Federal Office
for Information Security

Certification Report

BSI-CC-PP-0045-2009

for

Cryptographic Modules, Security Level "Enhanced", Version 1.01

from

Bundesamt für Sicherheit in der Informationstechnik

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-CC-PP-0045-2009

Common Criteria Protection Profile

Cryptographic Modules, Security Level "Enhanced", Version 1.01

developed by Bundesamt für Sicherheit in der Informationstechnik

Assurance Package claimed in the Protection Profile:
Common Criteria Part 3 conformant
EAL 4 augmented by
ADV_IMP.2, ALC_CMC.5, ALC_DVS.2 and AVA_VAN.5

Common Criteria Recognition Arrangement for Components up to EAL 4

Common Criteria

The Protection Profile identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 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 Protection Profile 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 Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile 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, 27 February 2009
For the Federal Office for Information Security

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 as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of products which are intended to meet common consumer needs for IT security. The development and certification of a PP or the reference to an existent one gives consumers the possibility to express their IT security needs without referring to a special product. Product or system certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued.

Certification of the Protection Profile is carried out on the instigation of the BSI or a sponsor.

A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1].

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.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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) [2]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1[6]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [7]
- Procedure for the Issuance of a PP certificate by the BSI

2 Recognition Agreements

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

2.1 International Recognition of CC - Certificates

An arrangement (Common Criteria 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 February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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

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

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 PP Cryptographic Modules, Security Level "Enhanced", Version 1.01, has undergone the certification procedure at BSI.

The evaluation of the PP Cryptographic Modules, Security Level "Enhanced", Version 1.01, was conducted by the ITSEF atsec information security GmbH. The evaluation was completed on 30 September 2008. The ITSEF atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant and sponsor is: Bundesamt für Sicherheit in der Informationstechnik

The PP was developed by: Bundesamt für Sicherheit in der Informationstechnik

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

4 Validity of the certification result

This Certification Report only applies to the version of the Protection Profile as indicated.

In case of changes to the certified version of the Protection Profile, 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 Protection Profile, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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

5 Publication

The PP Cryptographic Modules, Security Level "Enhanced", Version 1.01, has been included in the BSI list of the certified Protection Profiles, which is published regularly (see also Internet: http:// www.bsi.bund.de and [3]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

---

6 Information Technology Security Evaluation Facility

7 Bundesamt für Sicherheit in der Informationstechnik, Zertifizierungsstelle, Postfach 20 03 63, 53133 Bonn, Germany

B Certification Results

The following results represent a summary of

- the certified Protection Profile,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Protection Profile Overview

The Protection Profile Cryptographic Modules, Security Level "Enhanced", Version 1.01, [4] is established by the Bundesamt für Sicherheit in der Informationstechnik as a basis for the development of Security Targets in order to perform a certification of an IT-product (TOE).

The PP describes the security requirements for cryptographic modules which provide Endorsed cryptographic security functions with secret or private cryptographic keys and is resistant against high attack potential. These Endorsed cryptographic security functions protect the confidentiality or the integrity or both of user data according to a security policy of an IT system. The TOE uses, manages and protects the cryptographic keys for these Endorsed cryptographic security functions.

The TOE is logically defined by the provided security functions depending on the implemented cryptographic algorithms and protocols. The cryptographic algorithms and protocols provide at least one of the following security functions based on cryptographic key management.

- Encryption to protect the confidentiality of information represented in ciphertext data, which are known to an attacker if only the decryption key for these data is kept confidentially. The encryption key shall be assigned to the authorized receiver of the information and in case of asymmetric cryptographic algorithm may be public.
- Decryption to support the protection in confidentiality of information represented in ciphertext data. The decryption key for these data shall be kept confidentially.
- Digital signature creation to support the services origin authentication, data integrity, and non-repudiation for the signed data to the signer. The signature-creation key shall be kept private.
- Digital signature verification, which allow to detect any modification of the signed data and to proof the origin and the integrity of unmodified signed data. The signature verification key shall be authentically assigned to the holder of the signature-creation key and may be public available to the verifier.
- Generation and the verification of Message Authentication Codes to detect modification of the related data by anybody not knowing the message authentication key used for the Message Authentication Code of these data.
- Prove of its own identity to an external entity based on the knowledge of a private key without revealing this secret to the verifier.
- Verification of the identity of an external entity based on a public key assigned to this entity.

