Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0237-2006

for

IBM Tivoli Identity Manager
Version 4.6

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-0237-2006

IBM Tivoli Identity Manager Version 4.6

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:

PP Conformance:	**Protection Profile BSI-PP-0024-2006**
Functionality:	**BSI-PP-0024-2006 conformant plus product specific extensions 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. February 2006

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

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)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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 29 October 1992, Bundesgesetzblatt I p. 1838, 2019

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 Identity Manager, Version 4.6 has undergone the certification procedure at BSI.

The evaluation of the product IBM Tivoli Identity Manager, Version 4.6 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and distributor is:

IBM Corporation
600 Anton Blvd
Costa Mesa, CA 92626, 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. February 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 Identity Manager, Version 4.6 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
600 Anton Blvd
Costa Mesa, CA 92626, 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

The Target of Evaluation (TOE) is the IBM Tivoli Identity Manager (also refered as ITIM hereafter). It is compliant to the Identity Management Protection Profile (IMPP), Version Number 1.17, 12 January 2006, BSI registration ID: BSI-PP-0024-2006 [9].

The IBM Tivoli Identity Manager (ITIM) provides a solution for central management of users and their accounts on different systems in a network. Each employee of an organization is represented by an identity within the ITIM server. Within ITIM, there exist a way of interacting with services (i.e. the systems) in a network infrastructure to manage accounts on these services. This interaction is provided by ITIM connectors that direct the management of accounts to so-called adapters. By defining within ITIM which identity shall have access to which of the services managed by ITIM, ITIM is able to provide appropriate information for account creation for that identity to each of these services, or managed resources.

Identities within ITIM can be grouped by membership to Organizational Roles, or roles. Such Organizational Roles are intended to reflect the roles that exist within an organization that uses ITIM for identity management. Organizational Roles are used by Provisioning Policies to determine which identities accounts on which managed resources. A Provisioning Policy defines a number of services and attributes a user shall have on these services (e.g. membership of groups on the service) and is associated with dedicated Organizational Roles.

An identity may be member of an ITIM Group, or group. This requires an identity to be entitled to the ITIM service, i.e. to have an account on the ITIM server (this is not the case per se for the identities managed by ITIM). ITIM Groups specify the kind of access a user has on ITIM. Fine grained access control is then performed by evaluating ACIs (Access Control Item, i.e. ITIM specific access control policies) that delegate specified rights to ITIM Groups.

The IT product IBM Tivoli Identity Manager, Version 4.6 was evaluated by atsec information security GmbH. The evaluation was completed on 02. February 2006. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor and distributor is

IBM Corporation
600 Anton Blvd
Costa Mesa, CA 92626, USA

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL3 (Evaluation Assurance Level 3 augmented by ALC_FLR.1 – Basic flaw remediation). For the evaluation of the CC component ALC_FLR.1 the mutually regognised CEM supplementation “ALC_FLR – Flaw remediation”, Version 1.1, February 2002 ([6]) was used.

1.2 Functionality

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

The following SFRs are taken from CC part 2:

Security Functional Requirement	Identifier
SFRs from CC Part 2 for the TOE, contained in IMPP	
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FDP_ACC.1 (ETC)	Subset access control
FDP_ACC.2 (ACF)	Complete access control
FDP_ACF.1 (ACF)	Security attribute based access control
FDP_ACF.1 (ETC)	Security attribute based access control
FDP_ETC.2	Export of user data with security attributes
FIA_AFL.1	Authentication failure handling
FIA_ATD.1 (ACF)	User attribute definition
FIA_ATD.1 (ETC)	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
FMT_MSA.1	Management of security attributes
FMT_MSA.3 (ACF)	Static attribute initialisation
FMT_MSA.3 (ETC)	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-bypassability of the TSP
FPT_TDC.1	Inter-TSF basic TSF data consistency

SFRs for the TOE taken from CC Part 2

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

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

Security Functional Requirement	Identifier
SFRs from CC Part 2 for the TOE environment, contained in IMPP	
FAU_STG.1	Protected audit trail storage
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency
FTP_ITC.1	Inter-TSF trusted channel

SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.2.

