# Certification Report

**Bundesamt für Sicherheit in der Informationstechnik**

## BSI-DSZ-CC-0373-2007

for

## PhenoStor® Card Reader GRE100010

from

## Bayer Innovation GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

**Deutsches IT-Sicherheitszertifikat**

erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI
Bundesamt für Sicherheit
in der Informationstechnik

**BSI-DSZ-CC-0373-2007**

## PhenoStor® Card Reader GRE100010

from

## Bayer Innovation GmbH

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3* (ISO/IEC 15408:2005) for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

**Evaluation Results:**

| | |
|---|---|
| Functionality: | **Product specific Security Target**<br>**Common Criteria Part 2 extended** |
| Assurance Package: | **Common Criteria Part 3 conformant**<br>**EAL 3** |

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 09. März 2007

The President of the Federal Office
for Information Security

IT Security Certified
SOGIS - MRA

Dr. Helmbrecht L.S.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

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.

# 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 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)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

[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 7 July 1992, Bundesgesetzblatt I p. 1230

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

[5] Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

# 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

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

## 2.2 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 (CC-MRA). 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

# 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 PhenoStor® Card Reader GRE100010 has undergone the certification procedure at BSI.

The evaluation of the product PhenoStor® Card Reader GRE100010 was conducted by T-Systems GEI GmbH. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Bayer Innovation GmbH
Merowingerplatz 1
40225 Düsseldorf

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 09. März 2007.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

# 4 Publication

The following Certification Results contain pages B-1 to B-22.

The product PhenoStor® Card Reader GRE100010 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Bayer Innovation GmbH
Merowingerplatz 1
40225 Düsseldorf

# 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.

# Contents of the certification results

# 1 Executive Summary

The Target of Evaluation (TOE) is the PhenoStor® Card Reader GRE100010.

The TOE is a card reader device for holographic memory cards providing the functionality of reading data from a holographic storage card and securely transmitting the data to the interface unit connected to the card reader.

The TOE basically consists of an optical module for reading out data from a holographic memory card, a standard microcontroller with dedicated software for the main control of the card reader as well as the STMicroelectronics ST19WP18-D security controller with its dedicated software and embedded software running on ST19WP18-D.

The TOE physically reads sensitive data that is symmetrically encrypted and MACprotected or symmetrically encrypted and digitally signed from a PhenoStor® holographic card and sends the data to the Interface Unit (IU), which is out of the evaluation scope. The IU decides which data is needed for the application. If this data is cryptographically protected, it is sent to the TOE where it is decrypted and its signature (or MAC) is verified. Then the data is sent to the IU through a secure communication channel.

All the cryptographic keys on the TOE can be updated by the administrator (through the Administrator Unit (AU)) at any time in the end user phase. The security of the card reader is based upon the STMicroelectronics ST19WP18-D which is a smartcard integrated circuit with its dedicated software certified in compliance with Common Criteria 2.2, EAL5 augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 and in accordance with Smartcard IC Platform Protection Profile BSI-PP-0002-2001 [9] and Protection Profile Smartcard Integrated Circuit PP/9806 [10]. The cryptographic functionality of the certified cryptographic library (3DES, RSA, SHA-1) of ST19WP18-D is used for protecting the communication within the TOE, and for the secure communication channel between the TOE and IU and between the TOE and the administrator’s device, respectively.

Additionally, the data on the holographic memory card can be analogue scrambled but the analogue scrambling is neither part of the security functionality nor analysed during the evaluation.

The IT product PhenoStor® Card Reader GRE100010 was evaluated by T-Systems GEI GmbH. The evaluation was completed on 21. Dezember 2006. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Bayer Innovation GmbH
Merowingerplatz 1
40225 Düsseldorf

[8] Information Technology Security Evaluation Facility

## 1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL 3 (Evaluation Assurance Level 3 - methodically tested and checked).

## 1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

| **Security Functional Requirement** | **Addressed issue** |
|---|---|
| **FCS** | **Cryptographic support** |
| FCS_CKM.1 | Cryptographic key generation |
| FCS_CKM.4 | Cryptographic key destruction |
| FCS_COP.1 | Cryptographic operation |
| **FDP** | **User data protection** |
| FDP_ACC.2 | Complete access control |
| FDP_ACF.1 | Security attribute based access control |
| FDP_ETC.2 | Export of user data with security attributes |
| FDP_ITC.1 | Import of user data without security attributes |
| FDP_RIP.1 | Subset residual information protection |
| FDP_SDI.2 | Stored data integrity monitoring and action |
| FDP_UCT.1 | Basic data exchange confidentiality |
| FDP_UIT.1 | Data exchange integrity |
| **FIA** | **Identification and authentication** |
| FIA_UAU.1 | Timing of authentication |
| FIA_UID.1 | Timing of identification |
| **FMT** | **Security Management** |
| FMT_MSA.1 | Management of security attributes |
| FMT_MSA.2 | Secure security attributes |
| FMT_MTD.1 | Management of TSF data |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security roles |
| **FPT** | **Protection of the TOE Security Functions** |
| FPT_FLS.1 | Failure with preservation of secure state |

| Security Functional Requirement | Addressed issue |
|---|---|
| FPT_PHP.3 | Resistance to physical attack |
| FPT_TST.1 | TSF testing |
| FPT_SEP.1 | TSF domain separation |
| **FTP** | **Trusted path / channel** |
| FTP_ITC.1 | Inter-TSF trusted channel |