The TOE manages the cryptographic keys necessary for its implemented cryptographic algorithms and protocols. The cryptographic key management controls the access and the use of the cryptographic keys by the Endorsed cryptographic functions. The cryptographic key management includes at least one of the following techniques:

- Generation of cryptographic keys using a random number generator and implementing the key generation algorithms depending on the intended use of the keys.
- Import of cryptographic keys in encrypted form or cryptographic key components using split-knowledge procedures.
- Key agreement protocols establishing common secrets with external entities.

The TOE may export cryptographic keys to authorized external entities while protecting the confidentiality and the integrity as required for the intended use of the cryptographic key.

In many cases the mutual authentication of communicating entities and the key agreement are combined to initiate secure communication between trusted parties protecting the confidentiality and integrity of the transmitted data.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [4], chapter 3.1. Based on these assets the security environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Protection Profile [4], chapter 3.2, 3.3 and 3.4.

These Assumptions, Threats and Organisational Security Policies are split into Security Objectives to be fulfilled by a TOE claiming conformance to this PP and Security Objectives to be fulfilled by the IT-Environment of a TOE claiming conformance to this PP. These objectives are outlined in the PP [4], chapter 4.

The Protection Profile [4] requires a Security Target based on this PP or another PP claiming this PP, to be fulfil the CC Requirements for strict conformance.

2 Security Functional Requirements

Based on the Security Objectives to be fulfilled by a TOE claiming conformance to this PP the security policy is expressed by the set of Security Functional Requirements to be implemented by a TOE. It covers the following issues:

- Key Management,
- Cryptographic Operation,
- Mode Transition,
- Red-Black Separation,
- Audit and
- Physical Protection

These TOE Security Functional Requirements (SFR) are outlined in the PP [4], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the SFR claim is called:

Common Criteria Part 2 extended

3 Assurance Requirements

The TOE security assurance package claimed in the Protection Profile is based entirely on the assurance components defined in part 3 of the Common Criteria. Thus, this assurance package is called:

Common Criteria Part 3 conformant
EAL 4 augmented by
ADV_IMP.2, ALC_CMC.5, ALC_DVS.2 and AVA_VAN.5

(for the definition and scope of assurance packages according to CC see part C or [1], part 3 for details).

4 Results of the PP-Evaluation

The Evaluation Technical Report (ETR) [5] was provided by the ITSEF according to the Common Criteria [1], the Methodology [6], the requirements of the Scheme [2] and all interpretations and guidelines of the Scheme (AIS) [7] as relevant for the TOE.

As a result of the evaluation the verdict PASS is confirmed for the assurance components of the class APE.

The following assurance components were used:

APE_INT.1 PP introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

The results of the evaluation are only applicable to the Protection Profile as defined in chapter 1.

5 Obligations and notes for the usage

The following aspects need to be fulfilled when using the Protection Profile:

none

6 Protection Profile Document

The Protection Profile Cryptographic Modules, Security Level "Enhanced", Version 1.01, [4] is being provided within a separate document as Annex A of this report.

7 Definitions

7.1 Acronyms

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

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CSP Critical Security Parameter

EAL Evaluation Assurance Level

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SF Security Function

SFP Security Function Policy

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functions

7.2 Glossary

Administrator - An authorized user who has been granted the authority to manage the TOE. These users are expected to use this authority only in the manner prescribed by the guidance given to them.

Augmentation - The addition of one or more requirement(s) to a package.

Authentication interface/port - Data interface respective port used for input of confidential authentication data.

