Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0305-2006

for

IBM Tivoli Access Manager for Operating Systems Version 5.1 with Fixpack 17

from

IBM Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0305-2006

IBM Tivoli Access Manager for Operating Systems Version 5.1 with Fixpack 17

from

IBM Corporation

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, Part 1 Version 0.6*, *Part 2 Version 1.0 extended by CEM supplementation "ALC_FLR – Flaw remediation", Version 1.1, February 2002* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL3 augmented by ALC_FLR.1 – Basic Flaw Remediation**

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, March 24th, 2006

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 +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

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

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

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

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

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

Contents

Part A: Certification

Part B: Certification Results

Part C: Excerpts from the Criteria

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 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- CEM supplementation on “ALC_FLR – Flaw remediation”, Version 1.1, February 2002

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

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 22 September 2000 in the Bundesanzeiger p. 19445

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 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was 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).

2.2 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 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

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 IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17 has undergone the certification procedure at BSI.

The evaluation of the product IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The developer is:

IBM Corporation
11501 Burnet Road
Austin, TX 78758, USA

The certification is concluded with

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

This work was completed by the BSI on March 24th, 2006.

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-30.

The product IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17 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] IBM Corporation
11501 Burnet Road
Austin, TX 78758, USA

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	3
2	Identification of the TOE	12
3	Security Policy	13
4	Assumptions and Clarification of Scope	14
5	Architectural Information	15
6	Documentation	17
7	IT Product Testing	18
8	Evaluated Configuration	20
9	Results of the Evaluation	21
10	Comments/Recommendations	23
11	Annexes	24
12	Security Target	25
13	Definitions	26
14	Bibliography	28

1 Executive Summary

IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17 is a specific implementation of the access control framework defined by the ISO 10181-3 standard [9] and the Authorization API (aznAPI) [10].

IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17 is a complete authorization solution for Operating Systems. The TOE's authorization services allow an organization to control user access to protected information and resources. By providing a centralized, flexible, and scalable access control solution, the TOE allows secure and well-managed operating systems infrastructures to be built.

In addition to the security policy management feature, the TOE supports authentication decision enforcement for administrative users, the application of login and password policies to user accounts of underlying resources, authorization, data security, secure communication and resource management capabilities.

The product bundle IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17 comprises the following product components, representing the TOE:

- Tivoli Access Manager Base 5.1, with Fixpack 6
  (also called Policy Server in the following)
- Tivoli Access Manager Operating Systems 5.1, with Fixpack 17
  (also called TAMOS Resource Manager in the following)

These two product components in turn comprise several installation packages. Details on these packages and how to obtain them can be found in chapter 2 of this report.

Details on the user guidance documentation delivered with the TOE can be found in chapter 6 of this report.

The operating system platforms the TOE is allowed to run on are the following:

- IBM AIX 5.2
- Sun Solaris 2.8
- HP-UX 11i V1
- RedHat Enterprise Linux AS/WS Version 3 Update 2 on i386 architectures
- Novell SUSE Linux Enterprise Server 8 Service Pack 3 on i386 architectures

For more details on environmental constraints and the evaluated configuration of the TOE please refer to chapters 1.5 and 1.6 of this report. For possible combinations of operating system platforms runing the the Policy Server and TAMOS Resource Manager please refer to the Security Target [7], chapter 2.8.

The IT product IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17 was evaluated by atsec information security GmbH. The evaluation was completed on 15.03.2006. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The developer is:

IBM Corporation
11501 Burnet Road
Austin, TX 78758, USA

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL3 (Evaluation Assurance Level augmented). The assurance level was augmented by ALC_FLR.1 – Basic Flaw Remediation

1.2 Functionality

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

The TOE Security Functional Requirements (SFR) used in the Security Target are Common Criteria Part 2 extended as shown in the following table:

Security Functional Requirement	Identifier
Components taken from CC part 2:	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1(1) & (2)	Audit Review (Policy Server & TAMOS RM)
FAU_SEL.1(1) & (2)	Selective audit (Policy Server & TAMOS RM)
FAU_STG.1	Protected audit trail storage
FCS_CKM.1(1)	Cryptographic key generation (Symmetric algorithms)
FCS_CKM.1(2)	Cryptographic key generation (RSA)
FCS_CKM.2(1)	Cryptographic key distribution (RSA public keys)
FCS_CKM.2(2)	Cryptographic key distribution (Symmetric keys)
FCS_COP.1(1)	Cryptographic operation (RSA)
FCS_COP.1(2)	Cryptographic operation (Symmetric operations)

