Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0342-2007

for

Outbound Downgrade Filter
of ASDE Link-1 Forward Filter version 1.5

from

NATO C3 Agency

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-0342-2007

Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5

from

NATO C3 Agency

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** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4**

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, 14. June 2007

The President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)3018 9582-0, Infoline +49 (0)3018 9582-111, Fax +49 (0)3018 9582-5477

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)

---

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 Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5 has undergone the certification procedure at BSI.

The evaluation of the product Outbound Downgrade Filter Link-1 Forward Filter version 1.5 was conducted by CSC Deutschland Solutions GmbH. The CSC Deutschland Solutions GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor is:

NATO C3 Agency
Oude Waalsdorperweg 61
p/o Postbus 174
2501 CD The Hague
The Netherlands

The certification is concluded with

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

This work was completed by the BSI on 14. June 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-24.

The product Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5 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] NATO C3 Agency
Oude Waalsdorperweg 61
p/o Postbus 174
2501 CD The Hague
The Netherlands

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 TOE is the Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5. It is a software application of an Air Situation Data Exchange (ASDE) that will permit one-way Link-1 message streams to be securely and automatically screened for the contents considered to be classified within a trusted and secure environment (typically a transmitting NATO facility such as a Control and Reporting Centre). The screening rules applied depend upon a mode of operation (peace, exercise, crisis response or article 5 operational mode).

The Link-1 Forward Filter aims at downgrading sanitized outbound CLASSIFIED[8] Link-1 Messages into NATO UNCLASSIFIED/Partner Nations RELEASABLE Link-1 Messages. When classified messages are encountered, the content of these messages will not be transmitted. When Link-1 message fields containing information considered to be classified are encountered, the bits in those fields will be set to zero before the message itself will be transmitted. The Link-1 Forward Filter sends the downgraded and sanitized messages out over unencrypted and unprotected serial communications lines.

The Link-1 Forward Filter can also be used to verify that the Link-1 data received from the Partner Nations equals the Link-1 format but this is not a function under evaluation.

The Link-1 Forward Filter runs mandated on a secure and certified operating system, that is served by an accompanying hardware platform, which is located in a secured location, that can only be accessed by authorised personnel who have been ‘screened’ as a condition of their employment by NATO.

The IT product Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5 was evaluated by CSC Deutschland Solutions GmbH. The evaluation was completed on 13. April 2007. The CSC Deutschland Solutions GmbH is an evaluation facility (ITSEF)[9] recognised by BSI.

The sponsor is

NATO C3 Agency
Oude Waalsdorperweg 61
p/o Postbus 174
2501 CD The Hague
The Netherlands

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],

[8] ‘CLASSIFIED‘ is used as placeholder for the real classification (e.g. NATO CONFIDENTIAL)

[9] Information Technology Security Evaluation Facility

part 3 for details). The TOE meets the assurance requirements of assurance level EAL4 (TOE evaluation: methodically designed, tested, and reviewed).

1.2 Functionality

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

The following SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
FAU	Security audit
FDP	User data protection
FMT	Security Management
FPT	Protection of the TOE Security Functions
FRU	Resource utilisation
FTP	Trusted path/channels

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

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

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

Security Functional Requirement	Addressed issue
FAU	Security audit
FDP	User data protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TOE Security Functions

Table 2: 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 chapter 5.4.

All security functional requirements for the IT environment are implemented by Secure_IT_Platform.

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

TOE Security Function	Addressed issue
SF.Downgrade	This function aims at downgrading sanitized O.Data_Class from the classified to unclassified partition on the Secure Operating System.

