (development and initialisation).

b)   Cardag Deutschland GmbH, An der Allee 6, 99848 Wutha-Farnroda (embedding).

For the development and production sites regarding the "Infineon Technologies Smart Card IC (Security Controller) SLE78CLX480P / M7820 A11 with optional RSA2048/4096v1.1.18, EC v1.1.18 and SHA-2 v1.1 libraries and with specific IC dedicated software" from Infineon Technologies AG refer to the certification report BSI-DSZ-CC-0640-2010 [12]. The additional maintenance procedures BSI-DSZ-CC-0640-2010-MA-01 and BSI-DSZ-CC-0640-2010-MA-02 for the underlying IC are explicitly excluded from the present certification of the composite product TCOS Signature Module Version 1.0 Release 1/SLE78CLX480P.

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

This page is intentionally left blank.