[8] Information Technology Security Evaluation Facility

Security Functional Requirement	Identifier
FDP_ACC.2(1)	Complete access control (Object-space access control policy)
FDP_ACC.2(2)	Complete access control (Management access control policy)
FDP_ACF.1(1)	Security attribute based access control (Object-space)
FDP_ACF.1(2)	Security attribute based access control (Management)
FIA_AFL.1(1) & (2)	Authentication failure handling (Policy Server & TAMOS RM)
FIA_ATD.1(1) & (2)	User attribute definition (User & Administrator)
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action (Policy Server)
FIA_UID.1	Timing of identification
FIA_UID.2	User identification before any action (Policy Server)
FIA_USB.1	User-subject binding
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1(1)	Management of security attributes
FMT_MSA.1(2)	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RVM.1	Non-bypassability of the TSP
FPT_TRC.1	Internal TSF consistency
FTP_ITC.1	Inter-TSF trusted channel
Componentes not been taken from CC part 2:	
FAU_GEN.3-TAMOS	Audit data generation

Table 1: SFRs claimed for the TOE

Note: only the titles of the Security Functional Requirements are provided here. For more details and application notes please refer to the ST chapter 5.2.1.

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

Security Functional Requirement	Identifier
Components for the LDAP Server located in the TOE environment:	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of user data without security attributes
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
Components for the Operating System underlying the Policy Server:	
FIA_UID.1	Timing of identification
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
Components for the Operating System underlying the TAMOS RM:	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps

Table 2: SFRs claimed for the TOE environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapters 5.3.1 to 5.3.3.

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

TOE Security Function	Addressed issue
F.Audit	Configurable Audit of security relevant events for the Policy Server and the TAMOS RM.
F.Authentication	Authentication of users and administrators. Please note that user authentication is supported by a LDAP server being part of the operational environment of the TOE.
F.Authorization	Authorization decisions of the TOE are based on Access Control Lists (ACL) and “Protected Object Policies” (POP). The following kinds of objects can be protected by the TOE: (i) Operating System Objects (like Files, Directories, Network connections, ...) and (ii) Tivoli Access Manager Management Objects.
F.Management	The TOE provides management functionality for administrators concerning the following aspects: (i) User and group Management, (ii) ACL and POP Management and (iii) TOE Certificate Management.
F.Communication	The TOE uses the SSL v3 protocols to secure the communication between different parts of the TOE and between the TOE and the TOE environment.

Table 3: TOE Security Function

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

1.3 Strength of Function

The TOE’s strength of functions is claimed ‘medium’ (SOF-medium) for specific functions as indicated in the Security Target [7], chapter 5.4 and 6.2.

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

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

The following threats as defined in the Security Target [7], chapter 3.2.1 are averted by the TOE:

Name of Threat	Description
T.BYPASS	An authorized user of a managed resource or network-based attacker accesses resources protected by the TOE in a way that bypasses the TSF, exploiting non-TSF portions of the

Name of Threat	Description
	TOE.
T.COM_ATT	An attacker intercepts the communication between the TOE and an external entity or between distributed parts of the TOE in order to get access to protected information, to impersonate as an authorized user or part of the TOE or to manipulate the data transmitted between the TOE and an external or internal entity.
T.UAACTION	An undetected violation of the TSP may be caused as a result of an authorized user of a managed resource or network-based attacker attempting to perform actions that they are not authorized to do.
T.UAUSER	An authorized user of a managed resource or a network-based attacker may impersonate an authorized user of the TOE. This includes the threat of an authorized user that tries to impersonate as another authorized user without knowing the authentication credentials.

Table 4: Threats to be averted by the TOE

The TOE and its environment has to comply to the following Organisational Security Policy (OSP) (refer to [7], chapter 3.3):

Name of OSP	Description
P.ACCOUNTABILITY	The administrators of the system shall be held accountable for their actions within the system.
P.ADM_DELEGATION	Specific administration tasks as well as management operations to defined subsets of the resources protected by the TOE may be delegated to administrators that are only allowed to perform the management tasks within their defined area of responsibility and are not able to extend this area themselves.