TOE Security Function	Addressed issue
SF. Audit_Export	This function aims at recording audit logs of all operations done by the security functions in order to trace all changes made on the Link-1 data.
SF.Check_Integrity	This function aims at checking the integrity of the downgraded O.Data_Unclass by recalculating its cyclic redundancy check.
SF.Check_Sanitarization	This function aims at verification and sanitization of O.Data_Class mandated by the O.Filter_Rule_Set appropriate for the current SA.Oper_Mode.
SF.Disregard	This function aims at disregarding and deleting invalid outcomes of other security functions in a controlled manner to prevent unelaborated distribution of O.Data_Class or O.Data_Unclass.
SF.Pack	This function shall add a cyclic redundancy check to the sanitized O.Data_Class. The added cyclic redundancy check is used to verify after the downgrade the resulting O.Data_Unclass is not altered
SF.Sanitize	This function aims at the sanitization of O.Data_Class as mandated by the O.Filter_Rule_Set appropriate for the current SA.Oper_Mode
SF.Set_Mode	This function will set the appropriate set of filter rules that will be enforced by the operation R.Sanitize.
SF.StartStop	This function records the date and time of the testframe start-up and shutdown.
SF.Test	This function will test the correct operation of the filter and the Secure_IT_Platform.
SF.Verify_Outbound	This function aims at verification of syntactical compliance of the O.Data_Class received from the L1-Provider.
SF.Consider_Logout	This function aims at recognition of an (unexpected) end of the operator console process.
SF.Operator_Input	This security function records start and stop of the operator console as well as all user input.
SF.Keep_Alive	This function aims at sending O.Ping to the testframe every 10 seconds when no other O.Command will be sent.
SF.Sec_Com_Op	This function aims at building up a secure network connection to the testframe part in order to be able to exchange O.Command and O.Output_Message in a secure way.
SF.Sec_Com_Testframe	This function aims at building up a secure network connection to the operator console in order to be able to exchange O.Command and O.Output_Message in a secure way
SF. Keep_Alive_Check	This function aims at receiving O.Command (including O.Ping) from the operator console and controlling the information flow between the L1-providing System and LIFOS.

Table 3: Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

1.3 Strength of Function

The TOE does not use any probabilistic or permutational mechanisms, and thus a Strength of Function claim is not appropriate. Therefore, no Strength of Function is claimed.

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

1.4.1 Definition of subjects, objects and operations

Non-human Subjects

The systems (equipment) that interact with the TOE are:

L1-Provider	Link-1 Providing System (or equivalent system such as an ASDE Buffer) that supplies a Link-1 Stream to the TOE. The L1-Provider is located in an IT environment with the same regime as the TOE, which is authorised to process CLASSIFIED information.
LIFOS	Accredited hardware system consisting of information diodes that ensure the flow of serial line data in one direction only. LIFOS is connected to the TOE and to a non-NATO system, which is expected to follow similar rules as within the NATO establishment, but is not under NATO control. LIFOS is located in an IT environment that is authorised to contain NATO crypto equipment.
Secure_IT_Platform	Certified secure IT Platform on which the TOE runs, consisting of a secure operating system and accompanying hardware. The secure software is the SUN Trusted Solaris 8 operating system as specified in [9]. The hardware comprises the SUN Blade/SPARC 100/150 and serial communication cards.

Authorized human subjects

The only user that interacts with the TOE is:

S.SysOper	User role defined by Secure_IT_Platform. This role is the operator of the TOE and is allowed to start and stop the TOE (both parts) via the Console. In addition, the role may start and stop the system, allocate system resources such as disks, start and stop queues, etc.

The users that are present within the TOE environment are:

S.Audit	User role defined by Secure_IT_Platform. This role is the Auditor of the audit output of the TOE and of audits in the TOE IT environment. Only the S.Audit role can analyse,

	back up and restore system audit logs when the testframe part of the TOE is not running. The audit logs are regularly reviewed.
S.ISSO	User role defined by Secure_IT_Platform. This role is the Information System Security Officer of the TOE IT environment. Only the S.ISSO role can create new user accounts and establish or change security related settings like contents of the label encoding file, user clearance limits, etc. At least two on-site named persons shall always be allocated to this role.
S.SysAdmin	User role defined by Secure_IT_Platform. This role is the system administrator of the TOE IT environment. S.SysAdmin shall undertake normal UNIX administration duties such as maintaining user passwords, etc. S.SysAdmin is the only role able to modify user accounts, but cannot create new accounts. No user able to operate in the S.SysAdmin role shall also have the possibility to operate in the S.ISSO or S.Audit role. At least two on-site named persons shall always be allocated to this role.