Table 1: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

| Security Functional Requirement | Addressed issue |
|---|---|
| **FCS** | **Cryptographic support** |
| FCS_RND.1 | Quality metric for random numbers |
| **FPT** | **Protection of the TOE Security Functions** |
| FPT_EMSEC.1 | TOE Emanation |

Table 2: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [7] chapter 5.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

| Security Functional Requirement | Addressed issue |
|---|---|
| **FCS** | **Cryptographic support** |
| FCS_CKM.1 | Cryptographic key generation |
| FCS_CKM.4 | Cryptographic key destruction |
| FCS_COP.1 | Cryptographic operation |
| **FDP** | **User data protection** |
| FDP_UCT.1 | Basic data exchange confidentiality |
| FDP_UIT.1 | Data exchange integrity |
| FDP_ITC.2 | Import of user data with security attributes |
| **FTP** | **Trusted path/channels** |
| FTP_ITC.1 | Inter-TSF trusted channel |

Table 3: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [7] chapter 5.3.

These Security Functional Requirements are implemented by the TOE Security Functions:

| TOE Security Function | Addressed issue |
|---|---|
| SF.1 | Trusted channel with confidentiality, integrity and authenticity |
| SF.2 | TOE state integrity protection during and after interruption of the normal procedure |
| SF.3 | Decryption and verification of encrypted A.ProtectedData |
| SF.4 | Protection against unauthorized personalization |
| SF.5 | Access denial |
| SF.6 | Protection against unauthorized change of keys |
| SF.7 | Protection against unauthorized access to decrypted A.ProtectedData |
| SF.8 | Generation of random numbers |
| SF.9 | Key derivation functions (KDFs) |
| SF.10 | Security domain |

Table 4: Security Functions

For more details please refer to the Security Target [7], chapter 6.1.

## 1.3 Strength of Function

The TOE's strength of functions is claimed 'medium' (SOF-medium) for specific functions as indicated in the Security Target [7], chapter 6.1.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

## 1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The assets to be protected by the TOE consist of user data and symmetric keys. They are denoted by:

A.ProtectedData: the user data;

A.SymkeyData: the symmetric key used for decrypting and MAC checking the data from a PhenoStor® card;

A.PubkeySignature: the public key for checking the signature of the data from a PhenoStor® card;

A.SymkeyIU: the symmetric key used for securing communication between the security controller and the IU;

A.SymkeyRNG: used in the creation of the initial state of the deterministic random number generator;

A.SymkeyAdmin: the symmetric key used by the administrator for updating A.SymkeyData, A.SymkeyIU, A.SymkeyAdmin, A.PubkeySignature

All the assets have to be protected against manipulation and disclosure within the TOE, i.e. the confidentiality, integrity and authenticity of the data has to be ensured by the TOE.

The TOE has to resist against the following threats:

T1: An attacker could try to manipulate A.ProtectedData on its way from the holographic memory card through the TOE to the IU or from the IU to the place in TOE where its processing starts, in order to provide the TOE with manipulated decrypted A.ProtectedData.

T2: An attacker could try to reveal or manipulate A.ProtectedData, A.SymkeyData, A.SymkeyIU, A.SymkeyRNG, A.SymkeyAdmin or to manipulate A.PubkeySignature by manipulating the program execution or the program code in the TOE (e.g. buffer overflow or glitches).

T3: An attacker could try to get information about A.ProtectedData, A.SymkeyData, A.SymkeyIU, A.SymkeyRNG, A.SymkeyAdmin through sidechannel attacks (active and passive) on the TOE.

T4: An attacker could try to manipulate A.ProtectedData, A.SymkeyData, A.SymkeyIU, A.SymkeyRNG, A.SymkeyAdmin, A.PubkeySignature through active physical attacks on the TOE.

T5: After its processing within the TOE, A.ProtectedData is about to be transmitted to the IU. An attacker could try to reveal or manipulate A.ProtectedData during this transmission as well as to generate manipulated A.ProtectedData and provide the IU with it on behalf of the TOE.

T6: An attacker could try to exchange the IU against some other device (with some key known to him) in order to obtain A.ProtectedData.

T7: An attacker could try to reveal or manipulate A.SymkeyData, A.SymkeyIU, A.SymkeyRNG, A.SymkeyAdmin or manipulate A.PubkeySignature on their way from the administrator to the place of their final storage within the TOE.