Table 5: Organisational Securit Policies

1.5 Special configuration requirements

The following constraints are given for the TOE (refer also to Security Target [7], chapter 2.7):

1. The evaluated configuration has one Policy Server system and one or more Resource Manager/Authorization Evaluator systems:
   - The Policy Server component of the TOE is installed and operated on a dedicated system within a physically protected environment. Optionally, the TAMOS RM can be installed on the Policy Server.
   - Resource Manager and Authorization Evaluator are always installed and operated on the same system. The evaluated configuration does not include Authorization Evaluator components running on a machine separate from the Resource Manager that uses them.

- All Resource Manager/Authorization Evaluator systems operate independent from each other and are only connected to the central Policy Server.
- The Policy Server and all the Resource Manager/Authorization Evaluator systems only use the operating systems platform combinations as defined in [7], chapter 2.7, Table 1.

2. The following components and/or configurations are not part of the evaluated configuration and must not be used:
   - The use of the Web Portal Manager and integration with the Tivoli Desktop for the administration of the TOE is not supported. Instead only the command line interfaces of pdadmin and TAMOS RM and the pdadmin C API are supported in the evaluated configuration.
   - No Application Development Kit is installed.
   - Active Directory is not supported. Only LDAP is supported as interface to the user registry. Multiple LDAP replicas are supported, whereas the number of LDAP masters in the environment is restricted to one.
   - No hardware encryption device is used. The cryptographic services are fully provided by the software implementation of the GSKit component.
   - Language packs other than English are not supported. Only the English language pack for the TOE is evaluated.
   - Non-certified authentication mechanisms and non-password based authentication mechanisms are not supported. On underlying operating systems managed by TAMOS RM the TOE supports only password-based authentication mechanisms listed in the Administrator Guide for the TAMOS ROM as being certified.
     For administrators requesting access via the pdadmin interface for the Policy Server, only password-based authentication is supported.
   - Weak or no encryption of internal communications. Communication between the LDAP server and the TOE as well as the communication between the Policy Server and the Resource Manager/Authorization Evaluator systems is protected using the SSLv3 protocol with one of the ciphersuites defined in this Security Target. The use of unencrypted communication is disabled in the TOE.
3. The following components of the TAMOS product are not evaluated as part of the TOE, but can be used and are then considered part of the IT environment:
   - The log router daemon operating on the audit log files for remote distribution.
   - The Tivoli Enterprise Console daemon providing audit data for remote access.

4. The following components of the TAMOS product are part of the TOE, but do not contain security functionality that is subject to evaluation:
   - The integrated Watchdog functionality of the TOE.
   - The TCB mechanisms of the TAMOS product, such as checksum verification of files being defined as a member of the TCB.

To install, set-up and use the evaluated configuration of the TOE the guidance documents as outlined in chapter 6 have to be followed.

1.6 Assumptions about the operating environment

The following assumptions about the operating environment are made in the Security Target [7], chapter 3.1. They are reproduced here:

Name of Assumption	Description
A.ADMIN	The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator guidance. Base administrators will perform administration activities from a secure environment using terminals and/or workstations they trust via secured connections to the Policy Server. All administrative commands themselves will be executed on the Policy Server or on a TAMOS RM.
A.BOOT	During operating system startup it is ensured that the TAMOS RM is started before user logins can occur.
A.DIR_PROT	The directory server used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the directory. This includes the assumptions that queries are properly authenticated, that replicas are held consistent according to a well-defined policy, and that communication between TOE and LDAP server is SSL v3 encrypted.
A.FRIENDLY_OS	The underlying operating system of a resource manager works as specified. In particular, the operating system kernel is assumed to be well behaved with regard to the TSF parts operating in kernel mode. It does not alter, hinder or otherwise influence the kernel mode operation of the TOE, it rather supports them.
A.OS_CONF_MGMT	The operating systems of the machines running the TOE are assumed to be configured and maintained by trained and trustworthy personnel such that the underlying systems provide a reliable basis for the operation of the TOE software.
A.PAM	The authentication mechanisms in the underlying operating system for the TAMOS RM effectively identify the operating system users and associate them with correct user IDs. Furthermore, the PAM mechanism (or loadable authentication module mechanism on AIX) enforces the invocation of the TOE's login module, if so configured.
A.PHYS_PROT	The machines running the TOE software need to be protected against unauthorized physical access and modification. All