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

TOE Security Function	Addressed issue
F.I&A	Identification and authentication The TOE identifies users (including administrators) by user name and authenticates them by password.
F.Authorization	Authorization (access control) The ITIM server performs authorization for user actions, commonly referred to as requests, based on Access Control Item (ACI).
F.Auditing	Auditing The TOE is capable of auditing internal events (e.g. the modification of provisioning policies or the creation of new users) by generating audit information for all transactions that is stored in a data base provided by the IT environment.

TOE Security Function	Addressed issue
F.Provisioning	Provisioning The TOE provides, by means of connectors and adapters for managed resources, user credentials to managed resources.
F.Data_Feed	Service Reconciliation and Identity Feeds The TOE provides the capability of gathering account information from managed resources. Reconciliation retrieves and compares user information stored on a managed resource with the corresponding data stored in the Tivoli Identity Manager database.

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 the F.I&A security function (as indicated in the Security Target [7], chapter 6).

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

Since the Security Target claims conformance to the IMPP, all threats and OSPs defined there (refer to [9], chapter 3.2 and 3.3) are applied for the TOE as well. The defined threats and policies are summarized below.

Threats:

- T.BYPASS (bypassing the TSF)
- T.COM_ATT (intercepting the communication / manipulation of transmitted data)
- T.UNAUTHORIZED (access to information by an unauthorised user)

Organizational Security Policies:

- P.ACCOUNTABILITY (accountability of the user for security-relevant transactions)
- P.FEED (Proper association between data imported into the TOE and corresponding data already existent in the TOE)
- P.PROVISION (Restrictions for provisioning of accounts)

1.5 Special configuration requirements

The configuration requirements for the TOE are defined in chapter 2.8 of the Security Target [7] and are summarised here (for the complete information please refer to the Security Target):

- Only adapters that are part of the evaluated configuration of the TOE (i.e. the adapters identified are allowed to be used). No other adapters in the IT

environment may be connected to the TOE, including LDAP or vendor specific adapters.

- The ITIM server component of the TOE is installed and operated on a dedicated Web Application Server that communicates via network connections with clients, adapters and the resources in the IT environment (e.g. LDAP registry, RDBMS) as supportive to the TOE.
- Only the English user interface (and guidance) is to be used.
- The TOE must not be operated in a multi-tenant setup.
- The usage of low-level APIs (as opposed to the exported API) to extend the functionality of the TOE's Core Services by plugging in user-specific extensions is prohibited.
- The Web Application Server and MQSeries are installed on one dedicated machine that is physically and logically protected. Clustering is disabled.
- The Directory Server and RDBMS are installed either together on one or separated on two systems. They are for dedicated use by the TOE only and configured accordingly (e.g. restricted network availability). The underlying machine(s) are dedicated to run only these applications.
- All network communication is protected, either by cryptographic (SSL / TLS) or organizational (restricted network access) means.
- Access to network sockets opened by adapters for configuration with the agentCfg tool is restricted to "root" users, or administrators, on the local operating system hosting the adapter. High quality passwords must be set for the adapter configuration.
- Single Sign-On is not supported.

1.6 Assumptions about the operating environment

The assumptions about the operating environment required for the evaluated configuration are defined in chapter 2.8 of the Security Target [7]. They are summarised below (for the complete information please refer to the Security Target):

- The underlying operating environment for the ITIM server is IBM WebSphere Application Server 5.1 as specified in section 2.7, the JDK as distributed with this WebSphere version and the embedded JMS engine, as delivered with the single-server installation process for the TOE.
- The underlying operating systems for the adapters that are part of the evaluated configuration are
  - Windows Server 2003 Enterprise Edition for the Windows AD Adapter
  - Windows Server 2003 Enterprise Edition for the Oracle Database Adapter for Windows

- The interface provided by the IT environment for the Oracle Database Adapter for Windows is the Oracle Client Software version 9i.
- IBM Tivoli Directory Server Version 5.2 with Fix Pack 2 as LDAP v3 compatible directory server.
- The Relational Database Management System (or, transaction database) is either
  - IBM DB2 Universal Database Enterprise Edition server and IBM DB2 runtime client, Version 8.2
  - Oracle Version 9i
  - Microsoft SQL Server 2000
- Mozilla 1.7 and Microsoft Internet Explorer 6.0 with Service Pack 1 for access to the presentation services (i.e. the user and administration interface), using the Java Runtime Environment provided with them.