T8: An attacker could try to exchange the administrator’s device against some other device (with some key known to him) in order to manipulate (e.g. exchange) A.SymkeyData, A.SymkeyIU, A.SymkeyRNG, A.SymkeyAdmin, A.PubkeySignature in the TOE.

T9: An attacker could try to reveal or manipulate A.ProtectedData, A.SymkeyData, A.SymkeyIU, A.SymkeyRNG, A.SymkeyAdmin or to manipulate A.PubkeySignature by using the TOE personalization interface to manipulate program code or data.

The following OSPs are defined for the TOE:

P1: Procedures for the development, design, implementation and testing as required in the ST19WP18-D Security Target [15], which states an augmentation and refers to the Protection Profiles BSI-PP-0002-2001 [9] and PP/9806 [10], shall be applied.

P2: Procedures for the manufacturing, delivery and storage as required in the ST19WP18-D Security Target [15], which refers to the Protection Profiles BSI-PP- 0002-2001 [9] and PP/9806 [10], shall be applied.

## 1.5 Special configuration requirements

The TOE will be operated in only one configuration that will be set up by the manufacturer before delivery. All necessary administrative actions that have to be taken before the usage of the TOE are described in the „Administrator-Sicherheitshandbuch“ [11].

## 1.6 Assumptions about the operating environment

The following assumptions are defined for the TOE environment:

| Identifier | Definition |
|---|---|
| AE1 | Data stored on a PhenoStor® card is protected |
| AE2 | All used keys are cryptographically strong |
| AE3 | All keys used in the environment are protected against manipulation and disclosure |
| AE4 | All random numbers in the environment used for cryptographic purposes are cryptographically good. |
| AE5 | A.ProtectedData is protected against disclosure and manipulation |
| AE6 | The IU verifies that the TOE knows A.SymkeyIU before accepting data received from the TOE |
| AE7 | The administrator’s device verifies that the TOE knows the current A.SymkeyAdmin before sending data to the TOE |

Table 5: Assumptions for the TOE environment

Note: Only the titles of the assumptions are provided. For more details please refer to chapter 4 of this report or the Security Target [7], chapter 3.2.

## 1.7 Disclaimers

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

**Phenostor® Card Reader GRE100010.**

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Date | Form of Delivery |
|---|---|---|---|---|---|
| 1 | HW /SW | PhenoStor® Card Reader GRE100010 | Version 1.1 | See below | personally or by delivery company |
| 2 | DOC | Benutzer-Sicherheitshandbuch, (AGD_USR.1), PhenoStor® [12] | Version 1.1 | 21.09.2006 | encrypted and signed via email or postal on storage media |
| 3 | DOC | Administrator-Sicherheitshandbuch mit Installation, Generierung und Anlauf (ADO_IGS.1 und AGD_ADM.1), PhenoStor® [11] | Version 1.3 | 27.10.2006 | encrypted and signed via email or postal on storage media |
| 4 | Keys | Relevant (customer specific) keys (at least the A.SymkeyAdmin for personalisation) | - | - | encrypted and signed via email or postal on storage media |

Table 6: Deliverables of the TOE

The TOE Phenostor® Card Reader GRE100010 consists of hard- and software.

The hardware consists of

- the PhenoStor® boards version 1.1 labelled as phenostor-mbX-v1.1-Y, where X denotes the individual number of a PhenoStor® board and Y is the date of its receipt. Each board mainly consists of the Atmel ATmega128 controller, optical module, Ethernet interface, serial port interface, keyboard, display and non-intelligent hardware components incl. the plastic case and
- the PhenoStor® ST19WP18-D TSSOP28 controllers version 1.0 labelled as phenostor-tssopX-v1.0-Y, where denotes the individual number of the received reel and Y is the date of its receipt.

The software consists of

- com.zip #7 is the COM module running on the standard controller (25.08.2006, p. 5 of [14]);
- esc.zip #16 is the ESC module running on the standard controller (21.08.2006, p. 5 of [14]);
- bootloader.zip #4 contains the bootloader software (18.10.2006, p. 17 of [14]);
- secmodule.zip #4 contains the SEC module (SEC_ROM / SEC_EEPROM) (18.10.2006, p. 18 of [14]).

A card reader is delivered from the developer escrypt GmbH to the distributer Bayer Innovation GmbH or to the integrator of the project for delivery to the end user, or it is delivered directly to the end user. The delivery can be done by delivery companies or personally. The integrator and the end user, respectively, shall verify the integrity of the security relevant part of the card reader after delivery. For this purpose they shall check whether the card reader has knowledge of the secret keys transferred in parallel over a secure channel to the end user as described below (e.g., by checking whether the card reader is able to decrypt a message encrypted with the appropriate secret key).