Name of Assumption	Description
	machines running parts of the TOE software require this protection.
A.PWD_SAFE	Administrators and other users have to protect their passwords used for authentication to the TOE such that no unauthorized access to them is possible.
A.USER	Users of the TOE are not hostile and do not try to deliberately attack the TSF. Especially, they do not possess greater attack potential as assumed in the description of the threat environment for the TOE.
A.USER_PASSWORD	The underlying operating system for a resource manager ensures that users are authenticated.
A.FRIENDLY_LDAP	The LDAP server performs its functions as specified.

Table 6: Assumption for the operational environment

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:

IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Tivoli Access Manager Base comrising the installation packages: • Policy Server (pdmgrd) • Runtime • IBM GSKit • IBM Directory Client (LDAP)	5.1	Secure Download[9]
2	SW	Tivoli Access Manager for Operating Systems comprising the installation packages: • TAMOS • Runtime • IBM GSKit • IBM Directory Client (LDAP)	5.1	Secure Download
3	SW	Fixpack 6 for Tivoli Access Manager Base 5.1 and Fixpack 17 for Tivoli Access Manager for Operating Systems comprising: • Fixpack 6 for Policy Server and Runtime • Fixpack 17 for TAMOS • GSKit 7.0.3.3 • IBM Directory Client 5.2.	see column Identifer	Seucre Download
3	DOC	Guidance documents as outlined in chapter 6 of this report.	see chapter 6	Secure Download

Table 7: Deliverables of the TOE

The installation of the packages as listed above will result in the following component versions, comprising the evaluated configuration:

- Policy Server 5.1.0.6
- TAMOS 5.1.0.17
- Runtime 5.1.0.6
- GSKit 7.0.3.3
- IBM Directory Client 5.2

[9] Only the IBM's Passport Advantage's secure download (Restartable Transfer) applet is allowed for downloading the TOE. Simple HTTP or FTP download is not an evaluated way to get the TOE.

3 Security Policy

The TOE is an implementation of the ISO 10181-3 and the Authorization API (aznAPI) framework. Its main purpose is to provide Authentication and Authorization decisions and allow/deny access to protected resources. This is supplemented by audit functionality, secure communication between TOE components and between the TOE and the outside world. Management functionality as well as non-bypassability is provided as well.

Therefore the Security Policy of the TOE is defined by the following TOE security functional requirements:

- All SFR components being part of the CC class FIA (like FIA_SOS.1 defining the authentication policy constraints).
- Iterations of FDP_ACC.2 and FDP_ACF.1 defining (i) the Object-Space access control policy and (ii) the management access control policy that controls access to resources protected by the TOE.

A detailed description/definition of the Security Policy enforced by the TOE is given in the Security Target [7], chapter 5.2.1.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

The following assumptions are identified as been relevant for a secure TOE usage. A complete definition of these assumptions can be found in [7], chapter 3.1 or chapter 1.6 of this report.

- A.ADMIN
- A.OS_CONF_MGMT
- A.PWD_SAFE
- A.USER

4.2 Environmental assumptions

The following assumptions are related to physical and connectivity aspects. A definition can be found in the Security Target [7], chapter 3.1. They are also provided in chapter 1.6 of this report.

- A.BOOT
- A.DIR_PROT
- A.FRIENDLY_OS
- A.PAM
- A.PHYS_PROT
- A.USER_PASSWORD
- A.FRIENDLY_LDAP

4.3 Clarification of scope

The following threat is not averted by the TOE. Additional support from the operating environment of the TOE is necessary (for detailed information about the threat and how it is covered by the environment refer to the Security Target [7], especially chapter 3.2.2 and chapter 8.1).

TE.BYPASS: An authorized user of a managed resource or network-based attacker accesses resources protected by the TOE in a way that bypasses the TSF due to the absence of protection mechanisms in the underlying system.

In addition the TOE is supported by a LDAP directory server (being part of the operational environment) in performing user authentication. The TOE does also rely on the underlying operating systems.