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 Identity Manager, Version 4.6

The TOE consists of IBM Tivoli Identity Manager (ITIM) Server, ITIM Oracle Database Adapter for Windows, and ITIM Windows AD Adapter. For the evaluated configuration, the TOE is only provided as installation image via IBM's Passport Advantage distribution channel. Therefore, all relevant documentation for the TOE including user and administrator guidance and guidance for the secure installation and configuration of the TOE, is provided online at IBM's web site (see also chapter 6 of this report and documents [10] to [16]). Additional guidance where to find the appropriate documents on IBMs web sites can be found in [16].

3 Security Policy

The TOE decides in its notion of subjects between persons and users. While the TOE Security Functions (TSF) are primarily focused on users of the TOE, the TSP also aim at protecting information related to identities that are not users of the TOE itself. The different subjects are as follows:

A person (or, identity) is identified by name and further information associated with her or him, e.g. aliases and membership of an Organizational Role. Persons are part of an Organization or Organizational Unit within the organizational hierarchy managed by the TOE.

An user (or, ITIM user) is a person having an account on the TOE, i.e. the person has been provisioned with an account for the ITIM service. He is able to access the TOE's user or administrative interfaces, to authenticate against the TOE, and is subject to access control and auditing performed by the TOE. The term user includes all users of the TOE regardless of their role.

A group (or, ITIM group) is a concept to represent a number of dedicated users by membership. Groups relate to the ITIM service and can be subject of Access Control Item. All users that are members of a group which is subject to an ACI are therefore subject to that ACI.

An organizational role is a similar concept than a group, representing a number of persons (as opposed to users). It is used for people management, e.g. when it comes to the definition of provisioning policies. Association of a person with a role may be achieved e.g. by position of the person in the organization's hierarchy. All persons that are assigned to an organizational role which is subject to a Provisioning Policy are subject to this Provisioning Policy.

Persons can be provisioned with accounts on a remote service, or on the ITIM service. While the latter makes a user out of a person in terms of the TOE Security Policy, the term account does not refer to a not further specified resource (e.g., a Windows machine or Oracle Database), but to the concept of service entitlement and provisioning in general.

Before a person can be associated with ITIM groups or organizational roles, there needs to exist an identity in ITIM representing the person. Upon creation, identities are assigned to an Organization or subordinated elements within a organization tree (i.e. business units). ITIM provides the concept of Organizations, which can be organized on lower hierarchies by defining Locations, Organizational Units, Administrative Domains, and Business Partner Organizations.

A more detailed description/definition of the Security Policy enforced by the TOE is given in the Security Target [7], chapter 2.2 and 2.5.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the Organisational Security Policies to which the TOE complies the following usage assumptions arise:

- P.ACCOUNTABILITY (accountability of the user for security-relevant transactions)
- P.FEED (Proper association between data imported into the TOE and corresponding data already existent in the TOE)
- P.PROVISION (Restrictions for provisioning of accounts)

Based on the personnel assumptions the following usage conditions consist:

- A.ADMIN (The system administrative personnel are well trained to securely and trustworthy administer all aspects of TOE operation)
- A.USER (Users of the TOE will protect their passwords used for authentication against the TOE)

For a detailed description of the usage assumptions refer to the Security Target [7], especially chapter 3.1 and 3.3.

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (for more details, please refer to Security Target [7], chapter 3.1.2):

- A.PHYS_PROT (The machines providing the runtime environment for the TOE need to be protected against unauthorized physical access and modification)
- A.AGENT (It is assumed that the runtime environment for an adapter operates as specified with respect to the interfaces exposed to the TOE for exchange of account information)
- A.DIRECTORY (The directory server used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the directory)
- A.RDBMS (The RDBMS used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the data base)
- A.SERVER (The machines providing the runtime environment for all parts of the TOE other than adapters 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 system and hardware.