The relevant keys, the administrator security guide and the user security guide are sent to the end user by trusted delivery. One possibility is the usage of PGP or a similar software between escrypt GmbH and the end user such that all data is transmitted encrypted and digitally signed, another way is the delivery in an encrypted and digitally signed manner on a storage medium (e.g. a CD) by delivery companies, a third way is personal delivery. When using software for encrypting and signing the data such as PGP, it has to be made sure that the keys are authentic. Hence, the fingerprint must be verified by phone or the keys must be exchanged personally.

An alternative way of delivery is to trust Bayer Innovation GmbH or the project integrator and to deliver the keys and the security guides on a storage medium to Bayer Innovation GmbH or the project integrator in a secure manner as described above. Bayer Innovation GmbH then stores the keys and the security guides in a secure environment providing confidentiality and integrity. For instance, the keys can be stored on a CD that is locked away in a safe, or the keys are stored on a secure PC with encrypted hard disk and user authentication that is not connected to a computer network.

It is ensured that the delivery of the keys plus security guidelines on the one hand and the card reader on the other hand is performed separately. In case of improper delivery, appropriate corrective actions are performed, even considering sending a new card reader, if necessary.

The card readers and the delivered storage media carry the complete name of the TOE including the version number such that the end user knows that he received the correct items. The assembling step within escrypt GmbH is supervised by the development officer, the completeness of the TOE and the correctness of the procedures is always verified and all necessary details of each delivery activity are carefully documented.

After receipt of the TOE the administrator has to load the keys into the TOE. This procedure is described in the „Administrator-Sicherheitshandbuch“ [11].

# 3 Security Policy

The TOE is a holographic memory card reader and is designed for handling any kind of confidential and manipulation sensitive information, which is stored on a mobile storage medium and has to be processed digitally. The security policy of the TOE is to protect sensitive data from disclosure and manipulation while transferring it from a PhenoStor® holographic card through the TOE to the IU. Data stored on the card is encrypted and signed (or MACprotected) and, therefore, cannot be read or undetectably modified without knowing the corresponding keys. The corresponding keys are stored safely in the security controller of the TOE, which is able to decrypt data and to verify signatures (and MACs), but which transfers decrypted data solely via trusted channels.

# 4 Assumptions and Clarification of Scope

## 4.1 Usage assumptions

The following assumtions regarding the usage of the TOE have to be fulfilled:

AE1: The user marks as protected, digitally signs (or MAC-protects) and encrypts all the data that is to be stored on a PhenoStor® card and that he wants to be protected (i.e. the A.ProtectedData).

AE3: All the keys A.SymkeyData, A.SymkeyIU, A.SymkeyRNG, A.SymkeyAdmin, PrivkeySignature in the environment (administrator, interface unit, card writer) are protected against manipulation and disclosure. The key A.PubkeySignature is protected against manipulation. The IU knows A.SymkeyIU, the security controller knows A.SymkeyData, A.SymkeyIU, A.SymkeyRNG, A.SymkeyAdmin, A.PubkeySignature, the administrator knows all the keys (including PrivkeySignature).

## 4.2 Environmental assumptions

The following assumtions about the TOE environment have to be fulfilled:

AE2: All the keys A.SymkeyData, A.SymkeyIU, A.SymkeyRNG, A.SymkeyAdmin, A.PubkeySignature, PrivkeySignature are generated according to the administration manual, that is, they are cryptographically good and strong.

AE4: All random numbers in the environment (IU, AU, card writer) used for cryptographic purposes are cryptographically good.

AE5: A.ProtectedData is protected against disclosure and manipulation within the card writer, the IU and all other devices entitled to have access to any information about A.ProtectedData.

AE6: The IU verifies that the TOE knows A.SymkeyIU before accepting data received from the TOE.

AE7: The administrator’s device verifies that the TOE knows the current A.SymkeyAdmin before sending data to the TOE.

### 4.3 Clarification of scope

The administrator’s unit, the interface unit, the memory card and card writer are not part of the TOE but are needed in the IT environment for the functioning the card reader. They are provided by Bayer Innovation GmbH.

The data on the holographic memory card can be analogue scrambled but the analogue scrambling is neither part of the security functionality nor analysed during the evaluation.

## 5 Architectural Information

The TOE is divided into the following four subsystems:

- SRS (security relevant subsystem):
  hardware: ST19WP18-D security controller
  software: SEC module
- AVR:
  hardware: AVR ATmega128 standard controller
  software: COM and ESC module
- Optical module:
  hardware: card reader (card slot, a light source, a camera, a control chip, photo sensors, and a phase mask enabling analogue scrambling of thelight beam.)
  software: OPT module
- Non-intelligent HW components:
  hardware only (data transmission lines, power supply wires, capacitors, standard Ethernet controller with a connector, display, keyboard, etc.)

