Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0222-2003

for

IBM Tivoli Access Manager for e-business
Version 4.1 with Fixpack 5

from

IBM Corporation

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

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0222-2003

IBM Tivoli Access Manager for e-business
Version 4.1 with Fixpack 5

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)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
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, 16. October 2003

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS-MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

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

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

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[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 “ALC_FLR – Flaw remediation”, Version 1.1, February 2002

---

[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 Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd 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.

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 e-business, Version 4.1 with Fixpack 5 (also shortly called IBM TAM in the remainder of this document) has undergone the certification procedure at BSI.

The evaluation of the product IBM Tivoli Access Manager for e-business, Version 4.1 with Fixpack 5 was conducted by atsec information security GmbH. The atsec is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and developer is:

IBM Corporation
Tivoli Securiy Product Development
Austin, TX – USA

The certification is concluded with

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

This work was completed by the BSI on 16. October 2003.

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-32.

The product IBM Tivoli Access Manager for e-business, Version 4.1 with Fixpack 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 0228/9582-111.

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
Tivoli Security Product Development
9442 Capital of Texas Highway
Austin, TX 78759, 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

IBM Tivoli Access Manager for e-Business 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 e-Business is a complete authorization solution for corporate Web, client/server, Tivoli Access Manager applications, and legacy (pre-existing) applications. Tivoli Access Manager authorization allows an organization to securely control user access to protected information and resources, by providing a centralized, flexible, and scalable access control solution. Tivoli Access Manager is used in conjunction with standard Internet-based applications to build secure and well-managed intranets.

At its core, the TOE provides Authentication and Authorization services for protected objects. This core functionality is supplemented by an audit functionality, secure communication between TOE components and between the TOE and its environment. The TOE offers functionality to securely administer the aspects described above.

The product bundle Tivoli Access Manager for e-business 4.1 with Fixpack 5 comprises the following product components, representing the TOE

- Tivoli Access Manager Base 4.1, with Fixpack 5 for Base
- Tivoli Access Manager WebSEAL 4.1, with Fixpack 5 for WebSEAL

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:

- AIX 5.2
- Solaris 8
- Windows 2000 Advanced Server SP3
- SuSE Linux Enterprise Server 8

For more details on environmental constraints and the evaluated configuration of the TOE please refer to chapter 1.5 of this report.

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

Security Functional Requirement	Identifier
SFRs from CC Part 2:	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit Review
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
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)
FDP_ACC.2(1)	Complete access control
FDP_ACC.2(2)	Complete access control
FDP_ACF.1(1)	Security attribute based access control
FDP_ACF.1(2)	Security attribute based access control
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-authenticating
FIA_UID.1	Timing of identification
FIA_UID.2	User identification before any action
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

Security Functional Requirement	Identifier
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

The IT product IBM Tivoli Access Manager for e-business, Version 4.1 with Fixpack 5 was evaluated by atsec information security GmbH. The evaluation was completed on 07 October 2003. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor and developer is:

IBM Corporation
Tivoli Securiy Product Development
Austin, TX – 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 part C of this report, or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL3 (Evaluation Assurance Level 3). The assurance level 3 is augmented by:

ALC_FLR.1 – Basic flaw remediation.

For the evaluation of the CC component ALC_FLR.1 the mutually recognized CEM supplementation “ALC_FLR – Flaw remediation”, Version 1.1, February 2002 ([3]) was used.

1.2 Functionality

The TOE provides the following Security Functions (please refer to the Security Target [7], chapter 6.1 for a complete listing and precise definition):

F.Audit

Configurable Audit of security relevant events.

[8] Information Technology Security Evaluation Facility

F.Authentication

Authentication of users and administrators. In the case of administrators successful audit is required before they can perform any administrative action. In the case of users, defined access to defined resources may be possible for users that are not authenticated. The administrator can define for which resources user authentication is necessary and for which not.

F.Authorization

Authorization decisions of the TOE are based on Access Control Lists (ACL) and “Protected Object Policies” (POP). Three different kind of objects can be protected by the TOE: (i) Web Objects, (ii) Tivoli Access Manager Management Objects and (iii) User-defined 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 and TLS v1 protocols to secure the communication between different parts of the TOE and between the TOE and the TOE environment.