5 Architectural Information

The TOE is a specific implementation of the access control model defined in [ISO 10181-3] and [AZNAPI]. The overall TOE architecture and boundaries are illustrated in figure 1. The TOE offers the enforcement of Access Control Decisions based on Access Control Policy (ACL) rules. The Authentication Mechanism as well as the “Initiator Security Attributes” Database are implemented using a Directory Server, which holds the user and ACL information and is itself is not part of the TOE. Also the Target system which holds the actual resource to be protected is not part of the TOE.

In this model a user submits a request for a resource (e. g. accessing a file that is protected by the TOE). This request is intercepted by the TOE, which implements access control checking on top of the native operating system functions. The TOE performs the following actions:

- Checking if the requested resource is known to be not protected. If this is true, the request is passed through to the operating system.
- Checking if the user has the right to access the requested resource for the requested operation. If not, the request is rejected. If yes, the request is passed through to the underlying operating system.

To explain how the access rights are checked an overview on the Tivoli Access Manager components is provided first (please see figure 1 for an architectural overview of the TOE):

The “Resource Manager” is implemented as part of the TOE by the TAMOS RM. This component includes also the “Authorization Evaluator” as a subsystem.

The “Policy Server” is responsible to define and maintain the access control policy. It uses the “Master Authorization Policy” database to store the access control policy rules. To speed up the time required to make an access decision, the “Authorization Evaluator” manages a replica of the “Master Authorization Policy”.

The Policy Server informs all Authorization Evaluators about modifications to the “Master Authorization Policy“. An Authorization

Evaluator can also request the Policy Server to submit a new copy of the Master Authorization Policy. Also the Policy Server can request an Authorization Evaluator to update the replica of the Master Authorization Policy to make sure that the Authorization Evaluator has the latest version.

Administration of the TOE is performed via a workstation or terminal directly connected to the Policy Manager component. Only the command line interface and C language API for administration are part of the evaluated configuration.

The TAMOS RM can be further managed by commands provided by the TAMOS RM. These commands can be initiated by an appropriately authorized user logged into the underlying operating system the TAMOS RM is running on.

Administration includes the management of the Master Authorization Policy (defining access rules for protected objects) as well as management of the TOE. It should be noted that access rights of administrators to administrative objects of the TOE are also stored and maintained in the Master Authorization Policy; this specifically includes the management commands provided by the TAMOS RM.

To enhance authentication capabilities the TOE uses modules that extend the native authentication process of the host operating system by applying a login policy defined within the TOE.

For administrator authentication, the TOE uses a directory server. The directory server provides a repository for user and administrator attributes and credentials. Authentication of users is done by the Resource Manager in combination with host operating system, authentication of administrators is performed by the Policy Server by using the external Directory Server.

The communication link between the TOE and the LDAP server is protected using the SSL v3 protocol. The TOE uses the GSKit library for the implementation of those protocols and their underlying cryptographic functions. The GSKit library is therefore part of the Policy Server and part of the Resource Manager. Also, the communication link between the Policy Server and the different Resource Managers is secured by SSL v3 using the GSKit library.

The Master Authorization Policy as well as the Replica Authorization Policy are databases. The Master Authorization Policy is a database held by the Policy Server and the Replica Authorization Policy is a database held by each Authorization Evaluator.