Figure 1 below depicts a top level block diagramm of the TOE architecture:

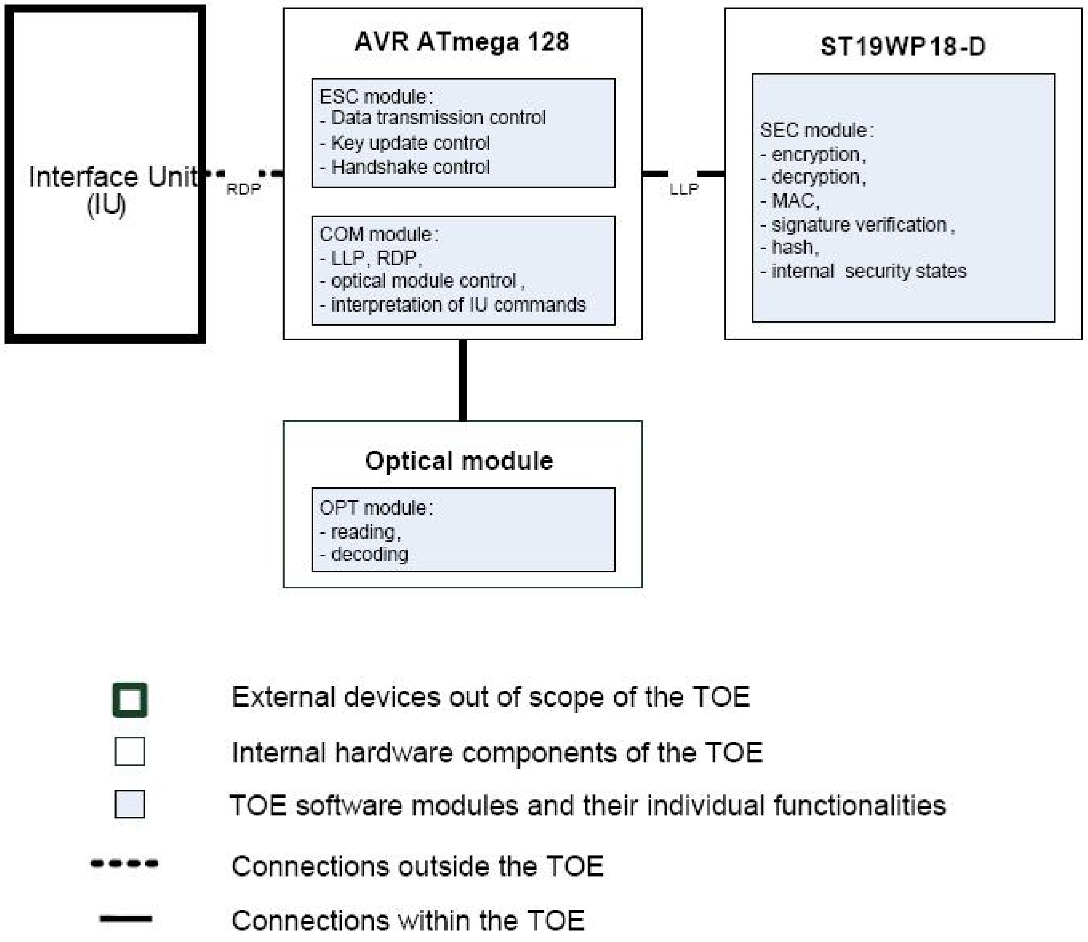
Interface Unit (IU)
RDP
AVR ATmega 128
ESC module:
- Data transmission control
- Key update control
- Handshake control
COM module:
- LLP, RDP,
- optical module control,
- interpretation of IU commands
LLP
ST19WP18-D
SEC module:
- encryption,
- decryption,
- MAC,
- signature verification,
- hash,
- internal security states
Optical module
OPT module:
- reading,
- decoding
External devices out of scope of the TOE
Internal hardware components of the TOE
TOE software modules and their individual functionalities
Connections outside the TOE
Connections within the TOE

Figure 1: Architecture of the TOE

# 6 Documentation

The documentations [11] and [12] are provided with the product by the developer to the customer for secure usage of the TOE in accordance with the Security Target.

Developers of the Interface Unit, the Administrator Unit and the Card Writer should follow the guidelines in the Guidance for implementing the Interface Unit, Administrator Unit and Card Writer [13].

# 7 IT Product Testing

## 7.1 Developer Test Effort

Test cases were included for the personalization of the TOE as well as the usage phase of the TOE. Some tests at the usage phase make use of an emulator of the ST19WP18-D which is a reasonable approach as these tests deal with internal processes of the TOE that cannot be adequately tested at an external interface. Further, tests are included to show that the TOE remains in a secure state if tampered with the voltage supply of the ST19WP18-D or bus lines between the AVR and the ST19WP18-D.