4.3 Clarification of scope

The threat listed below has to be averted in order to support the TOE security capabilities but is not addressed by the TOE itself. It has to be addressed by the operating environment of the TOE (for detailed information about the threats and how the environment can cover them refer to the Security Target [7], chapter 3.2).

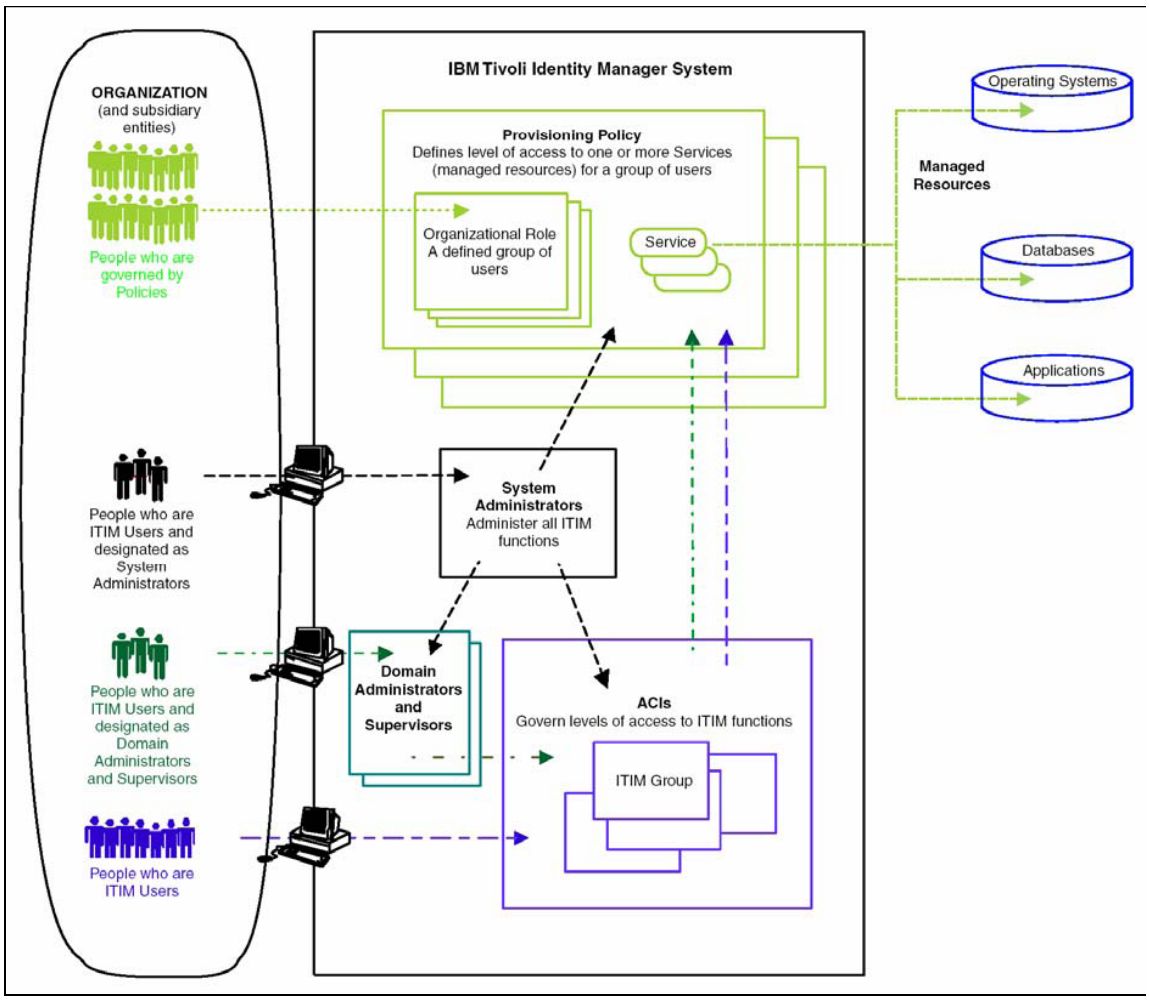
- TE.COM_ATT (An attacker intercepts communication between the TOE and an external entity or between different parts of the TOE)

5 Architectural Information

The target of evaluation (TOE) is the IBM Tivoli Identity Manager (ITIM), Version 4.6.