1.3 Strength of Function

The TOE’s strength of function is rated ‘medium’ (SOF-medium) for the password based authentication of clients as part of the security function F.Authentication (refer to Security Target [7], chapter 6.2).

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). Therefore the strength of the cryptographic algorithms used in F.Communication to implement the SSLv3 and TLSv1 protocols (including the generation of keys and certificate based authentication) have not been rated.

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

A summary of the threats defined in [7], chapter 3.2.1 is provided here. For the precise description of the threats please refer to [7]:

T.BYPASS:

An attacker accesses protected resources of the TOE bypassing the TSF, exploiting non-TSF portions of the TOE.

T.UAACTION:
An undetected violation of the TSP may be caused as a result of an attacker (possibly, but not necessarily, a person allowed to use the TOE) attempting to perform actions that the individual is not authorized to do.

T.UAUSER:
An attacker (possibly, but not necessarily, a person allowed to use the TOE) 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.

T.COM_ATT:
An attacker intercepts the communication between the TOE and an external entity or between different parts of the TOE in order to get access to confidential 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.

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

P.AUTHORIZED_USERS:
Only those users who have been authorized to access web resources protected by the TOE may access those resources after they have been successfully authenticated (unless a protected web resource is defined to be accessible by unauthenticated users, in which case no prior authentication is required).

P.AUTHORIZED_ADMIN:
Only administrators authorized for access to defined management resources of the TOE may access those resources after they have been successfully authenticated.

P.NEED_TO_KNOW:
The system must allow to limit the access to, modification of, and destruction of the information in protected web resources to those authorized users which have a “need to know” for that information.

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 web 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.

1.5 Special configuration requirements

The TOE is an implementation of the ISO 10181-3 and the Authorization API (aznAPI) framework. This framework knows the following logical components:

- Policy Server
- Authorization Evaluator
- aznAPI
- Resource Manager

For more details on these components refer to the architectural description in this report (chapter 5) or the information provided in the Security Target (chapters 2.1 to 2.6)

The following constraints are given for the TOE:

- The Policy Server component of the TOE is installed and operated on a dedicated system that communicates via a network connection to the Resource Manager / Authorization Evaluator.
- The Resource Manager and Authorization Evaluator are installed and operated on the same system. They communicate with each other via a library interface (the aznAPI). They communicate with the Policy Server via a network connection with a dedicated application layer protocol running over SSL v3 or TLS v1.
  Note that the evaluated configuration does not include Authorization Evaluator components running on a machine separate from the Resource Manager that uses them.
- The evaluated configuration has one Policy Server and one or more Resource Manager / Authorization Evaluator systems. All Resource Manager / Authorization Evaluator systems operate independent from each other and are only connected to the central Policy Server.
  Load balancing and failover configurations of Resource Manager / Authorization Evaluator systems are therefore not supported in the evaluated configuration.
  The SOF-Claim for password based authentication holds true for four instances of Resource Manager / Authorization Evaluator systems. So only four Resource Manager / Authorization Evaluator systems are allowed in the evaluated configuration.
- The Policy Server and all the Resource Manager / Authorization Evaluator use the same operating system as a basis. Configurations using different operating system platforms for different components of the TOE are not part of the evaluated configuration.
- Communication between client systems and the TOE, the web server systems and the TOE, 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 SSL v3 or TLS v1 protocol with one of the cipher suites defined in the Security Target, chapter 6.1.5. Please refer to chapter 5 of this report or to the Security Target (chapters 2.1 to 2.6) for a more detailed description of the TOE architecture.
The use of unencrypted communication is disabled in the TOE. Also the use of version 2 of the SSL protocol is disabled for communication to client systems and target systems. Within the TOE all components are configured to use SSL v3 or TLS v1. The external LDAP server also needs to support SSL v3 or TLS v1 and has to be configured to use either of those as its preferred protocol.
For the SSL/TLS cipher suites supported by the TOE refer to the Security Target [7], chapter 6.1.5.

