Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-S-0040-2015

for

Dream Chip Technologies GmbH Germany

of

Dream Chip Technologies GmbH

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-S-0040-2015

Common Criteria

Design Center

Dream Chip Technologies GmbH Germany

of	Dream Chip Technologies GmbH
Life cycle phase:	Development of Smard Card ICs Software and Testing
Assurance (*):	Common Criteria Part 3 conformant - ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 - ALC_DEL.1, ALC_TAT.3
Valid until:	15 April 2017

The site identified in this certificate has been evaluated by an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by BSI Scheme procedures including the Supporting Document Guidance CCDB-2007-11-001 Site Certification, October 2007, Version 1.0, Revision 1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific site as indicated above and in conjunction with the complete content of the Certification Report and the Site Security Target.

(*) For information on the evaluated scope of the certified site and the application of the assurance components listed above and their relevance and applicability for the certified site see 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 site by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the site 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,16 April 2015

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 development and production sites for information technology products.

The results from a site certification can be re-used for product certifications. For products which have been certified using a site certificate an individual certificate will be issued.

Certification of a site is carried out on the instigation of the operator of the site.

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

The evaluation is 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 description of the site, the activities for which the site is responsible within a product life cycle, the details of the evaluation (strength and weaknesses) and instructions for the client of the site.

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

Contents

A Certification....7
1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)....7
2.2 International Recognition of CC - Certificates....8
3 Performance of Evaluation and Certification....8
4 Validity of the certification result....9
5 Publication....9
B Certification Results....11
1 Identification of the Site....11
2 Life cycle phase....11
3 Technical scope....11
4 Assumptions and Clarification of Scope....12
5 Documentation....13
6 Results of the Evaluation....13
7 Obligations and notes for the usage of the site....14
8 Site Security Target....14
9 Definitions....14
9.1 Acronyms....14
9.2 Glossary....15
10 Bibliography....15
C Excerpts from the Criteria....17

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 and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 17065 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- Supporting Document Guidance Site Certification [5]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Procedure for the issuance of a site certificate by the BSI

2 Recognition Agreements

Currently the Recognition Agreements in place do not cover the recognition of Site Certificates. However, the evaluation process performed was outlined according to the rules of the agreements and by using the agreed supporting document on Site Certification [5].

Therefore, the results of this evaluation and certification procedure can be re-used by the issuing scheme in a subsequent product evaluation and certification procedure.

In the following the scope of the current Recognition Agreements is outlined. These Recognition Agreements of IT security certificates - as far as such certificates are based on ITSEC or CC - are agreed under certain conditions in order to avoid multiple certification of the same product in different countries.

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

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition

---

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

3 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

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

level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above. Details on recognition and the history of the agreement can be found at http://www.sogisportal.eu.

Site Certificates are not covered by this Recognition Agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

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

Site Certificates are not covered by this Recognition Arrangement.

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 site Dream Chip Technologies GmbH Germany has undergone the certification procedure at BSI.

The evaluation of the site Dream Chip Technologies GmbH Germany was conducted by T-Systems GEI GmbH. The evaluation was completed on 23 March 2015. The T-Systems GEI GmbH is an evaluation facility (ITSEF) recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Dream Chip Technologies GmbH.

The operator of the site is: Dream Chip Technologies GmbH.

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 site and its evaluated scope as indicated. The confirmed assurance package is only valid on the condition that all assumptions and preconditions required by the site, as given in the following report and the Site Security Target [7], are observed.

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

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

The owner of the certificate is obliged:

- To archive all evaluated documents as outlined in the ETR [8] for a time frame of 5 years. Within this time frame the documents will be made available to BSI for the purpose of re-examination of the certificate on request and without any costs.
- When advertising the certificate or the fact of the site's certification, to refer to the Certification Report as well as to provide the Certification Report and the Security Target and if applicable the guidance documentation for the usage of the site mentioned herein to any client of the site.
- To inform the Certification Body at BSI immediately in the case security relevant changes at the site will be made.
- To inform the Certification Body at BSI immediately about vulnerabilities at the site that have been identified by the operator of the site or any third party.
- To inform the Certification Body at BSI immediately in the case that confidentiality of documentation and information related to the site or resulting from the evaluation and certification process is not given any longer.

Assuming nothing has changed at the site, validity of this certificate ends as outlined on the certificate.

5 Publication

The site Dream Chip Technologies GmbH Germany has been included in the BSI list of certified sites, which is published regularly (see also Internet: https://www.bsi.bund.de and [6]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Dream Chip Technologies GmbH
Steinriede 10
30827 Garbsen
Germany

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Site Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Identification of the Site

The evaluated site is:

Dream Chip Technologies GmbH
Steinriede 10
30827 Garbsen
Germany

The site comprises a solitaire building, completely rented by Dream Chip Technologies GmbH.