The IBM Tivoli Identity Manager (ITIM) provides a solution for central management of users and their accounts on the different systems in a network. Each employee of an organization is represented by an identity within the ITIM server. ITIM has a way of interacting with services (i.e. the systems) in a network infrastructure to manage accounts on these services. This interaction is provided by ITIM connectors that direct the management of accounts to so-called adapters: software that sits either directly on the remote system, e.g. on the operating system, interacting with the user management mechanisms of the operating system, or on a central adapter server with network interfaces to the managed system. By defining within ITIM which identity shall have access to which of the services managed by ITIM, ITIM is able to provide appropriate information for account creation for that identity to each of these services, or managed resources.

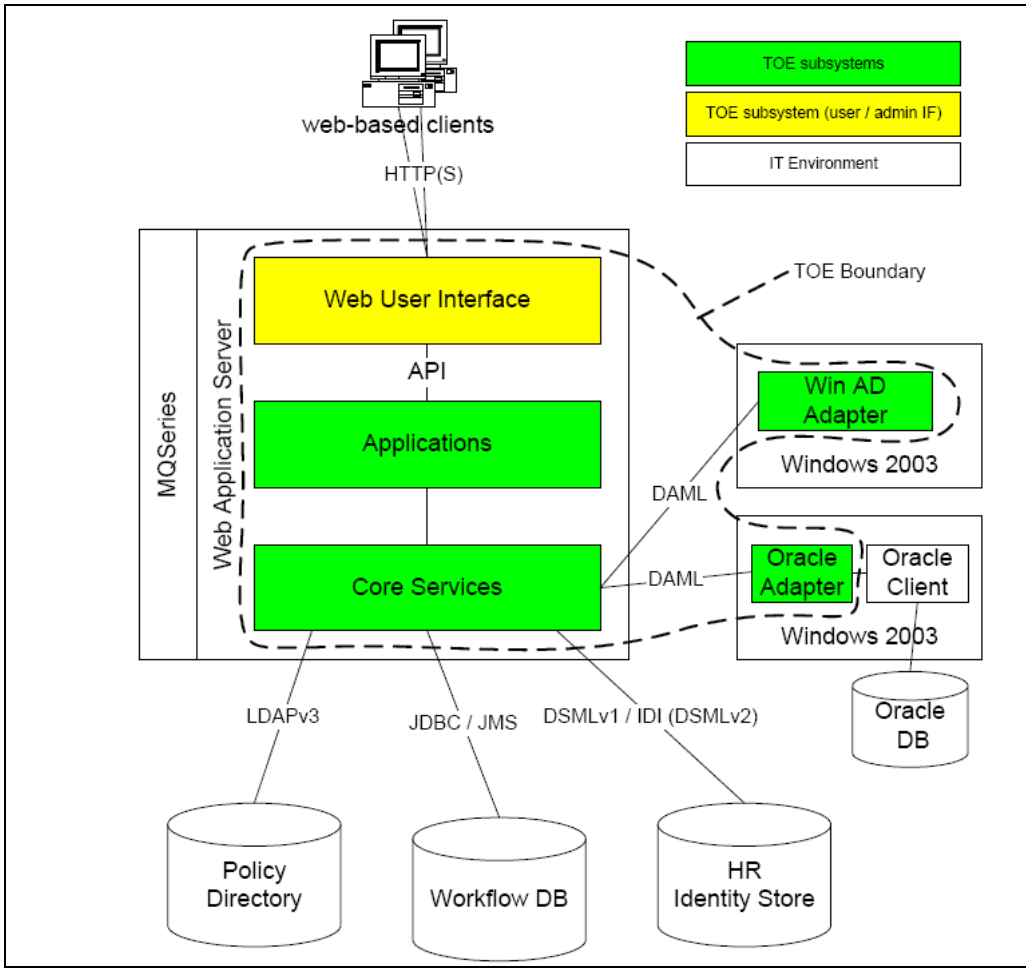
In the following picture, a basic overview of the ITIM architecture is given.