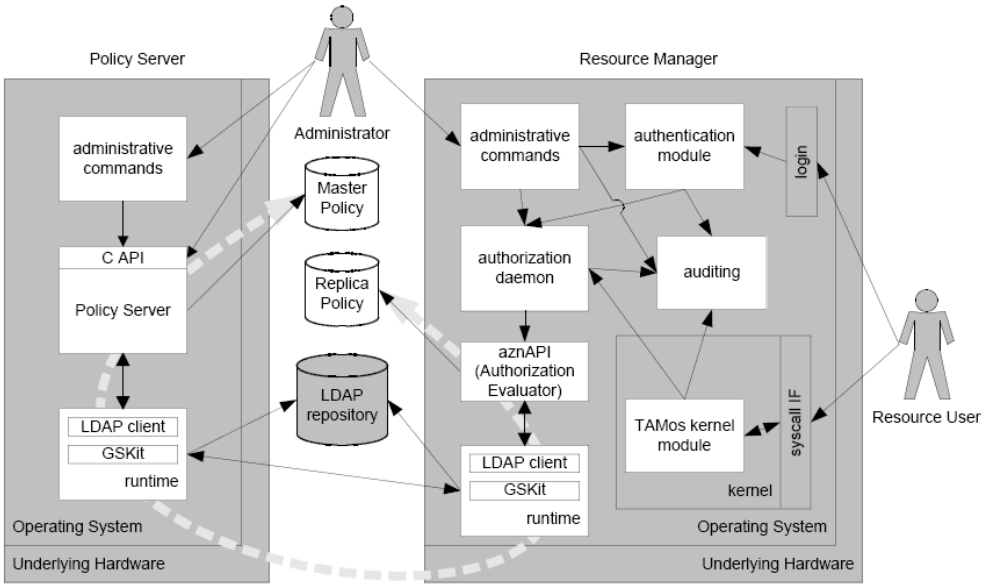

Figure 1: TOE Architecture

6 Documentation

The following documentation is provided with the product and has to be followed for a secure usage of the TOE.

- Base Installation Guide, Version 5.1 (November 2003)
- Base Administrator Guide, Version 5.1 (November 2003)
- TAMOS Installation Guide, Version 5.1 (November 2003)
- TAMOS Administrator Guide, Version 5.1 (November 2003)
- Command Reference, Version 5.1 (November 2003)
- Base Patch 5.1-TAM-FP06 Readme (05 October 2005)
- TAMOS Patch 5.1-PDO-FP17 Readme (16 December 2005)
- Administration C API Developer's Reference (November 2003)
- Error Message Reference (November 2003)
- TAMOS Release Notes (November 2003)
- TAMOS Problem Determination Guide (November 2003)
- Common Criteria Guide (December 2005)

Please note that for the purpose of the certified configuration of the TOE the Common Criteria Guide is the most important document.

7 IT Product Testing

Test configuration:

The evaluated configuration, as specified in the Security Target of IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17, is based on five types of underlying operating systems: IBM AIX 5.2, Sun Solaris 8, HP-UX 11i, SuSE Linux Enterprise Server 8 and Red Hat Enterprise Linux 3. Complete testing on all of these platforms has been carried out.

The notes on secure installation and configuration of the TOE, as provided to the customer, reflect specific constraints and requirements for the evaluated configuration, as mandated by the TOE description, IT security environment and objectives for the TOE environment defined in the Security Target. By requiring the test scenario to be set up according to this guidance, compliance with the evaluated configuration is achieved.

All test scenarios contained a system comprising the Policy Manager (pdmgrd) and the TAMOS RM resource manager of the TOE.

Test coverage/depth:

The developer has provided a test coverage and depth of testing analysis, demonstrating that all aspects of TSF behavior have been tested.

Tests for the evaluated configuration of the TOE have been devised to test all aspects of TSF behaviour, as it has been specified throughout the functional specification and high-level design. A correspondence analysis provided by the developer shows coverage of all TSF, subsystems and interfaces that affect the security functional behaviour of the TOE. The coverage has been determined to be overall sufficient.

Summary of Developer Testing Effort:

Test configuration:

The tests have been carried out on the test configuration as described above.

Testing approach:

To demonstrate that all aspects of TSF behavior are tested the developer used a mixed approach of automated and manual testing.

Complete testing on all of the OS platforms described above have been performed.

Testing results:

The test records of the developer show that all tests on all test platforms were executed successfully, i.e. the actual test results met the expected test results.

Summary of Evaluator Testing Effort:

Test configuration:

All tests were run at the developer's site in Austin, TX. The developer granted access to their testing environment and their network.

The TOE was installed as required by the respective guidance documentation (please refer to chapter 6 of this report).

Testing approach:

A subset of the automated and manual developer tests were re-run and subsequently analyzed for correct results.

In addition a set of own evaluator tests have been devised and performed focusing on different kinds of TOE security functionality.

Testing result:

All evaluator tests on the tested OS platforms were executed successfully.

Evaluator penetration testing:

Penetration tests have been performed by the evaluation facility to assess possible vulnerabilities found during the evaluation of the different CC assurance classes. The TOE withstood the penetration efforts.

8 Evaluated Configuration

The Target of Evaluation is the IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17. The product bundle comprises the following product components, representing the TOE

- Tivoli Access Manager Base 5.1, with Fixpack 6
- Tivoli Access Manager Operating Systems 5.1, with Fixpack 17

These product components in turn comprise several installation packages which are listed in detail in chapter 2 of this report.