Authentication keys - General term for keys used for authentication of data (i.e. Data authentication keys) or the identity of an entity (i.e. Entity authentication keys)

Authentication reference keys - Private key for proof of their own identity claimed in an asymmetric authentication protocol

Authentication verification keys - Public Key assigned to a claimed identity of an entity for verification of the knowledge of a private key by means asymmetric authentication protocol

Automated key transport - The transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols).

Backup data - User data and TSF data of the TOE that are integrated in a backup file.

Backup key components - Cryptographic key components that are used for the encryption of confidential backup data, e.g., for the encryption of cryptographic keys and other critical security parameters.

Black data - Cryptographically protected user data representing user information. If this information needs protection in confidentiality the data shall be encrypted. If this information needs protection in integrity a cryptographic MAC or digital signature shall be associated with this data to detect modification.

Bypass mode - Mode of operation in which the cryptographic module provides services without cryptographic processing (e.g., transferring plaintext through the cryptographic module).

Bypass state - State related to the bypass mode in the Finite state model (cf. ADV_ARC.1).

Compromise - The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs).

Confidentiality - The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

Control input interface/port - Interface respective port intended for all input commands, signals, and control data (including function calls and manual controls such as switches, buttons, and keyboards) used to control the operation of a cryptographic module shall enter via the “control input” interface.

Critical security parameter (CSP) - Security-related information (e.g., secret and private cryptographic keys, and TSF data like authentication data) whose disclosure or modification can compromise the security of a cryptographic module.

Critical TSF - TSF that, upon failure, could lead to (i) the disclosure of secret keys, private keys, or CSPs or (ii) modification of public root keys. Examples of the critical functionality

include but are not limited to random number generation, operation of the cryptographic algorithm, and cryptographic bypass.

Crypto officer - An authorized user who has been granted the authority to perform cryptographic initialization and management functions (including key management) cryptographically unprotected data in the red area of the IT system. These users are expected to use this authority only in the manner prescribed by the guidance given to them. (The “cryptographic administrator” is some times called “crypto officer” in the guidance documentation) (the same as Cryptographic administrator)

Cryptographic algorithm - A well-defined computational procedure that takes variable inputs that usually includes a cryptographic key and produces an output, e.g., encryption, decryption, a private or a public operation in a dynamic authentication, signature creation, signature verification, generation of hash value.

Cryptographic boundary - An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

Cryptographic checksum - A checksum that is created by performing a cryptographic algorithm. The cryptographic checksum can be associated with the original data in order to provide a mechanism to verify that the original data has not been changed.

Cryptographic functions - TSF implementing cryptographic algorithms and/or protocols for encryption and decryption, signature creation or verification, calculation of Message Authentication Code, entity authentication or key management.

Cryptographic key (key) - A parameter used in conjunction with a cryptographic algorithm that determines the transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, a digital signature computed from data, the verification of a digital signature computed from data, a Message Authentication Code computed from data, a proof of the knowledge of a secret, a verification of the knowledge of a secret or an exchange agreement of a shared secret.

Cryptographic key component (key component) - A parameter used in conjunction with other key components in an Endorsed security function to form a plaintext cryptographic key by a secret sharing algorithm (e.g., the cryptographic plaintext key is the xor-sum of two key components)

Cryptographic module - The set of hardware, software, and/or firmware that implements Endorsed security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Cryptographic protocol - A cryptographic algorithm including interaction with an external entity (e.g., key exchange)

Data input interface/port - Interface respective port intended for all data (except control data entered via the control input interface) that is input to and processed by the cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and status information from another entities).

Data output interface/port - Interface respective port intended for all data (except status data output via the status output interface) that is output from the cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and control information for another entity).

Data path - The physical or logical route over which data passes; a physical data path may be shared by multiple logical data paths.

Decryption algorithm - Algorithm of decoding a cipher text into the plaintext using a decryption key. The decryption algorithm reproduces the plaintext which where used to

calculate the cipher text with the corresponding encryption algorithm and the corresponding encryption key .