The ITIM server component is completely based on the Java 2 Platform, Enterprise Edition (J2EE) technology. The ITIM server component relies on services in the IT environment provided by the J2EE framework as implemented by the Web Application Server. There are different services provided by the Web Application Server, including J2EE services and interfaces to these services, HTTP and HTTPS, interfaces, Java Transaction Service (JTS), Remote Method Invocation (RMI) APIs, and more. For a complete description of the ITIM server including these services, please refer to the Security Target [7], chapter 2.6

The ITIM adapters run directly on native operating systems and have been implemented in native programming languages (mostly C and C++). They rely on the services provided by these operating systems in terms of runtime environment, and interact with the managed resources via the interfaces provided for user account management by the managed resources (in case of the Windows AD Adapter this is the Active Directory Server Interface (ADSI), and in case of the Oracle Database Adapter for Windows this is the Oracle Client Software).

The following figure provides a general overview of the TOE with parts in the yellow/green shaded area indicating the parts that implement the TSF:



6 Documentation

The following guidance documentation is delivered to the user:

- “Common Criteria Guide”, Version 4.6, August 2005
- Archive holding the API documentation for customers
- “Server Installation and Configuration Guide for WebSphere Environments”, First Edition, June 2005
- “Oracle Adapter for Windows Installation Guide”, Sixth Edition, June 2005
- “Planning for Deployment Guide”, First Edition, June 2005
- “Active Directory Adapter Installation and Configuration Guide”, Ninth Edition, June 2005
- ITIM Online Help and Information Center, http://publib.boulder.ibm.com/tividd/td/ITIM/wwhelp46/en_US/HTML/en/wwhelp/wwhelp/wwhimpl/js/html/wwhelp.htm, Version 4.6
- “Release Notes”, Second Edition, June 2005
- “Problem Determination Guide”, Second Edition, June 2005

To install and configure the TOE such that it matches the configuration described in the Security Target the user has to follow the guidance provided in “Common Criteria Guide”, “Server Installation and Configuration Guide for WebSphere Environments”, “Oracle Adapter for Windows Installation Guide”, “Active Directory Adapter Installation and Configuration Guide”, and “ITIM Online Help and Information Center”.

7 IT Product Testing

7.1 Summary of developer testing effort

Test configuration

The test configuration used for developer testing covers different permutations of:

- Operating systems: AIX 5.2, AIX 5.3, Windows 2003, SLES8 on xSeries, RHEL3, Solaris 9
- WebSphere application server version 5.1.1, 5.1.1.1, 5.1.1.2, 5.1.1.3
- Databases: DB2 8.1 FP7, DB2 8.2 (equals to DB2 8.1 FP8), Oracle 9.0.2.1, MSSQL Server 2000
- LDAP servers: SunOne 5.2, IDS 5.2
- Browsers: Mozilla 1.6, Mozilla 1.7, Internet Explorer 6
- Configuration: single system or systems allocated on several servers

In addition, the adapter test documents outline the configuration needed for testing the adapters. This includes the specification of the software components needed for testing. These documents also state which adapter versions have been tested: Windows AD adapter 4.6.2 and Oracle adapter version 4.6.1.

The developer has performed his tests on the above listed platforms.

It was verified that testing covers the different implementations of security functionality offered by the software (storing of TOE data, protection of TOE execution domain, providing of reliable time stamps). Since all different implementations have been tested, the remaining software systems do not differ in their security functionality.

Testing approach

The test cases for general testing are maintained in a Lotus Notes database called TTT whereas the test cases for adapter testing are maintained in separate documents. Since almost all test cases are manual test cases using the WebGUI, the test procedures provide step-by-step instructions for establishing initial test conditions, executing the test instructions, validating the test results and performing cleanup work.

The test cases for verifying the API functionality instruct the tester to use a test tool called "SHOCK". The test tool provides its own setup instructions to produce initial test conditions. These instructions explain how to set up the LDAP database to include the required entries and attributes.