S.SysOper, S.Audit, S.ISSO and S.SysAdmin are all authorised to access the IT environment of the TOE. Authorisation is settled conform to NATO regulations. These persons are characterized as follows:

- Competent to perform their duties;
- Able to perform the appropriate security procedures;
- Have an appropriate screening of at least the site level of accreditation;
- Are trusted not to abuse his authority;
- Are trusted not to compromise security measures;
- Are not considered to be hostile;
- Are capable of making mistakes (although not intentionally).

Security Attributes of Subjects

SA.Oper_Mode	This security attribute defines the four possible operational modes of the L1-Provider and the TOE. • Peace Operational Mode • Exercise Operational Mode • Crisis Response Operational Mode • Article 5 Operational Mode

SA.OS_MAC_Level — This security attribute defines the four mandatory access control operational levels of the Secure_IT_Platform[10]. These levels are (from highest to lowest classification):

- Admin high, Classified,
- Unclassified,
- Software,
- Admin Low.

SA.OS_Priv_Level — This security attribute defines the privileges (*privileged* or *unprivileged*) to determine if a subject may execute a trusted system call, or a general system call of the Secure_IT_Platform in a trusted manner (i.e., file write with MAC override). SA.OS_Priv_Level is independent of SA.OS_MAC_Level.

SA.Subject_Identity — Associated security attribute for a subject that equals the name of the subject, i.e. L1-Provider and LIFOS.

Objects

For all objects the following security attribute holds:

SA.Security_Label — This security attribute defines the two classification levels that data processed by the TOE and its environment can have. The classification levels are CLASSIFIED and NATO UNCLASSIFIED/PN RELEASABLE.

The (data) objects for the TOE that the TOE will operate upon are:

O.Data_Audit — Audit data log record produced by the TOE. The data has SA.Security_Label ‘CLASSIFIED‘.

O.Data_Class — A packet of data having a sequence number and SA.Security_Label ‘CLASSIFIED’. The packet can take the following forms:

1. *Bit stream:* Series of bits that are probably a Link-1 message.
2. *Link-1 Message:* Link-1 Message.
3. *Sanitized Link-1 Message*: Link-1 Message sanitized by the operation R.Sanitize (see section operations).

O.Data_Unclass — A sanitized O.Data_Class having SA.Security_Label ‘NATO UNCLASSIFIED/PN RELEASABLE’.

---

[10] All authorized human subjects have a SA.OS_MAC_Level defining in which operation level they are allowed to operate:
- S.SysOper, S.Audit, S.ISSO operate at SA.OS_MAC_Level ‘Admin high, Classified’
- S.SysAdmin operates at SA.OS_MAC_Level ‘Admin Low’.

O.Filter_Rule_Set	The set of rules that define which (parts of) O.Data_Class need to be sanitized given by the SA.Oper_Mode of the L1-Provider of this ST. The set has SA.Security_Label ‘CLASSIFIED’.
O.Command	Messages send from the operator console to the testframe part of the TOE. These messages contain commands for the testframe entered by the user at the operator console.
O.Ping	A special O.Command the operator console sends regularly to the testframe. This informs the testframe that the operator console is running.
O.Output_Message	Messages send from the testframe part of the TOE to the operator console. These messages contain information the operator console has to display.

Operations

R.Audit_Trail	This operation writes O.Data_Audit to an audit trail of the Secure_IT_Platform.
R.CRC_Check	This operation confirms or denies whether the cyclic redundancy check of O.Data_Unclass equals the cyclic redundancy check calculated by R.CRC_Pack for the corresponding sanitized O.Data_Class.
R.CRC_Pack	This operation calculates a cyclic redundancy check over a sanitized O.Data_Class and the cyclic redundancy check is added to this sanitized O.Data_Class.
R.Disregard	This operation disregards all data in O.Data_Class or O.Data_Unclass.
R.Downgrade	This operation generates a new O.Data_Unclass with the data of a sanitized O.Data_Class.
R.Sanitize	This operation applies O.Filter_Rule_Set on O.Data_Class. This means this operation generates a new O.Data_Class that contains a Link-1 Message which fulfils O.Filter_Rule_Set (some bits are zeroed or a blank message).
R.Set_Mode	This operation sets the O.Filter_Rule_Set to one of the SA.Oper_Mode values.
R.Test	This operation checks the integrity of the TOE and the presence of the Secure_IT_Platform.
R.Verify_Outbound	This operation confirms or denies whether O.Data_Class coming from L1-Provider conforms syntactically to [11].