2 Life cycle phase

This certification of the site supports the following life cycle phases of a product life cycle according to the Security IC Platform Protection Profile [9]:

- IC Embedded Software development and testing (phase 1)
- IC Dedicated Software development and testing (phase 2)
- Development and characterization/validation testing of secure smart card ICs (phase 2)

3 Technical scope

The certified site is intended to be used by only one specific client, namely NXP Semiconductors Business Unit Identification (BU ID). The site is used for Smart Card IC Development and connected over a secured VLAN-connection to the NXP-network. No other processes like packaging, transportation, delivery or production are involved, as the site works logically “inside” NXPs network for development only.

To perform its activities the site uses the NXP BU ID provided and managed remote IT-infrastructure. Locally available IT equipment like workstations or VPN router is also provided and managed by NXP BU ID directly. The site works according to NXP BU ID processes.

The full version of the Site Security Target [7] is the basis for this certification. It is based on the Life Cycle Definition and the Security Problem Definition Definition as outlined in the Security IC Platform Protection Profile [9].

The certification of the site covers the following development steps:

- Specification of reference architectures and specific architectures
- Design of hardware modules
- Creation of source code for embedded and IC dedicated software
- Creation of development related documents
- Test specification and definition of related test vectors

- Creation of data sheet and application note material
- Execution of the tests foreseen by the test specification using the defined test vectors
- Creation of the documentation for this site evaluation (SST, ALC-Documentation)

The development is done according to the NXP BU ID Product Creation, described in internal document Release Manual [10].

This site does not perform temperature and timing validations.

The Security Problem Definition for this site comprises security problems derived from threats against relevant assets and for the type of TOE considered as well as security problems derived from the configuration management requirements. The assets, assumptions, threats and organisational security policies are defined in the document Site Security Target [7], chapter 4. Only aspects that are applicable to the life cycle phase 1 and phase 2 according to the Security IC Platform Protection Profile [9] are considered here.

The security objectives for the site are derived from these threats and organisational security policies as stated in the Site Security Target [7], chapter 5.

The Site Security Target claimed the following Common Criteria Part 3 life cycle security assurance components to be part of the evaluation:

- CM capabilities - ALC_CMC.5
- CM scope - ALC_CMS.5
- Delivery - ALC_DEL.1
- Development security - ALC_DVS.2
- Life-cycle definition - ALC_LCD.1
- Tools and techniques - ALC_TAT.3

The specific scope of these components relevant at this site is explained in the Site Security Target [7], chapter 7. As outlined in the Site Security Target, the activities of the site are not related to TOE Delivery ALC_DEL and Tools and techniques ALC_TAT. However, the components have been claimed in order to ensure the assessment of related items during the evaluation process and therefore to support the reuse of the evaluation results in a product evaluation accordingly.

For the assessment of the security measures attackers with high attack potential are assumed. This allows an evaluation of products using this site according to the assurance component AVA_VAN.5. For more details please refer to the Site Security Target [7], chapter 3.

4 Assumptions and Clarification of Scope

The assumptions defined in the Site Security Target are not covered by the site itself. These aspects have to be followed by NXP BU ID. The following topics are of relevance:

- Setup and maintenance of the nesessary development environment
- Project setup

Details can be found in the Site Security Target [7], chapter 4.4.

5 Documentation

There is no evaluated documentation being provided to the client of the site. The client has to follow the requirements as stated in the Assumptions in the Site Security Target [7], chapter 4.4.

6 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 site.

Specifically the Supporting Document Guidance CCDB-2007-11-001 Site Certification [5] and AIS 47 "Regelungen zu Site Certification" [4] were used.

For smart card IC specific methodology the CC supporting document “The Application of CC to Integrated Circuits” (see [4] AIS 25) was used.

All assurance components claimed in the Site Security Target [7], chapter 7 are confirmed to be Common Criteria Part 3 conformant.

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

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

- CM capabilities - ALC_CMC.5
- CM scope - ALC_CMS.5
- Development security - ALC_DVS.2
- Life-cycle definition - ALC_LCD.1

The following assurance components have been covered by the evaluation, but the evaluation concluded that the site does not provide contributions to the security objectives and therefore these components are not applicable to the site:

- Delivery - ALC_DEL.1
- Tools and techniques - ALC_TAT.3

For reusing the evaluation results in product evaluations, the specific scope of the assurance components as relevant at this site and outlined in the Site Security Target has to be assessed if it fits into the product life cycle considered.

As the assurance components assessed are derived from the assurance level EAL6 of the CC assurance class "Life-cycle Support", this site certificate supports product evaluations up to the assurance level EAL6.