Destruction of data - A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.

Differential power analysis (DPA) - An analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm.

Digital signature - The result of a asymmetric cryptographic transformation of data which, when properly implemented, provides the services of 1. origin authentication, 2. data integrity, and 3. signer non-repudiation.

Electromagnetic compatibility (EMC) - The ability of electronic devices to function satisfactorily in an electromagnetic environment without introducing intolerable electromagnetic disturbances to other devices in that environment.

Electromagnetic emanation analysis (EMEA) - Analysis of electromagnetic emissions from a device, equipment, or system to gain information about its internal secrets or processes

Electromagnetic interference (EMI) - Electromagnetic emissions from a device, equipment, or system that interfere with the normal operation of another device, equipment, or system.

Electronic key entry - The entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The user of the key may have no knowledge of the value of the key being entered.)

Encrypted key - A cryptographic key that has been encrypted using an Endorsed security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.

Encryption algorithm - Algorithm of processing a plaintext into a ciphertext using a encryption key in a way that decoding of the cipher text into the plain text without knowledge of the corresponding decryption key is computationally infeasible.

End User - An authorized user assumed to perform general security services, including cryptographic operations and other Endorsed security functions.

Endorsed - For this protection profile, endorsed by the certification body for the evaluation of products of an intended type and resistance against attacks with attack potential addressed by the vulnerability analysis component in the security target.

Endorsed mode of operation - For this protection profile, a operational mode of the cryptographic module that employs only Endorsed security functions (e.g., installation, start-up, normal operation, maintenance; not to be confused with a specific mode of an Endorsed security function, e.g., DES CBC mode)

Endorsed security function - For this protection profile, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either a) specified in an Endorsed standard, b) adopted in an Endorsed standard and specified either in an appendix of the Endorsed standard or in a document referenced by the Endorsed standard, or c) specified in the list of Endorsed security functions.

Environmental failure protection (EFP) - The use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions or fluctuations outside of the module's normal operating range.

Environmental failure testing (EFT) - the use of testing to provide a reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions or fluctuations outside of the mod'le's normal operating range.

Error detection code (EDC) - A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

Error mode - Mode of operation when the cryptographic module has encountered an error condition as defined in FPT_FLS.1 (term is used for description of the Mode transition SFP).

Error state - State related to the Error mode in the Finite state model (cf. ADV_ARC.1).

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.

Firmware - The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) and cannot be dynamically written or modified during execution.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Hardware - The physical equipment used to process programs and data.

Hash-based message authentication code (HMAC) - A message authentication code that utilizes a keyed hash.

Higher Order Side Channel Analysis - A side channel analysis that additionally analyzes the masking of a device, equipment, or system in order to gain information about its internal secrets or processes.

Informal - Expressed in natural language.

Information processing - The organisation, manipulation and distribution of information.

Initialization vector (IV) - A vector used in defining the starting point of an encryption process within a cryptographic algorithm.

Input data - Information that is entered into a cryptographic module for the purposes of transformation or computation using an Endorsed security function.

Integrity - The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Internal secrets - Confidential data inside the cryptographic boundary not intended for export (e.g., secret or private plaintext keys, authentication reference data).

IT system - For this protection profile, an IT system using the TOE to protect user data during transmission over or storage on media to which unauthorised user have access to.

Key-CSP entry mode - Mode of operation in which cryptographic keys and CSPs enter the cryptographic module.

Key-CSP entry state - State related to the Key-CSP entry mode in the Finite state model (cf. ADV_ARC.1).

Key encrypting key - A cryptographic key that is used for the encryption or decryption of other keys.

Key establishment - The process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).

Key interface/port - Data interface respective port used for the input and output of plaintext cryptographic key components and CSPs.

Key loader - A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.

Key management - The activities involving the handling of cryptographic keys and other related security parameters (e.g., Ivs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.

Key material - Any media storing key components or keys for offline key exchange.