- No hardware encryption device is used. The cryptographic services are fully provided by the software implementation of the GSKit component.
- The TOE is configured to use password based authentication and SSL client certificate based authentication for the authentication of users. Other authentication mechanisms for user authentication are disabled.
- The TOE is configured to use password based authentication for administrators that request access to the TOE via the pdadmin interface.
- The use of the Web Portal Manager component for the administration of the TOE is **not** supported. Instead only the command line interface of pdadmin and a C language API are supported in the evaluated configuration.
- No Application Development Kit is installed in the evaluated configuration.
- Only LDAP is supported for the access to the directory server. Active Directory or other protocols are not supported. LDAP Replica are also not supported.
  Please note that the LDAP server used by the TOE is not part of the TOE.

Policy Server and all Resource Manager / Authorization Evaluator within an evaluated configuration use the same operating system platform (but run on different machines). Those platforms have to be one of the following:

- AIX 5.2
- Solaris 8
- Windows 2000 Advanced Server SP3
- SuSE Linux Enterprise Server 8

No explicit restrictions on the usable hardware were made in the Security Target [7].

To install, set-up and use the evaluated configuration of the TOE the guidance documents [11], [12], [13], [14], [15], [16], [17], [18] and [19] 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. The are reproduced here:

A.NOBYPASS:
It has to be ensured that protected resources can not be accessed in a way that bypasses the TOE. All internal and external access attempts to protected resources have to be channeled through the TOE.

A.CLIENT_KEYMAN:
Users have to administer and protect private keys of their client system used for authentication and key exchange with the TOE in a secure way. This includes the secure generation of strong keys as well as the protection of private keys against any kind of unauthorized access and use.

A.CLIENT_PWMAN:
Users have to protect their passwords used for authentication to the TOE such that no unauthorized access to them is possible.

A.ADM_PWMAN:
Administrators have to protect their passwords used for authentication to the TOE such that no unauthorized access to them is possible.

A.PHYS_PROT:
The machines running the TOE software need to be protected against unauthorized physical access and modification. All machines running parts of the TOE software require this protection.

A.SINGLE_APP:
Any machine used to run all or a part of the TOE software are assumed to be used solely for this purpose and are not used to run other application software except those required for the management and maintenance of the underlying operating system and hardware.

A.OS_CONF_MGMT:
The operating system of the machines running the TOE are assumed to be configured and maintained by trained and trustworthy personnel such that the operating system provides a reliable basis for the operation of the TOE software. Especially it is assumed that the operating system is configured such that no unauthorized access to functions provided by the operating system software (including network daemons) is possible either locally or via any network connection.

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 documentation. They 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.

A.USER:

Users of the TOE are not hostile and trying to deliberately attack the TSF. They also carefully protect their authentication information within their operating environment.

A.DIR_PROT:

The directory server used by the TOE provides protection mechanism against unauthorized access to TSF data stored in the directory. This includes the requirement for authentication when accessing user entries and the configuration to use SSL v3 or TLS v1 as the preferred protocol to protect the communication links.

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 is called:

IBM Tivoli Access Manager for e-business, Version 4.1 with Fixpack 5

The product bundle comprises the following product components, representing the TOE

- Tivoli Access Manager Base 4.1, with Fixpack 5 for Base
- Tivoli Access Manager WebSEAL 4.1, with Fixpack 5 for WebSEAL

These product components in turn comprise several installation packages which are listed here:

- Tivoli Access Manager Base CD-ROM image. It has to be obtained via IBM's Passport Advantage's secure download (Restartable Transfer) applet. In case of AIX 5.2, Solaris 8, Windows 2000 SP3: version 4.1.0.0 has to be downloaded; In case of SuSE Linux Enterprise Server 8: version 4.1.0.2 is required to be downloaded. The images comprise:
  - Policy Server (pdmgrd)
  - Runtime
  - IBM GSKit
  - IBM Directory Client (LDAP)
- Tivoli Access Manager Web Security (also known as WebSEAL) CD-ROM image. It has to be obtained via IBM's Passport Advantage's secure download (Restartable Transfer) applet. In case of AIX 5.2, Solaris 8, Windows 2000 SP3: version 4.1.0.0; in case of SuSE Linux Enterprise Server 8: version 4.1.0.2 has to be downloaded. The images comprise:
  - WebSEAL (webseald)
  - Runtime
  - IBM GSKit
  - IBM Directory Client (LDAP)
- Fixpack 5 for Tivoli Access Manager Base 4.1 and Fixpack 5 for Tivoli Access Manager WebSEAL, has to be obtained on a dedicated CD-ROM for the evaluated configuration from IBM Customer Support, comprising
  - Fixpack 5 for Policy Server and Runtime
  - Fixpack 5 for WebSEAL and Runtime
  - GSKit 5.0.5.74
  - IBM Directory Client 4.1 with Fixpack 2.