Test result

The test results maintained in the TTT tool for the general test cases and in the adapter test documents for the adapter test cases show that the following stages of testing were performed:

- functional tests of components
- regression tests

The test results list for each test result verdict of the respective test case. All test results from all tested platforms show that the expected test results are identical to the actual test results.

Test coverage

Since a mapping provided by the developer shows that the tests cover all individual TSF identified for the TOE, it could be verified that all TSFI are covered with testing. This therefore satisfies the requirements for the evaluation.

Test depth

Since a mapping of test cases to subsystems of the high-level design is provided by the developer, it could be verified that all subsystems are covered by test cases. Using the high-level design, the coverage of internal interfaces was shown.

7.2 Summary of evaluator testing effort

Test configuration

The following software has been installed by the evaluator (on a system preinstalled with Windows 2003 server):

- DB2 8.1 FixPack 8 (equals to 8.2)
- ITDS 5.2 and FixPack 2
- WebSphere application server (WAS) 5.1 with FP1, CF1, CF3 (resulting in version 5.1.1.1)
- ITIM server version 4.6 (build 5707 according to the footer of the WebGUI)
- Windows AD adapter 4.6.2
- Oracle adapter 4.6.1

The evaluator installed the software as outlined in the installation guidance for the ITIM server as well as for the adapters. After successful installing the evaluator applied the configuration outlined in the CC guide. Each configuration aspect has been covered by the evaluator in order to bring the system in its evaluated configuration.

Evaluator tests performed

In addition to repeating a sampled subset of the developer tests, the evaluator devised tests for a subset of the TOE. For choosing this subset, the evaluator performed sampling based on the functionality the test cases test.

Test results

The tests were performed at the at the developer's facility. The systems available for testing are listed above.

All test cases devised by the evaluator passed successfully, i.e. the actual test results matched the expected results.

Also for all the developer test cases rerun by the evaluator the actual test results matched the expected results. Therefore this testing also passed successfully.

Evaluator penetration testing

The evaluator has devised a set of penetration tests based on the developer's vulnerability analysis and based on the evaluator's knowledge of the TOE gained by the other evaluation activities. All penetration tests have been based on suspected obvious vulnerabilities. The evaluator conducted those tests and did not find any test that resulted in a penetration of the TOE with low attack potential. Also the vulnerability analysis did not identify any vulnerability that could be exploited with low attack potential. Therefore the evaluator has determined as a result of his activities that the TOE is resistant against attacks with low attack potential.

8 Evaluated Configuration

According to the Security Target the evaluated configuration of the TOE and its IT environment are defined as follows (refer also to the Security Target [7]):

- Only adapters that are part of the evaluated configuration of the TOE (i.e. the adapters identified) are to be used. No other adapters in the IT environment may be connected to the TOE, including LDAP or vendor specific adapters. The adapters that are part of the evaluated configuration use the DAML protocol (as opposed to FTP) for communication with the ITIM server.
- The ITIM server component of the TOE is installed and operated on a dedicated Web Application Server that communicates via network connections with clients, adapters and the resources in the IT environment (e.g. LDAP registry, RDBMS) as supportive to the TOE.
- “Event notifications” of adapters (remote password synchronization) and identity feeds are not supported in the evaluated configuration. The DSML and IDI identity feeds are operated by using their reconciliation functionality.
- Only the English user interface (and guidance) is to be used.
- The TOE must not be operated in a multi-tenant setup.
- The usage of low-level APIs (as opposed to the exported API) to extend the functionality of the TOE’s Core Services by plugging in user-specific extensions is prohibited.
- The Web Application Server and MQSeries are installed on one dedicated machine that is physically and logically protected. Clustering is disabled.
- The Directory Server and RDBMS are installed either together on one or separated on two systems. They are for dedicated use by the TOE only and configured accordingly (e.g. restricted network availability). The underlying machine(s) are dedicated to run only these applications.
- All network communication is protected, either by cryptographic (SSL / TLS) or organizational (restricted network access) means.
- Access to network sockets opened by adapters for configuration with the agentCfg tool is restricted to “root” users, or administrators, on the local operating system hosting the adapter. High quality passwords must be set for the adapter configuration.
- Single Sign-On is not supported.