For the assessment of the security measures attackers with high attack potential have been assumed. This supports an evaluation of products using this site according to the assurance component AVA_VAN.5.

The evaluation has confirmed for the type of product considered that the development life cycle is covered as described in chapter 2.

The certification results only apply to the site as indicated in the certificate, the scope as defined in the Site Security Target and on the condition that all the stipulations are kept as detailed in this Certification Report.

This certificate is not an endorsement of the site 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 site by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

7 Obligations and notes for the usage of the site

The relevant information for using the evaluated scope of the site within product evaluations is given in the Site Security Target [7]. During a product evaluation the evidence for the fulfilment of the Assumptions given in section 4.4 of the SST shall be examined by the evaluator of the product when re-using the results of this site evaluation. Note that the sponsor of a potential product evaluation has to ensure that all information required by the Assumptions is made available.

The specific scope of the ALC assurance components as evaluated and as outlined in the Site Security Target has to be assessed if it fits into the product life cycle considered.

The assets assessed, any limitations in covering confidentiality or integrity aspects and the resistance level (AVA_VAN) applied have to be considered according to the SST when re-using the evaluation results in a product evaluation.

8 Site Security Target

For the purpose of publishing, the Site Security Target is provided within a separate document as an annex of this report. It is a sanitised version of the complete Site Security Target [7] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

9 Definitions

9.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement

SST Site Security Target

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

9.2 Glossary

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

Client - The term "client" is used to describe the subcontracting relationship between the developer/manufacturer of the product and the site providing a specific manufacturing step described in the SST. The term is used to prevent confusion regarding the words "customer" and "consumer" that are reserved in CC for the recipient (addressee) of the finished product.

Extension - The addition to an SST 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.

Life cycle phase – part of a life cycle of a product.

Informal - Expressed in natural language.

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

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

Site Security Target - A statement of security needs for a specific identified development or production site.

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

Site - A part or the whole of an existing or anticipated TOE development environment. A site may consist of one geographical location, be a part of one location, or may span (parts of) multiple locations. A site may consist of one organisational unit, be part of an organisational unit, or may span (parts of) multiple organisational units.

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

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

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

10 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

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

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

[5] Supporting Document Guidance CCDB-2007-11-001 Site Certification, October 2007, Version 1.0, Revision 1

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

[7] Site Security Target Lite, BSI-DSZ-CC-S-0040, Revision 1.1, 05.03.2015, Dream Chip Technologies GmbH (sanitised public document)
Site Security Target, BSI-DSZ-CC-S-0040, Revision 1.1, 09.12.2014, Dream Chip Technologies GmbH (full version, confidential document)

[8] Evaluation Technical Report, Version 1.0, 09.03.2015, T-Systems GEI GmbH, (confidential document)

[9] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, Eurosmart, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0084-2014

[10] PV3-00101 Release Manual, NXP Semiconductors, Quality Systems, BU ID, Rev. 25, 02.04.2014

[7] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers - including JIL Document
- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen - including JIL Document and CC Supporting Document
- AIS 32, Version 7, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) - including JIL Document and CC Supporting Document
- AIS 47, Version 1.1, Regelungen zu Site Certification

C Excerpts from the Criteria

Supporting Document Guidance CCDB-2007-11-001 Site Certification:

Class AST: Site Security Target evaluation

Assurance class AST: Site Security Target evaluation defines requirements for the evaluation of an SST, to demonstrate that the SST is sound and internally consistent.

Assurance Class	Assurance Components
Class AST: Site Security Target evaluation	AST_INT.1 SST introduction
	AST_CCL.1 Conformance claims
	AST_SPD.1 Security problem definition
	AST_OBJ.1 Security objectives
	AST_ECD.1 Extended components definition
	AST_REQ.1 Security Assurance requirements
	AST_SSS.1 Site summary specification

AST: Site Security Target evaluation class decomposition

CC Part 3:

Security assurance components

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 ALC and AVA assurance class decompositon.

Assurance Class	Assurance Components
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

Assurance Class	Assurance Components
	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
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey (resistance level basic) AVA_VAN.2 Vulnerability analysis (resistance level basic) AVA_VAN.3 Focused vulnerability analysis (resistance level enhanced-basic) AVA_VAN.4 Methodical vulnerability analysis (resistance level moderate) AVA_VAN.5 Advanced methodical vulnerability analysis (resistance level high)

ALC and AVA assurance class decomposition

Evaluation assurance levels

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.

The following table shows the ALC and AVA related part of the EAL composition as defined in the CC part 3. 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.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
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
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

ALC and AVA related part of the Evaluation Assurance Levels