Non-Authorized subjects (Threat Agents)

The following subjects are capable to effectuate threats for the TOE (i.e. Threat Agents):

TA.Erroneous_User	S.SysOper, S.Audit, S.ISSO or S.SysAdmin capable of making mistakes with organizational security policies or accidentally modifying the Secure_IT_Platform or the TOE configuration, thereby allowing security violations to occur.
TA.Unclass_Receiver	Entity, human person or IT system not authorised to receive O.Data_Class. This entity is capable of receiving an outgoing Link-1 data stream from the TOE outside the TOE environment.

1.4.2 Threats

T.BYPASS

O.Data_Class are passed from the Link-1 Providing System to the TOE. In the TOE these data are processed and recorded. After the processing these data become NATO UNCLASSIFIED/PN RELEASABLE. The O.Data_Class are only available on the interface with the Link-1 Providing System, within the TOE or from the recording (Audit_Trail).
A TA.Unclass_Receiver is able to read O.Data_Class either immediately, or in some point in the future, because TA.Erroneous_User has logically or physically bypassed the protection functions of the TOE. This may be possible due to errors in or an erroneous configuration of the underlying operating system or failures of the physical access controls to the hardware. This threat may occur at each time a TA.Erroneous_User has logical or physical access to the hardware, operating system or the TOE or when an already existing bug within the operating system becomes effect.

T.MODE_SYNC

A TA.Unclass_Receiver is able to read O.Data_Class because TA.Erroneous_User has not synchronized SA.Oper_Mode of the TOE with SA.Oper_Mode of the L1-Provider. This threat occurs when TA.Erroneous_User does not perform a required change of SA.Oper_Mode. Due to the fact that TA.Erroneous_User is allowed to change SA.Oper_Mode, only communication problems with the other L1-Provider or human failure could be the reason.

T.NEGLIGENCE

A TA.Erroneous_User makes a mistake, for instance inserting a wrong operational mode in the TOE (e.g. Exercise instead of Peace) that possibly violates P.DECLASSIFICATION_POLICY causing that TA.Unclass_Receiver is able to read O.Data_Class and S.Audit does not notice. This threat may occur when TA.Erroneous_User performs a change of SA.Oper_Mode. Due to the fact that TA.Erroneous_User is allowed to change SA.Oper_Mode, only human failures could be the reason.

T.OPERATOR_DOES_NOT_EXIT

A TA.Erroneous_User logs out of the operating system but does not exit the operator console before. This may happen because the user starts the operator console as independent process in the background or the operating system puts the process in the background during log off of the user. Therefore, this threat may occur at any time. The operator console keeps running and the time-out mechanism of the TOE testframe part does not work. Therefore, there is no human operator to monitor the warning messages the TOE generates. This may result in O.Data_Class sent out without appropriate sanitization to TA.Unclass_Receiver.

T.TOE_REPROGRAM

A TA.Erroneous_User may reprogram or modify the TOE binary stored on the hard disk, causing it to pass through O.Data_Class either immediately or in some point in the future. For this purpose TA.Erroneous_User can use the tools usually installed with the underlying operating system. This threat is possible because TA.Erroneous_User must have access to the TOE binary for his normal work and the appropriate tools are installed on the system. Due to the fact that the access to the TOE is not restricted for TA.Erroneous_User, this attack or mistake may occur every time TA.Erroneous_User works on the system.

1.4.3 Organisational Security Policies

P.DECLASSIFICATION_POLICY

The TOE shall implement and comply with the NATO declassification policy appropriate for downgrading classified information. This policy defines the

- *Filter rules*: the set of rules for the circumstances under which information will be allowed for declassification.
- *Condition*: the condition for an automated system under which the filter rules are allowed to be applied. The condition is: It shall be retrievable when an O.Data_Class has been sent out.