A customer has to download the installation images for Tivoli Access Manger Base and WebSEAL via a secured internet download. For the evaluated version

of the TOE these installation images have to be updated to Fixpack 5 (delivered on CD-ROM) which can be ordered via registered mail. Applying this two step installation process will result in the following versions of TOE components:

Tivoli Access Manager Base:

- Policy Server (pdmgrd), Version 4.1.0.5
- Runtime, Version 4.1.0.5
- IBM GSKit, Version 5.0.5.74
- IBM Directory Client (LDAP), Version 4.1 with Fixpack 2

Tivoli Access Manager WebSEAL:

- WebSEAL (webseald), Version 4.1.0.5
- Runtime, Version 4.1.0.5
- IBM GSKit, Version 5.0.5.74
- IBM Directory Client (LDAP) , Version 4.1 with Fixpack 2

Note: 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.

The following Guidance Documents are part of TOE delivery and have to be followed to ensure a secure installation and usage of the TOE: [11], [12], [13], [14], [15], [16], [17], [18], [19].

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 Web-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 5.1.1.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on personnel assumptions defined in [7], chapter 3.1 the following usage conditions exist:

- Users have to administer and protect private keys of their client system used for authentication and key exchange with the TOE in a secure way. This includes the secure generation of strong keys as well as the protection of private keys against any kind of unauthorized access and use. (A.CLIENT_KEYMAN)

- Users have to protect their passwords used for authentication to the TOE such that no unauthorized access to them is possible. (A.CLIENT_KEYMAN)

- Administrators have to protect their passwords used for authentication to the TOE such that no unauthorized access to them is possible. (A.ADM_PWMAN)

- Any machine used to run all or a part of the TOE software are assumed to be used solely for this purpose and are not used to run other application software except those required for the management and maintenance of the underlying operating system and hardware. (A.SINGLE_APP)

- The operating system of the machines running the TOE are assumed to be configured and maintained by trained and trustworthy personnel such that the operating system provides a reliable basis for the operation of the TOE software. Especially it is assumed that the operating system is configured such that no unauthorized access to functions provided by the operating system software (including network daemons) is possible either locally or via any network connection. (A.OS_CONF_MGMT)

- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation. They 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. (A.ADMIN)

- Users of the TOE are not hostile and trying to deliberately attack the TSF. They also carefully protect their authentication information within their operating environment. (A.USER)

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [7], chapter 3.1):

- It has to be ensured that protected resources can not be accessed in a way that bypasses the TOE. All internal and external access attempts to protected resources have to be channeled through the TOE. (A.NOBYPASS)

- The machines running the TOE software need to be protected against unauthorized physical access and modification. All machines running parts of the TOE software require this protection. (A.PHYS_PROT)

- The directory server used by the TOE provides protection mechanism against unauthorized access to TSF data stored in the directory. This includes the requirement for authentication when accessing user entries and the configuration to use SSL v3 or TLS v1 as the preferred protocol to protect the communication links. (A.DIR_PROT)