Key transport - Secure transport of cryptographic keys from one cryptographic module to another module.

Key usage type - Type of cryptographic algorithm a key can be used for (e.g., DES encryption, TDES MAC calculation, signature-creation with RSA PKCS#1 v1.5).

Logical external interface - A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals (see also the term “port” for the physical aspects of a logical external interface). In the CC terminology it covers all logical external interfaces of the TOE (direct or indirect interfaces to the TSF or interfaces to the non-TSF portion of the TOE, cf. CEM paragraph 529 for details).

Non-operational CSP - CSP used only for self test (e.g., for known answer tests) and maintenance operation (e.g., to test the operation of the cryptographic module after software update or repairing hardware components). Non-operational must not be used for protection of user the confidentiality or integrity of data by cryptographic operation.

Maintenance mode - Mode of operation for maintaining and servicing a cryptographic module, including physical and logical maintenance testing.

Maintenance state - State related to the Maintenance mode in the Finite state model (cf. ADV_ARC.1).

Manual key entry - The entry of cryptographic keys into a cryptographic module, using devices such as a keyboard.

Manual key transport - Non-electronic means of transporting cryptographic keys.

Masking - Computational process of adding random numbers to data in order to protect the confidentiality of the data against side channel analysis.

Message authentication with appendix - A digital signature scheme which requires the message as input to the verification algorithm. The signature is attached to the message

Message authentication with message recovery - A digital signature scheme with message recovery is a digital signature scheme for which a priori knowledge of the message is not required for the verification algorithm.

Microcode - The elementary processor instructions that correspond to an executable program instruction.

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operating conditions - Any environmental condition being accidental or induced outside of the normal range intended for the TOE may affect the correct operation or compromise of confidential information. These conditions include but are not limit to voltage of power supply, temperature, emanation which TOE environmental conditions.

Operational CSP - CSP used for protection of user the confidentiality or integrity of data by cryptographic operation.

Output data - Data containing information that is produced from a cryptographic module.

Password - A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Personal identification number (PIN) - An alphanumeric code or password used to authenticate an identity.

Permanent stored keys - Keys remains stored in the TOE after power off or reset.

Physical protection - The safeguarding of a cryptographic module, cryptographic keys, or CSPs using physical means.

Plaintext key - An unencrypted cryptographic key.

Port - A physical input or output interface of a cryptographic module that provides access to the module for physical signals, represented by logical information flows. Physically separated ports do not share the same physical pin or wire. In the CC terminology a port is a physical external interface of the TOE (direct or indirect interface to the TSF or interface to the non-TSF portion of the TOE, cf. CEM paragraph 529 for details).

Power interface/port - Interface respective port providing all external electrical power supply.

Power On/Off mode - Mode of operation that indicates whether the cryptographic module is supplied by a power source. These modes may distinguish between different power sources (e.g., primary, secondary, backup power source or none) being applied to a cryptographic module.

Power On/Off state - State related to the Power On/Off mode in the Finite state model (cf. ADV_ARC.1).

Private key - A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.

Protection Profile - An implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.

Public key - A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public.

Public key (asymmetric) cryptographic algorithm - A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.

Public key certificate - A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity.

Random Number Generator - Random Number Generators (RNGs) used for cryptographic applications produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are three basic classes physical true RNG, non-physical true RNG, and deterministic RNG. A physical true RNG produces output that dependents on some physical random source inside the TOE boundary only. A non-deterministic true RNG gets its entropy from sources from outside the TOE boundary

(e.g., by system data like RAM data or system time of a PC, output of API functions etc. or human interaction like key strokes, mouse movement etc.). A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial random value (seed).

Reference authentication data - Data known for the claimed identity and used by the TOE to verify the verification authentication data provided by an entity in an authentication attempt to prove their identity.

Red data - Cryptographically unprotected user data representing user information which need protection in confidentiality and / or integrity.

Removable cover - A cover designed to permit physical access to the contents of a cryptographic module.