According to the test approach there are different test configurations used. During personalization, the ST19WP18-D was fitted in the personalization device. Except for the emulator tests, testing of the usage phase operates the TOE in a grey-box approach, i.e., one logs and analyses the communication on the external interface but with the knowledge of the internal processes. At emulator tests the internal processing of the ST19WP18-D was observed at critical parts of the implementation that need to be secured to guarantee a secured state of the TOE, even if interrupted.

## 7.2 Evaluator Idenpendant Testing

Independent testing (comprising the subset of penetration test) was done at escrypt GmbH and at T-Systems GEI GmbH. At escrypt GmbH, all emulator test cases were carried out. Other test cases were carried out both at escrypt GmbH and at T-Systems GEI GmbH.

For evaluator testing, the developer handed over a TOE sample and the GUI aided test tool including all sources to the evaluators. The evaluators were able to develop their own test cases as part of this developer test tool, i.e., the test tool was reprogrammed for independent testing. The evaluators produced a log file as result of the test cases executed.

Test cases were included for the personalization of the TOE as well as the usage phase of the TOE. Some tests at the usage phase make use of an emulator of the ST19WP18-D which is a reasonable approach as these tests deal with internal processes of the TOE that cannot be adequately tested at an external interface.

According to the test approach there are different test configurations used. During personalization, the ST19WP18-D was fitted in the personalization device. Except for the emulator tests, testing of the usage phase operates the TOE in a grey-box approach, i.e., one logs and analyses the communication on the external interface and knows the specification on the internal processing. At emulator tests the internal processing of the ST19WP18-D was observed at critical parts of the implementation that need to be secured to guarantee a secured state of the TOE, even if interrupted.

The evaluators devised and conducted additional tests during the execution of the handshake protocols which manipulate only special data items. These tests were conducted to increase the confidence of the TOE security functions.

Other main directions for evaluator testing are (i) to verify procedures during programming and personalization, (ii) to check the resistance of the TOE against buffer overflow attacks, (iii) to verify the absence of any additional commands (as far as it can be done with reasonable effort at the external interface of the TOE), (iv) to verify the correctness of the implementation of the pseudo random number generator and the DFA countermeasures, (v) to verify the correct implementation of cryptographic key derivation functions and the handshake protocol, and (vi) to verify the resistance against tampering attacks with the voltage supply of the ST19WP18-D. During evaluator testing all security functions were covered.

For the repetition of developer tests, the evaluators selected a subset of test cases found in the developer test plan and procedures. The choice was motivated by the aim that as much security functions are included as possible. Except for SF.8 (Generation of random numbers) all security functions are covered by this subset.

The SF.8 (Generation of random numbers) was tested by using an independent reference implemetation. The correct operation (as specified) of the deterministic random number generator (and thus also SF.8) has been demonstrated.

# 8 Evaluated Configuration

The evaluated configuration of TOE consists of i) PhenoStor® Card Reader GRE100010 including the application software and ii) the pertaining guidance documentation ’Administrator- Sicherheitshandbuch mit Installation, Generierung und Anlauf (ADO_IGS.1 und AGD_ADM.1), PhenoStor®’ [11] and ‘Benutzer-Sicherheitshandbuch, (AGD_USR.1), PhenoStor®’ [12]. The software runs on the security controller ST19WP18-D from STMicroelectronics.

The environment for testing the TOE was provided by escrypt GmbH in Bochum. The TOE is labelled as stated above. The test were carried out at escrypt GmbH and at the T-Systems GEI GmbH.

For the tests, the software part of the TOE has been loaded into the security controller by using the Bootloader. This test configuration has been tested as been described in the previous section 7.

# 9 Results of the Evaluation

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

As the evaluation of the TOE was conducted as a composition evaluation, the ETR [8] includes also the evaluation results of the composite evaluation activities in accordance with CC Supporting Document, ETR-lite for Composition: Annex A Composite smart card evaluation [4, AIS 36]. The ETR [8] builds up on the ETR-lite for Composition document of the evaluation of the underlying the STMicroelectronics security controller ST19WP18-D (Certification Report 2005/41 [16] and Maintenance Report M-2006/05 [17] ).

The evaluation methodology CEM [2] was used for those components identical with EAL3.