P.INTER-TOE-COMMUNICATION

The two parts of the TOE shall establish a communication in such a way that

- the testframe receives all O.Command's from the operator console
- only the testframe receives the O.Command's
- the operator console receives all O.Output_Message's from the testframe
- only the operator console receives the O.Output_Message's

P.KEEP-ALIVE-POLICY

- If there is no other O.Command communication the operator console must send an O.Ping message to the testframe every 10 seconds.
- The testframe must be able to work without a running operator console but for three (3) minutes maximum.
- After this period of time the testframe has to stop working. This means, O.Data_Class from L1-Provider must be blocked.

P.TOE_DATA_INPUT

Outbound is defined as coming from the L1-Provider to the TOE.

The TOE shall be able to handle input streams with the following characteristics:

A bit stream coming from an L1-Provider can have any form and can possibly conform to [11].

P.TOE_FAIL_INSECURE

If the testframe part of the TOE software fails, a TA.Unclass_Receiver is able to read O.Data_Class either immediately or in some point in the future because the failure results in a forwarding of unsanitized messages.

The TOE shall be able to handle failures in the hardware, in the operating system or the TOE itself in such a way that unsanitized messages will not be forwarded.

1.5 Special configuration requirements

The TOE runs on a secure evaluated IT Platform and is connected via a security-accredited NC3A Link-1 Fibre Optic Secure Modem (LIFOS) to the receiving site at the partner nation ensuring that the sanitized data flows only from the classified side to the unclassified side to the Partner Nation as specified in [9].

1.6 Assumptions about the operating environment

- From the outside, attacks can only be performed via a data stream from the Partner Nation. It is assumed that this data stream has to pass a LIFOS and can therefore not reach the TOE.
- It is assumed that from the inside, Link-1 messages are received from a Link-1 Provider, which is assumed to be a NATO certified system.
- The NATO security policy concerning security principles, personnel security, physical security, security of information and information security (INFOSEC) is mandated for the TOE and its IT environment [NATO-SP]. The IT environment operates within a CLASSIFIED accredited facility for boundary protection devices and crypto devices.
- It is assumed that the operating system does not deny a communication between the two parts of the TOE.

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:

Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Testframe part of the Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5 including the configuration file	1.5	installed on hard-drive
2	SW	Operator Console of the Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5 including the configuration file	1.5	installed on hard-drive
3	DOC	System Installation Manual	1.5	hardcopy
4	DOC	System User Manual	1.5	hardcopy

Table 4: Deliverables of the TOE

The TOE will be installed together with the Trusted Operating System on a hard-drive and then delivered via courier separated from the other hardware.

The hard-drive containing the TOE is a classified registered item and will be handled in accordance with standard NATO procedures for the transport and registration of classified items. In particular the courier certificates assigned to the transport of the hard drive containing the TOE will carry serial numbers of the hard-drive as well as identification and stock numbers. Acknowledgement of proper reception of classified items shall be retransmitted to the registry of the sending party.

In order to protect the integrity of the binary, the TOE performs a self check at its start-up and prints out the calculated CRC checksum of the binary. This checksum will be sent to the final user by a separate letter transported by a courier or NATO secure intranet. The user checks the integrity by comparison of the checksums.

3 Security Policy

The Link-1 messages received by the TOE from a Link-1 providing system may be classified. It is not allowed that these messages or at least the classified parts of these messages will be sent out to partner nations.

Therefore, the classified parts of the messages shall be sanitized in order to be admissible to declassify the message to NATO UNCLASSIFIED/PN RELEASEABLE.

The sanitization and the declassification process shall comply with the NATO declassification policy appropriate for sanitization and declassification of classified information. This policy defines the

- *Filter rules*: The set of rules for the circumstances under which information will be allowed for declassification. This includes the rules for sanitization of (or parts of) classified messages. This rule set can be considered as definition of the NATO declassification policy. The TOE implements these rules.
- *Condition*: The condition for an automated system under which the filter rules are allowed to be applied. The condition is: It shall be retrievable when a classified Link-1 message has been sent out. More specific:
    - It must be prevented that a message with classified content will be sent out
    - It must be retrievable when a unclassified message derived from a classified message
    - It must be retrievable when an unclassified message has been sent out

The TOE and its IT environment must comply with the condition requirements.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

A.U.ONLY_WAY

The TOE assumes that it is the only path for the O.Data_Class to be downgraded to O.Data_Unclass so it can be passed on from an L1-Provider to LIFOS.