4.3 Clarification of scope

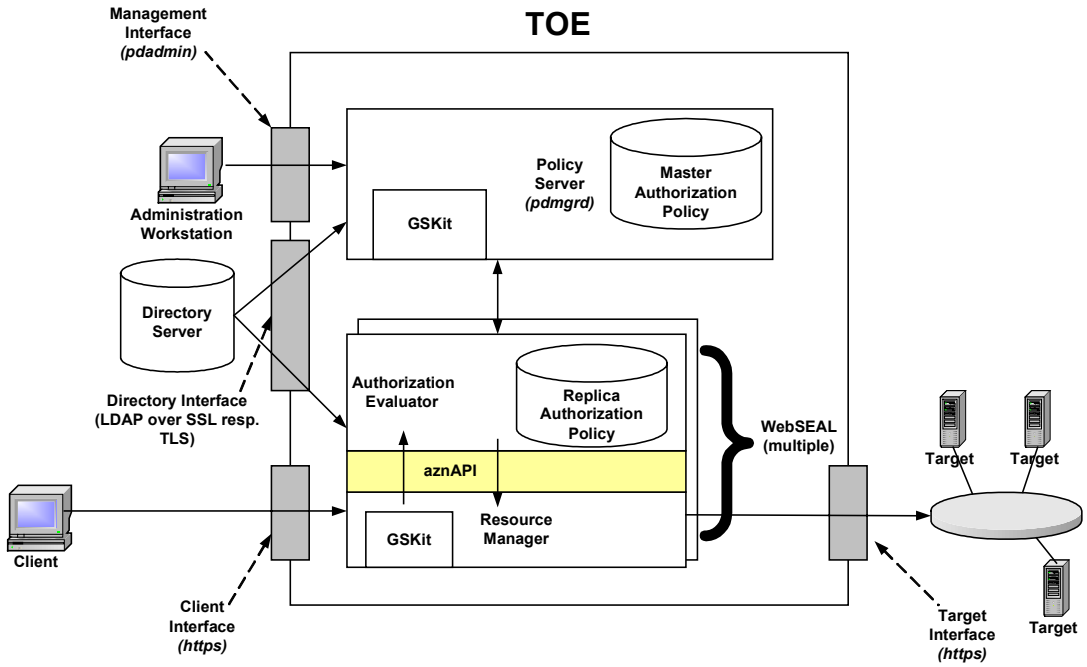
The following threat is not averted by the TOE. Additional support from the operating environment of the TOE is necessary (for detailed information about the threat and how it is covered by the environment refer to the Security Target [7], especially chapter 3.2.2 and chapter 8.1).

TE.GET_CRED:

An attacker may obtain credentials within the TOE environment that allow him to impersonate an authorized TOE user, or get unauthorized access to the directory information.

5 Architectural Information

The TOE is a specific implementation of the access control model defined in the ISO 10181-3 [9] and the Authorization API [10]. The overall TOE architecture is illustrated in the following figure where the biggest box indicates the TOE boundary.



The TOE offers the enforcement of Access Control Decisions based on Access Control Policy (ACL) rules. A Database storing user credentials is implemented using a Directory Server, which itself is not part of the TOE. Also the Target system which has the actual resource to be protected is not part of the TOE.

In this model a user on a client submits a request for a resource (e. g. accessing a URL on a network protected by the TOE). This request is intercepted by the TOE (much in the same way as an application gateway firewall system intercepts network requests). The TOE performs the following actions:

- Checking if the requested resource is protected but accessible to unauthenticated users. If this is true, the request is passed through.
- Checking if the user has already been authenticated (i. e. there is a protected session where the user has been authenticated). If not, and authentication is required for the target of the access attempt, the user is required to authenticate (this is the case for password based authentication. Certificate based authentication will always take place when the session is established). This authentication makes use of an external Directory Server which stores user attributes and user credentials.

- Checking if the user has the right to access the requested resource in the requested mode. If not, the request is rejected. If yes, the request is passed through to the server holding the resource (the TOE works like a reverse proxy here).

The “Resource Manager” is implemented within the TOE by the WebSEAL component. 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”.

Administration of the TOE is done via a command line interface or C language API in the evaluated configuration. The C language API may be used by an organization to define its own tools to automate some of the administration tasks. Such tools are not part of the evaluated configuration and it is up to the organization to ensure that those tools perform their task correctly.

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.

To perform authentication the TOE uses an external directory server supporting the LDAP protocol. The directory server is used as a repository for user and administrator attributes and credentials. Authentication of users is done by the Resource Manager, authentication of administrators is performed by the Policy Server and both use the external Directory Server as the authentication mechanism.