The verdicts for the CC, Part 3 assurance components (according to EAL 3 and the class ASE for the Security Target evaluation) are summarised in the following table:

| **Assurance classes and components** | | **Verdict** |
|---|---|---|
| Security Target evaluation | CC Class ASE | PASS |
| TOE description | ASE_DES.1 | PASS |
| Security environment | ASE_ENV.1 | PASS |
| ST introduction | ASE_INT.1 | PASS |
| Security objectives | ASE_OBJ.1 | PASS |
| PP claims | ASE_PPC.1 | PASS |
| IT security requirements | ASE_REQ.1 | PASS |
| Explicitly stated IT security requirements | ASE_SRE.1 | PASS |
| TOE summary specification | ASE_TSS.1 | PASS |
| Configuration management | CC Class ACM | PASS |
| Authorisation controls | ACM_CAP.3 | PASS |
| TOE CM coverage | ACM_SCP.1 | PASS |
| Delivery and operation | CC Class ADO | PASS |
| Delivery procedures | ADO_DEL.1 | PASS |
| Installation, generation, and start-up procedures | ADO_IGS.1 | PASS |
| Development | CC Class ADV | PASS |
| Informal functional specification | ADV_FSP.1 | PASS |
| Security enforcing high-level design | ADV_HLD.2 | PASS |
| Informal correspondence demonstration | ADV_RCR.1 | PASS |

| **Assurance classes and components** | | **Verdict** |
|---|---|---|
| Guidance documents | CC Class AGD | PASS |
| Administrator guidance | AGD_ADM.1 | PASS |
| User guidance | AGD_USR.1 | PASS |
| Life cycle support | CC Class ALC | PASS |
| Identification of security measures | ALC_DVS.1 | PASS |
| Tests | CC Class ATE | PASS |
| Analysis of coverage | ATE_COV.2 | PASS |
| Testing: high-level design | ATE_DPT.1 | PASS |
| Functional testing | ATE_FUN.1 | PASS |
| Independent testing – sample | ATE_IND.2 | PASS |
| Vulnerability assessment | CC Class AVA | PASS |
| Examination of guidance | AVA_MSU.1 | PASS |
| Strength of TOE security function evaluation | AVA_SOF.1 | PASS |
| Developer vulnerability analysis | AVA_VLA.1 | PASS |

Table 7: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL3
- The following TOE Security Functions fulfil the claimed Strength of Function:
  SF1, data and subject authentication during initialisation and usage of a trusted channel,
  SF3, decryption and verification of encrypted A.ProtectedData and
  SF8, generation of random numbers

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

The results of the evaluation are only applicable to the Phenostor® Card Reader GRE100010 with its components as listed in chapter 2, table 6 of this report.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

# 10 Comments/Recommendations

The operational documents [11] and [12] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

# 11 Annexes

none

# 12 Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete Security Target [6] used for the evaluation performed.

# 13 Definitions

## 13.1 Acronyms

| | |
|---|---|
| **3DES** | Triple-DES - Symmetric block cipher algorithm based on the DES |
| **AU** | Adimistrator Unit |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **CC** | Common Criteria for IT Security Evaluation |
| **DES** | Data Encryption Standard; symmetric block cipher algorithm |
| **EAL** | Evaluation Assurance Level |
| **IT** | Information Technology |
| **IU** | Interface Unit |
| **MAC** | Message Authentication Code |
| **PP** | Protection Profile |
| **RSA** | Rivest, Shamir, Adleman – a public key encryption algorithm |
| **SF** | Security Function |
| **SFP** | Security Function Policy |
| **SHA-1** | Secure Hash Algorithm 1 |
| **SOF** | Strength of Function |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSC** | TSF Scope of Control |
| **TSF** | TOE Security Functions |

| | |
|---|---|
| **TSP** | TOE Security Policy |

## 13.2 Glossary

**Augmentation** - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

**Extension** - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

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

**Informal** - Expressed in natural language.

**Object** - An entity within the TSC that contains or receives information and upon which subjects perform operations.

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

**Security Function** - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

**Security Target** - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

**Strength of Function** - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

**SOF-basic** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

**SOF-medium** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

**SOF-high** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

**Subject** - An entity within the TSC that causes operations to be performed.

**Target of Evaluation** - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

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

**TOE Security Policy** - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

**TSF Scope of Control** - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

# 14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-0373-2007, Version 1.8, 30.10.2006 , Security Target PhenoStor® Card Reader GRE100010, Bayer Innovation GmbH (confidential document)

[7] Security Target BSI-DSZ-0373-2007, Version 1.1, 08.03.2007 , Security Target Lite PhenoStor® Card Reader GRE100010, Bayer Innovation GmbH (sanitized public document)

[8] Evaluation Technical Report, Version 1.2, 18.12.2006, Evaluation Technical Report BSI-CC-DSZ-0373, T-Systems GEI GmbH (confidential document)

[9] Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001, developed by Atmel Smart Card ICs, Hitachi Ltd., Infineon Technologies AG, Philips Semiconductors

[10] Protection Profile Smartcard Integrated Circuit, Version 2.0, 09.1998, registered at the French Certification Body under the number PP/9806

[11] Administrator-Sicherheitshandbuch mit Installation, Generierung und Anlauf (ADO_IGS.1 und AGD_ADM.1), PhenoStor® Card Reader GRE100010, Version 1.3, 27.10.02006, Bayer Innovation GmbH

[12] Benutzer-Sicherheitshandbuch, (AGD_USR.1), PhenoStor® Card Reader GRE100010, Version 1.1, 21.09.2006, Bayer Innovation GmbH