4.2 Environmental assumptions

A.E.OUTSIDE

From the outside, attacks can only be performed via a data stream from the Partner Nation. It is assumed that this data stream has to pass a LIFOS and can therefore not reach the TOE.

Therefore, it exist no possibility that incoming messages from the outside interfere with the sanitization and downgrading process.

A.E.INSIDE

It is assumed that from the inside, Link-1 messages are received from a Link-1 Provider, which is assumed to be a NATO certified system.

A.E.RECORDING

The Trusted Operating System keeps a record of all actions on the system on the level of the operating system.

A.E.NATO_SECURITY_POLICY

The NATO security policy concerning security principles, personnel security, physical security, security of information and information security (INFOSEC) is mandated for the TOE and its IT environment. The IT environment operates within a CLASSIFIED accredited facility for boundary protection devices and crypto devices. Application of the policy includes the following:

1. Logical

   a. Only authorized personnel can have access to the Secure_IT_Platform.

   b. Remote access to the Secure_IT_Platform is not allowed.

   c. All users of the Secure_IT_Platform are appropriately identified and authenticated, and have the appropriate access rights and are held accountable for their actions.

   d. No user (program or human) of the Secure_IT_Platform can unintentionally delete, overwrite or manipulate any system programs, logs, or data.

2. Organisational

   a. S.Audit shall immediately notify S.ISSO in case of any threats or vulnerability that impacts P.DECLASSIFICATION_POLICY.

   b. Information shall be used only for its authorized purpose(s).

3. Personnel

   a. The personnel who need access to the TOE or the environment running the TOE must be screened according to site accreditation requirements.

   b. S.SysOper, S.Audit, S.ISSO and S.SysAdmin shall be held accountable for their actions.

   c. Only S.SysOper, S.Audit, S.ISSO and S.SysAdmin shall be able to access O.Data_Class.

4. Physical

   a. The TOE shall be located in a physically secured room within a NATO facility accredited for the site level of accreditation.

   b. Access to this room is restricted to authorized persons listed in access lists.

A.E.TOE_ACCESS_POLICY

S.SysOper is the only user role that is allowed to interact with the TOE.

A.E.INTER-TOE-COMMUNICATION

It is assumed that the operating system does not deny a communication between the two parts of the TOE.

5 Architectural Information

The TOE consists of two software applications. The testframe part and the operator console.

The testframe part is the actual filter and responsible for filtering and forwarding the frames flowing from the Link1 providing system to LIFOS.

The operator console is the interface to the user and controls the filter. It is responsible for getting the input of the human operator. The user is able to input commands at the Operator Console.