A customer has to download all installation packages via a secured internet download. For the evaluated version of the TOE these installation packages have to be updated to Fixpack 6 and Fixpack 17 for the TAM OS part respectively (also available via secure download). Applying this two step installation process will result in the following versions of TOE components:

- Policy Server 5.1.0.6
- TAMOS 5.1.0.17
- Runtime 5.1.0.6
- GSKit 7.0.3.3
- IBM Directory Client 5.2

The operating system platforms the TOE is allowed to run on are the following:

- IBM AIX 5.2
- Sun Solaris 2.8
- HP-UX 11i V1
- RedHat Enterprise Linux AS/WS Version 3 Update 2 on i386 architectures
- Novell SUSE Linux Enterprise Server 8 Service Pack 3 on i386 architectures

For setting up and running the TOE according to the evaluated configuration all guidance documents (refer to chapter 6) and the implications given by the Security Target have to be followed. These implications can also be found in chapter 1.5 and 1.6 of this report.

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 included in evluation levels up to EAL4. In addition the CEM supplementation on "ALC_FLR – Flaw remediation", Version 1.1, February 2002 was used.

The verdicts for the CC, Part 3 assurance components (according to EAL3 augmented by ALC_FLR.1 – Basic Flaw Remediation and the class ASE for the Security Target evaluation) are summarised in the following table:

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

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

Table 8: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- The assurance of the TOE is Common Criteria Part 3 conformant, EAL3 augmented by ALC_FLR.1.
- The following TOE Security Functions fulfil the claimed Strength of Function: F.Authentication (SOF-medium). Please see also chapter 10 of this report for a recommendation.

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

The results of the evaluation are only applicable to the IBM Tivoli Access Manager for Operating Systems, Version 5.1 with Fixpack 17 in the configuration as described in this report.

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

10 Comments/Recommendations

Please note that the likelihood of a password guessing attack (related to the SOF claim) will increase if a customer chooses to use centrally managed user IDs on several resource manager instances and the attack is performed in parallel. To keep the claimed strength of function it is therefore recommended to lock-out an account permanently after three unsuccessful tries.

The operational documents as liste in chapter 6 of this report 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.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
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 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

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

[5] CEM supplementation “ALC_FLR – Flaw remediation”, Version 1.1, February 2002

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

[7] Security Target BSI-DSZ-0305-2006, Version 1.6.5, 2006-02-01, Tivoli Access Manager for Operating Systems 5.1 Security Target, IBM Corporation

[8] Evaluation Technical Report BSI-DSZ-CC-0305-2006, Release 3, 2006-03-15, atsec information security GmbH (confidential document)

[9] ISO/IEC 10181-3: Information Technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework, 1996

[10] Open Group Technical Standard: Authorization (AZN) API, The Open Group, January 2000

Developer Guidance Documentation:

[11] Base Installation Guide, Version 5.1 (November 2003)

[12] Base Administrator Guide, Version 5.1 (November 2003)

[13] TAMOS Installation Guide, Version 5.1 (November 2003)

[14] TAMOS Administrator Guide, Version 5.1 (November 2003)

[15] Common Criteria Guide, (December 2005)

[16] Command Reference, Version 5.1 (November 2003)

[17] Base Patch 5.1-TAM-FP06 Readme (05 October 2005)

[18] TAMOS Patch 5.1-PDO-FP17 Readme (16 December 2005)

[19] Administration C API Developer’s Reference (November 2003)

[20] Error Message Reference (November 2003)

[21] TAMOS Release Notes (November 2003)

[22] TAMOS Problem Determination Guide (November 2003)

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / Final Interpretation 008

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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:

***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.

***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:

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

CC Part 3:

Assurance categorisation (chapter 2.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 2.1."

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class 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
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 9: Assurance family breakdown and map

Evaluation assurance levels (chapter 6)

"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 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 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in chapter 2 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 CC 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 10: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

"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 6.2.2)

"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 6.2.3)

"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 6.2.4)

"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 6.2.5)

"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 6.2.6)

"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 6.2.7)

"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 14.3)

AVA_SOF Strength of TOE security functions

"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 14.4)

AVA_VLA Vulnerability analysis

"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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“