[13] Guidance for implementing the Interface Unit, Administrator Unit and Card Writer, PhenoStor® Card Reader GRE100010, Version 1.2, 27.10.2006, Bayer Innovation GmbH

[14] Configuration List, PhenoStor® Card Reader GRE100010, Version 0.6, 07.12.2006, Bayer Innovation GmbH

[15] ST19WP18-D Security Target SMD_ST19WP18D_ST_06_001_V01.00, February 2006

[16] Certification Report 2005/41 - ST19WP18E microcontroller, 18 novembre 2005, SGDN/DCSSI

[17] Maintenance Report M-2006/05 - Secure microcontroller ST19WP18-D Reference certificate: 2005/41, DCSSII

This page is intentionally left blank.

# C Excerpts from the Criteria

CC Part1:

**Conformance results** (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

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

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

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

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

CC Part 3:

## **Assurance categorisation** (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

| **Assurance Class** | **Assurance Family** |
|---|---|
| ACM: Configuration management | CM automation (ACM_AUT) |
| | CM capabilities (ACM_CAP) |
| | CM scope (ACM_SCP) |
| ADO: Delivery and operation | Delivery (ADO_DEL) |
| | Installation, generation and start-up (ADO_IGS) |
| ADV: Development | Functional specification (ADV_FSP) |
| | High-level design (ADV_HLD) |
| | Implementation representation (ADV_IMP) |
| | TSF internals (ADV_INT) |
| | Low-level design (ADV_LLD) |
| | Representation correspondence (ADV_RCR) |
| | Security policy modeling (ADV_SPM) |
| AGD: Guidance documents | Administrator guidance (AGD_ADM) |
| | User guidance (AGD_USR) |
| ALC: Life cycle support | Development security (ALC_DVS) |
| | Flaw remediation (ALC_FLR) |
| | Life cycle definition (ALC_LCD) |
| | Tools and techniques (ALC_TAT) |
| ATE: Tests | Coverage (ATE_COV) |
| | Depth (ATE_DPT) |
| | Functional tests (ATE_FUN) |
| | Independent testing (ATE_IND) |
| AVA: Vulnerability assessment | Covert channel analysis (AVA_CCA) |
| | Misuse (AVA_MSU) |
| | Strength of TOE security functions (AVA_SOF) |
| | Vulnerability analysis (AVA_VLA) |

Table 1: Assurance family breakdown and mapping”

### **Evaluation assurance levels** (chapter 11)

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

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

### **Evaluation assurance level (EAL) overview** (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

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

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

| Assurance Class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Configuration management | ACM_AUT | | | | 1 | 1 | 2 | 2 |
| | ACM_CAP | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ACM_SCP | | | 1 | 2 | 3 | 3 | 3 |
| Delivery and operation | ADO_DEL | | 1 | 1 | 2 | 2 | 2 | 3 |
| | ADO_IGS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Development | ADV_FSP | 1 | 1 | 1 | 2 | 3 | 3 | 4 |
| | ADV_HLD | | 1 | 2 | 2 | 3 | 4 | 5 |
| | ADV_IMP | | | | 1 | 2 | 3 | 3 |
| | ADV_INT | | | | | 1 | 2 | 3 |
| | ADV_LLD | | | | 1 | 1 | 2 | 2 |
| | ADV_RCR | 1 | 1 | 1 | 1 | 2 | 2 | 3 |
| | ADV_SPM | | | | 1 | 3 | 3 | 3 |
| Guidance documents | AGD_ADM | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_USR | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life cycle support | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | | 1 | 2 | 2 | 3 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | 2 | 2 | 3 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_CCA | | | | | 1 | 2 | 2 |
| | AVA_MSU | | | 1 | 2 | 2 | 3 | 3 |
| | AVA_SOF | | 1 | 1 | 1 | 1 | 1 | 1 |
| | AVA_VLA | | 1 | 1 | 2 | 3 | 4 | 4 |

Table 6: Evaluation assurance level summary”

**Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 11.3)

“Objectives

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

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

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

**Evaluation assurance level 2 (EAL2) - structurally tested** (chapter 11.4)

“Objectives

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

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

**Evaluation assurance level 3 (EAL3) - methodically tested and checked** (chapter 11.5)

“Objectives

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

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

**Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed** (chapter 11.6)

“Objectives

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

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

**Evaluation assurance level 5 (EAL5) - semiformally designed and tested** (chapter 11.7)

“Objectives

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

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

**Evaluation assurance level 6 (EAL6) - semiformally verified design and tested** (chapter 11.8)

“Objectives

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

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

**Evaluation assurance level 7 (EAL7) - formally verified design and tested** (chapter 11.9)

“Objectives

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

**Strength of TOE security functions (AVA_SOF)** (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

**Vulnerability analysis (AVA_VLA)** (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”