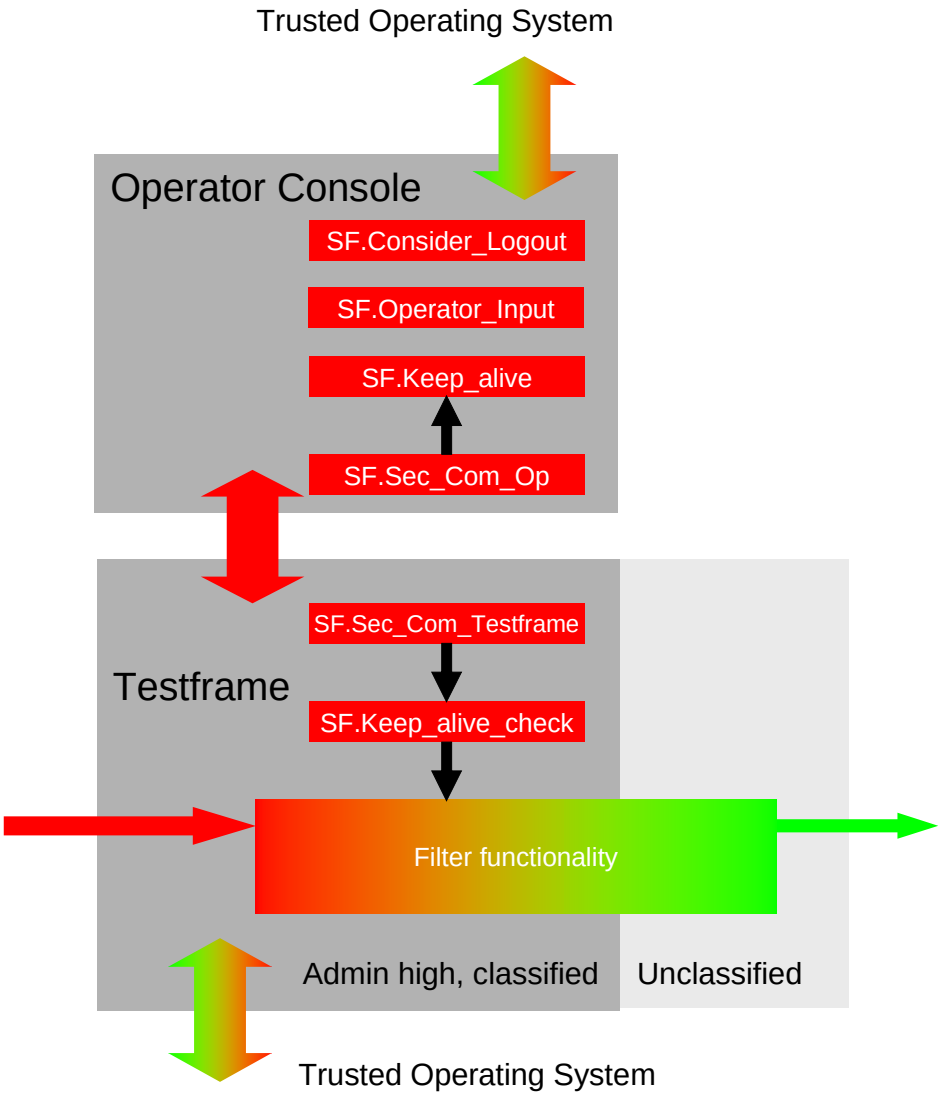

Figure 1: Overview of the Security Functions of the communication functionality and their relation.

6 Documentation

The following documentation belongs to the TOE:

[9] System Installation Manual, Link 1 Forward Filter (LFF) for Air Situation Data Exchange (ASDE) with Partner Nations (PN), Version 1.5, Feb 2007

[10] User Manual, Link 1 Forward Filter (LFF) for Air Situation Data Exchange (ASDE) with Partner Nations (PN), Version 1.5, Feb 2007

7 IT Product Testing

The following figure gives an overview over the test configuration employed by the developer and the evaluator for testing.