The communication links between the TOE and the LDAP server as well as between the TOE and the client systems and the TOE and the target systems is protected using the SSL v3 or TLS v1 protocol. Also the communication link between the Policy Server and the Resource Manager is secured by SSL v3 respectively TLS v1.

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.

6 Documentation

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

[11] Base Installation Guide, Version 4.1 (August 2003)

[12] Base Administrator Guide, Version 4.1 (August 2003)

[13] WebSEAL Installation Guide, Version 4.1 (August 2003)

[14] WebSEAL Administrator Guide, Version 4.1 (August 2003)

[15] Command Reference, Version 4.1 (August 2003)

[16] Base and Web Portal Manager, Patch 4.1-TAM-FP05 Readme (01 October 2003)

[17] WebSEAL Patch 4.1-AWS-FP05 Readme (20 August 2003)

[18] Administration C API Developer's Reference (August 2003)

[19] Error Message Reference (August 2003)

Please note that also the information provided in the Security Target [7] and this report have to be followed.

7 IT Product Testing

Test configuration

The evaluated configuration, as specified in the Security Target [7], is based on four types of underlying operating systems: IBM AIX 5.2, Sun Solaris 8, Microsoft Windows 2000 Advanced Server (SP3) and SuSE Linux Enterprise Server 8.

The TOE, as tested according to the test plans, is IBM Tivoli Access Manager for e-business, Version 4.1 with Fixpack 5 consisting of the two components (i) Tivoli Access Manager Base 4.1 with Fixpack 5, and (ii) Tivoli Access Manager WebSEAL with Fixpack 5.

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 was achieved. For details on the guidance documents please refer to chapter 6 of this report.

All test scenarios contained at least one system comprising the Policy Manager (pdmgrd) and one system comprising the WebSEAL resource manager of the TOE. For some test multiple resource managers more than one WebSEAL instance were part of the test scenario.

Test coverage/depth

The developer has provided a test coverage and depth of testing analysis, demonstrating that all aspects of TSF behavior are 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, whereas in general a lot of manual interaction of the testers is required.

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). In addition for some tests a cygwin environment was used.

Testing approach:

Automated and manual developer tests were re-run and subsequently analyzed for correct results.

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

Testing result:

All evaluator test were executed successfully on all OS platforms.

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 e-business, Version 4.1 with Fixpack 5. The product bundle comprises the following product components, representing the TOE

- Tivoli Access Manager Base 4.1, with Fixpack 5 for Base
- Tivoli Access Manager WebSEAL 4.1, with Fixpack 5 for WebSEAL

These product components in turn comprise several installation packages which are listed here:

- Tivoli Access Manager Base CD-ROM image. It has to be obtained via IBM's Passport Advantage's secure download (Restartable Transfer) applet. In case of AIX 5.2, Solaris 8, Windows 2000 SP3: version 4.1.0.0 has to be downloaded; In case of SuSE Linux Enterprise Server 8: version 4.1.0.2 is required to be downloaded. The images comprise:
  - Policy Server (pdmgrd)
  - Runtime
  - IBM GSKit
  - IBM Directory Client (LDAP)
- Tivoli Access Manager Web Security (also known as WebSEAL) CD-ROM image. It has to be obtained via IBM's Passport Advantage's secure download (Restartable Transfer) applet. In case of AIX 5.2, Solaris 8, Windows 2000 SP3: version 4.1.0.0; in case of SuSE Linux Enterprise Server 8: version 4.1.0.2 has to be downloaded. The images comprise:
  - WebSEAL (webseald)
  - Runtime
  - IBM GSKit
  - IBM Directory Client (LDAP)
- Fixpack 5 for Tivoli Access Manager Base 4.1 and Fixpack 5 for Tivoli Access Manager WebSEAL, has to be obtained on a dedicated CD-ROM for the evaluated configuration from IBM Customer Support, comprising
  - Fixpack 5 for Policy Server and Runtime
  - Fixpack 5 for WebSEAL and Runtime
  - GSKit 5.0.5.74
  - IBM Directory Client 4.1 with Fixpack 2.