The evaluated configuration of the TOE restricts the choice of products that can be selected by the customer to fulfill the dependencies of the ITIM server on its IT environment to the following products:

- The underlying operating environment for the ITIM server is IBM WebSphere Application Server 5.1 as specified in section 2.7, the JDK as distributed with

this WebSphere version and the embedded JMS engine, as delivered with the single-server installation process for the TOE.

- The underlying operating systems for the adapters that are part of the evaluated configuration are
  - Windows Server 2003 Enterprise Edition for the Windows AD Adapter
  - Windows Server 2003 Enterprise Edition for the Oracle Database Adapter for Windows
- The interface provided by the IT environment for the Oracle Database Adapter for Windows is the Oracle Client Software version 9i.
- IBM Tivoli Directory Server Version 5.2 with Fix Pack 2 as LDAP v3 compatible directory server.
- The Relational Database Management System (or, transaction database) is either
  - IBM DB2 Universal Database Enterprise Edition server and IBM DB2 runtime client, Version 8.2
  - Oracle Version 9i
  - Microsoft SQL Server 2000
- Mozilla 1.7 and Microsoft Internet Explorer 6.0 with Service Pack 1 for access to the presentation services (i.e. the user and administration interface), using the Java Runtime Environment provided with them.

For setting up / configuring the TOE all guidance documents (especially the documents [10] to [13]) have to be followed (refer also to chapter 6 of this report).

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [5] 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 (this includes especially the methodology for flaw remediation, [6]).

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

The verdicts for the CC, Part 3 assurance components (according to EAL3 augmented by ALC_FLR.1 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
Life cycle support	CC Class ALC	PASS

Assurance classes and components		Verdict
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 1: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conform to the Identity Management Protection Profile (IMPP), Version Number 1.17 [9]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- 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: SF F.I&A (Identification and authentication)

The results of the evaluation are only applicable to the IBM Tivoli Identity Manager, Version 4.6 used in its evaluated configuration (refer to the Security Target [7] and chapter 8 of this report).

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

10 Comments/Recommendations

The operational documents [10] to [13] contain necessary information about the usage of the TOE and all security hints therein have to be considered. 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.

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

ACI	Access Control Item
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
DSML	Directory Services Markup Language
EAL	Evaluation Assurance Level
LDAP	Lightweight Directory Access Protocol
IMPP	Identity Management Protection Profile
ITIM	IBM Tivoli Identity Manager
IT	Information Technology
J2EE	Java 2 Platform, Enterprise Edition
PP	Protection Profile
RDBMS	Relational Data Base Management System
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
UML	Unified Modeling Language
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
WAS	Web Application Server
XML	Extensible Markup Language

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

[6] Application Notes and Interpretations of the Scheme AIS33, Version 2 – “Methodologie zur Fehlerbehebung – Flaw Remediation”, 26.07.2002

[7] IBM Tivoli Identity Manager 4.6 Security Target (BSI-DSZ-CC-0237), Version 1.41, 12 January 2006, IBM Corporation

[8] Evaluation Technical Report, Version 2.0, atsec security information GmbH, 01 February 2006, (confidential document)

[9] Identity Management Protection Profile (IMPP), Version Number 1.17, 12 January 2006, IBM Corporation; BSI registration ID: BSI-PP-0024-2006

[10] Common Criteria Guide, Version 4.6, August 2005

[11] Active Directory Adapter Installation and Configuration Guide, Ninth Edition, June 2005

[12] Server Installation and Configuration Guide for WebSphere Environments, First Edition, June 2005

[13] Oracle Adapter for Windows Installation Guide, Sixth Edition, June 2005

[14] Planning for Deployment Guide, First Edition, June 2005

[15] Problem Determination Guide, Second Edition, June 2005

[16] ITIM Online Help and Information Center, http://publib.boulder.ibm.com/tividd/td/ITIM/wwhelp46/en_US/HTML/en/wwhelp/wwhelp/wwhimpl/js/html/wwhelp.htm, Version 4.6

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 2: 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 3: 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.