Reset - Action to clear any pending errors or events and to bring a system to normal condition or initial state (e.g., after power-up).

Secret key - A cryptographic key, used with a secret key cryptographic algorithm, that is uniquely associated with one or more entities and should not be made public.

Secret key (symmetric) cryptographic algorithm - A cryptographic algorithm which keys for both encryption and decryption respective MAC calculation and MAC verification are the same of can easily be derived from each other and therefore must be kept secret.

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

Seed key - A secret value used to initialize a cryptographic function or operation.

Self-test mode - Mode of operation in which the cryptographic module performs initial start-up self-test, self-test at power-up, self-test at the request of the authorised user and may perform other self-tests identified in FPT_TST.2.6.

Self-test state - State related to the Self-test mode in the Finite state model (cf. ADV_ARC.1).

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

Shutdown - Shutdown of the TOE initiated by the user (may not include reset after detection of error or power-off due to loss of power supply).

Side Channel Analysis - Class of passive attacks exploiting the physical emanation of a device, equipment, or system in order to gain information about its internal secrets or processes.

Signature-creation key - Private key for the creation of digital signatures

Signature-verification key - Public key for the verification of digital signatures

Simple power analysis (SPA) - A direct analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys.

Software - The programs and data components, usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution.

Split knowledge - A process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.

Status information - Information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or modes of the module.

Status output interface/port - Interface respective port intended for all output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of a cryptographic module.

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

System software - The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data.

Tamper detection - The automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module.

Tamper evidence - The external indication that an attempt has been made to compromise the physical security of a cryptographic module. (The evidence of the tamper attempt should be observable by an user subsequent to the attempt.)

Tamper response - The automatic action taken by a cryptographic module when a tamper detection has occurred (the minimum response action is the desctruction of plaintext keys and CSPs).

Target of Evaluation (TOE) - An information technology product or system and associated administrator and user guidance documentation that is the subject of an evaluation.

TEMPEST - A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. Note, TEMPEST is not limited to electromagnetic emanation.

Template Attack - Multivariate side channel analysis of the power or electromagnetic emission from a device, equipment, or system to gain information about its internal secrets or processes.

Timing analysis - Analysis of timing behaviour of a device, equipment, or system to gain information about its internal secrets or processes

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

TOE Security Functions (TSF) - A set of the TOE consisting of all hardware, software, and firmware that must be relied upon for the correct enforcement of the TOE Security Policy.

TOE security functions interface (TSFI) - A set of interfaces, whether interactive (man-machine interface) or machine (machine-machine interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected, and distributed within a Target of Evaluation.

Trusted channel - A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted path - A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

Unauthenticated User - An identified user not being authenticated and having rights as identified in the component FIA_UAU.1.

Unauthorized user - A user who may obtain access only to system provided public objects if any exist.

Unidentified User - A user not being identified and having rights as identified in the component FIA_UID.1

User - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE (includes both authorized and unauthorized entities).

User Mode - Mode of operation in which the cryptographic module performs security services, cryptographic operations, and other functions at the request of the authorised user.

User State - State related to the User mode in the Finite state model (cf. ADV_ARC.1).

Verification authentication data - Data provided by an entity in an authentication attempt to prove their identity to the TOE.

8 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

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

[3] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[4] Common Criteria Protection Profile Cryptographic Modules, Security Level "Enhanced", Version 1.01, July 24, 2008, BSI

[5] Evaluation Technical Report, Version, Version 1.1, September 30, 2008, atsec information security GmbH (confidential document)

[6] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

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

[8] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[9] NIST: FIPS PUB 186-2 Digital signature standard (DSS), January 27, 2000, with Change Notice 1, October 2001

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

“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 A.

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
AGD:	AGD_OPE.1 Operational user guidance

Assurance Class	Assurance Components
Guidance documents	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	2	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: Protection Profile Cryptographic Modules, Security Level "Enhanced", Version 1.01, [4] is provided within a separate document.

This page is intentionally left blank.