A customer has to download the installation images for Tivoli Access Manger Base and WebSEAL via a secured internet download (for more details refer to chapter 2). For the evaluated version of the TOE these installation images have

to be updated to Fixpack 5 (delivered on CD-ROM) which can be ordered via registered mail. Applying this two step installation process will result in the following versions of TOE components:

Tivoli Access Manager Base:

- Policy Server (pdmgrd), Version 4.1.0.5
- Runtime, Version 4.1.0.5
- IBM GSKit, Version 5.0.5.74
- IBM Directory Client (LDAP), Version 4.1 with Fixpack 2

Tivoli Access Manager WebSEAL:

- WebSEAL (webseald), Version 4.1.0.5
- Runtime, Version 4.1.0.5
- IBM GSKit, Version 5.0.5.74
- IBM Directory Client (LDAP) , Version 4.1 with Fixpack 2

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

- AIX 5.2
- Solaris 8
- Windows 2000 Advanced Server SP3
- SuSE Linux Enterprise Server 8

No explicit restrictions on the usable hardware were made in the Security Target [7].

Please note that

- the operating systems and the underlying hardware platforms,
- the Directory Server and
- the Web Server (also called Target System, refer to chapter 5 of this report)

are **not part of the TOE**.

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 Common Evaluation Methodology [2], the requirements of the Scheme [4] and all interpretations and guidelines of the Scheme (AIS) [5] as relevant for the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL3 with ALC_FLR.1 augmentation and the Security Target evaluation) are summarised in the following table:

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

The evaluation has shown that the TOE fulfils the claimed strength of function (SOF-medium) for the authentication function based on passwords as part of the security function F.Authentication. To ensure that this rating holds true not more than four instances of Resource Manager / Authorization Evaluator systems (WebSEAL) are allowed to be used in the evaluated configuration of the TOE.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). Therefore the strength of the cryptographic algorithms used in F.Communication to implement the SSLv3 and TLSv1 protocols (including the generation of keys and certificate based authentication) have not been rated.

The TOE has no vulnerabilities which are obvious or exploitable in the intended operating environment.

The results of the evaluation are only applicable to the product IBM Tivoli Access Manager for e-business, Version 4.1 with Fixpack 5 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [7] and the chapters 2, 4 and 8 of this report). The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, and if the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The User Guidance documentation (refer to chapter 6 of this report) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [7] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

A customer has to download the installation images for Tivoli Access Manger Base and WebSEAL using IBM's Passport Advantage's secure download (Restartable Transfer) applet. A simple HTTP or FTP download is not allowed for the evaluated TOE. This has to be imposed by a note on the download page of IBM's Passport Advantage download program.

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

API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IT	Information Technology
ITSEF	IT Security Evaluation Facility
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
SSL	Secure Socket Layer Protocol
TLS	Transport Layer Security Protocol
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] CEM supplementation “ALC_FLR – Flaw remediation”, Version 1.1, February 2002

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

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

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

[7] Security Target BSI-DSZ-0222-2003, Version 1.7, 2003-09-30, Tivoli Access Manager for e-Business 4.1 with Fixpack 5, IBM Corporation

[8] Evaluation Technical Report BSI-DSZ-0222-2003, Version 1.0, atsec information security GmbH, 2003-10-06

[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

User Guidance Documentation:

[11] Base Installation Guide, Version 4.1 (August 2003)

[12] Base Administrator Guide, Version 4.1 (August 2003)

[13] WebSEAL Installation Guide, Version 4.1 (August 2003)

[14] WebSEAL Administrator Guide, Version 4.1 (August 2003)

[15] Command Reference, Version 4.1 (August 2003)

[16] Base and Web Portal Manager, Patch 4.1-TAM-FP05 Readme (01 October 2003)

[17] WebSEAL Patch 4.1-AWS-FP05 Readme (20 August 2003)

[18] Administration C API Developer’s Reference (August 2003)

[19] Error Message Reference (August 2003)

– This page was 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 2.1 -Assurance family breakdown and mapping“

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 6.1 - 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.“