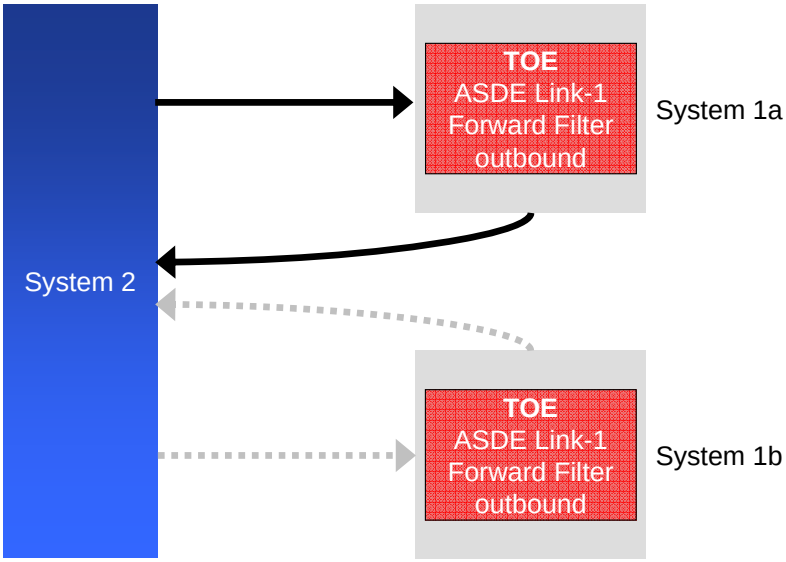

Figure 2: Test Configuration

Figure 2 shows the hardware configuration on a high level. Normally, the tests will be performed on System 1a. System 2 acts as Link-1 providing system and as Partner Nation. For technical reasons, some tests will be performed on System 1b. For these tests, the physical connections between System 1a and System 2 will be unlinked and the physical connection between System 1b and System 2 will be established.

SYSTEM 1a

This system works as ASDE L1FF system and is therefore installed and configured appropriately.

SYSTEM 1b

Some tests cannot be performed on a system running Trusted Solaris 8 because the additional software required for these tests cannot be installed there. Therefore, these tests will be performed on a system running Standard Solaris 8.

This system also works as ASDE L1FF system and is therefore installed and configured appropriately.

The hardware connection from SYSTEM 1a to SYSTEM 2 will be disconnected from SYSTEM 1a and connected to SYSTEM 1b, if appropriate.

The very first test case performs a TOE installation on the SYSTEM 1a. Due to the fact that the installation instructions for the TOE do not cover the installation of the operating system, SYSTEM 1b will be installed without performing a

special test case. It is presupposed that the SYSTEM 1b is already installed and configured at the start of the tests.

SYSTEM 2

This system works as Link-1 providing system and as Partner Nation system and is therefore installed and configured appropriately.

Developer Tests

The developer testing was performed successfully on the evaluated configuration of the TOE.

Complete coverage was achieved for all the TOE security functions as specified in the security target an the functional specification.

The overall test depth of the developer tests comprises the high-level design subsystems and the internal interfaces of those subsystems as required for the assurance level of the evaluation.

Evaluator Tests

A selected subset from the security test suite have been successfully repeated by the evaluation facility. The achieved test results matched the expected results as documented by the developer in the developer test documentation. Furthermore, a set of independent tests has been performed successfully by the evaluation facility.

8 Evaluated Configuration

The Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5 was evaluated in the configuration as described in the ETR [8] and summarised in this certification report. There is only one configuration of the TOE.

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.

The evaluation methodology CEM [2] was used for those components identical with EAL4.

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

The verdicts for the CC, Part 3 assurance components (according to EAL4 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
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the Implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
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
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.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

Assurance classes and components		Verdict
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Independent vulnerability analysis	AVA_VLA.2	PASS

Table 5: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant,
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4.

The results of the evaluation are only applicable to the Outbound Downgrade Filter of ASDE Link-1 Forward Filter version 1.5 as identified in table 4.

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 [9]/[10] 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

AIS Anwendungshinweise und Interpretationen (Guidance and Interpretations)

ASDE Air Situation Data Exchange

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
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
L1	Link-1
L1FF	Link-1 Forward Filter
LIFOS	Link-1 Fibre Optic Secure System
NATO	North Atlantic Treaty Organisation
NC3A	NATO Consultation, Command and Control Agency
PN	Partner Nations
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
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-CC-0342, version 1.12, date of issue: 01.02.2007 , Link1 Forward Filter (L1FF), NATO C3 Agency (confidential document)

[7] Security Target BSI-DSZ-CC-0342, 1.13, date of issue: 06.02.2007 , Link1 Forward Filter (L1FF), NATO C3 Agency (sanitized public document)

[8] Evaluation Technical Report, version 1.0, 13.04.2007, CSC Deutschland Solutions GmbH (confidential document)

[9] System Installation Manual, Link 1 Forward Filter (LFF) for Air Situation Data Exchange (ASDE) with Partner Nations (PN), Version 1.5, Feb 2007

[10] User Manual, Link 1 Forward Filter (LFF) for Air Situation Data Exchange (ASDE) with Partner Nations (PN), Version 1.5, Feb 2007

[11] NATO-MAS, Standardization Agreement Tactical Data Exchange - Link 1 (point-to-point), edition 4 (NATO UNCLASSIFIED)

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.”