Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0235

for

IBM Tivoli Directory Server
Version 5.2

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-0235-2004

IBM Tivoli Directory Server
Version 5.2

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* 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**

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, 02. March 2004

The President of the Federal Office
for Information Security

IT Security Certified

Dr. Helmbrecht L.S. 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)

---

[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, Japan in November 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 Directory Server Version 5.2 has undergone the certification procedure at BSI. It is a re-certification of BSI-DSZ-CC-0207-2003.

The evaluation of the product IBM Tivoli Directory Server Version 5.2 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, and vendor is the IBM Corporation.

The certification is concluded with

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

This work was completed by the BSI on ##. February 2004.

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 Directory Server Version 5.2 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
11501 Burnet Road
Austin, TX 78758 - USA

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) is IBM Tivoli Directory Server Version 5.2 (also called ITDS in short). ITDS is an implementation of the Lightweight Directory Access Protocol (LDAP) and meets the requirements of LDAP Version 3 as defined in RFC 2251–2256 and LDAP Version 2 as defined in RFC 1777.

It is a re-certification of BSI-DSZ-CC-0207-2003. The TOE includes additional functionality and is certified at a higher Evaluation Assurance Level. For more details refer to the Security Target [6].

LDAP is essentially a specialised database where the update operation is less frequent and dedicated to the common goal within the enterprise on consolidating and unifying the management of identity. IBM Tivoli Directory Server is built for identity management with role supports, fine-grained access control and entry ownership.

The IBM Tivoli Directory Server is a software product only, delivered over the Internet as a package including

- the TOE (the LDAP server and the administration daemon executables),
- user and administrative tools (like IBM Directory Server Client SDK 5.2 or the Web Administration Tool),
- a WebSphere Application Server,
- and an IBM DB2 database.

Note: Although delivered together with the TOE, the user and administrator tools, the WebSphere Application Server and the DB2 database are all excluded from the TOE and are considered part of the environment. **The TOE comprises the LDAP server and the administration daemon executables only.**
The TOE environment can also include applications that are not delivered with the IBM Directory Server, but are used as unprivileged tools, for example the Netscape browser needed to administrate the TOE or the Adobe Acrobat Reader to access the supplied online documentation.

The TOE provides the following evaluated security functionality:

- Identification and authentication
- Access control
- Auditing
- Management
- Reference mediation

To ensure a secure usage, a set of guidance documents is provided together with ITDS. Details can be found in chapter 6 of this report.

The TOE can use a variety of different hardware and operating system platforms to operate on. For the operating systems used during the evaluation of the TOE please refer to chapter 2 and 7. Please note that no hardware is provided with the TOE.

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	Functionality
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.2	Complete access control
FDP_ACF.1	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_UID.1	Timing of identification
FMT_MOF.1a[8]	Management of security functions behaviour
FMT_MOF.1b	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-bypassability of the TSP

[8] Notation of SFR component iteration: FXX_XXX.ya means iteration “a” of the SFR FXX_XXX.y

The TOE “IBM Tivoli Directory Server Version 5.2” was evaluated by:

atsec information security GmbH
Steinstraße 70
81667 München
Germany

The evaluation was completed on February 08, 2004. The atsec information security GmbH is an evaluation facility recognised by BSI (ITSEF)[9].

The sponsor and developer is:

IBM Corporation
11501 Burnet Road
Austin, TX 78758
USA

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see 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).

1.2 Functionality

The TOE ITDS provides the following Security Functions:

Name	Function
Audit	
F.AUDIT.1	Audit Generation
Access Control	
F.ACCESS_CONTROL	Access control to particular LDAP operations
Identification & Authentication	
F.I&A.1	Identification & authentication of TOE user
Management	
F.MANAGEMENT.1	Management of the Roles Directory Administrator, Administrative Group Members and End User
F.MANAGEMENT.2	Management of the authentication functionality
F.MANAGEMENT.3	Management of authorisation on directory entries

[9] Information Technology Security Evaluation Facility

Name	Function
F.MANAGEMENT.4	Management of audit functionality
Reference Mediation	
F.REF_MEDIATION	Non-bypassability of the TSF

Note: Only the titles of the SF and a short summary are provided here because they are very granular and almost self-explanatory. For a precise definition of the SF please refer to the Security Target ([6], chapter 6.1).

1.3 Strength of Function

The TOE's strength of function is claimed SOF-basic for password based user authentication (SFR FIA_SOS.1) only.

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

A summary of the threats defined in [6], chapter 3.2.1 is provided here. For the precise description of the threats please refer to [6]:

T.ENTRY:
Unauthorised, malicious access to a resource/information protected by the TOE.

T.ACCESS:
Unauthorised execution of operations.

T.ACCOUNT:
Security relevant actions occur without awareness by Directory Administrators.

T.BYPASS:
Bypass of the TOE security functions.

Please note that T.ACCESS is not entirely averted by the TOE. Instead, additional support from the TOE's environment is needed. For information which parts are averted by the TOE and which by the environment of the TOE, please refer to [6], chapter 8.1 (Security Objective Rationale) and to chapter 4.3 of this report.

The TOE has to comply to the following Organisational Security Policy (OSP).

P.PUBLIC:
Of the information under the control of the TOE, only public information should be made available to unauthenticated or anonymous users.

1.5 Special configuration requirements

According to the Security Target the TOE can be run on

- Microsoft Windows 2000,
- IBM AIX 5.2,
- Sun Solaris 8,
- HP UX-11i
- Red Hat Advanced Server 3.0, and
- SuSE Linux Enterprise Server 8.

Please note that

- the underlying hardware and the operating system used by the Directory Server,
- the Database used as back-end data store,
- the LDAP clients,
- the SSL module used for the protection of the path between the LDAP clients and the server and between LDAP servers and
- the replication service between LDAP servers

are **not part of the TOE.** They are hence out of evaluation scope. Please refer to [6], chapter 2.3 for more information.

No explicit restrictions on the usable hardware were made in the Security Target [6].

1.6 Assumptions about the operating environment

The following constraints concerning the operating environment are made in the Security Target.

The following constraints are based on the assumptions defined in [6], chapter 3.1. They are summarised here:

A.PHYSICAL

The TOE is operated in a physically secure environment.

A.NOEVIL

The TOE Administrators (i.e. the Directory Administrator and the Administrative Group Members) and TOE Environment Administrators are trustworthy to perform discretionary actions in accordance with security policies and not to interfere with the abstract machine (i.e. the hardware and operating system software the TOE runs on).

A.ADMIN

The TOE and TOE environment are competently installed and administered.

A.COMM

It is assumed that communication links between the TOE and LDAP clients (on external systems) are protected against unauthorised modification and disclosure of communication data.

A.COOP

Authorised end users are trusted and expected to act in a co-operating manner in a benign environment.

A.TIME

It is assumed that a reliable time function is provided by the TOE environment.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation is called:

IBM Tivoli Directory Server Version 5.2

The IBM Tivoli Directory Server is a software product only, delivered over the Internet as a package including:

Component	TOE / Not TOE
IBM Tivoli Directory Server package	
The LDAP daemon executable and Administration daemon executable.	TOE
Installation and Configuration Tools and GSKit 6 (SSL package only)	Not TOE
User and administrative tools (like the IBM Directory Server Client SDK 5.2 or the Web Administration Tool).	Not TOE
A WebSphere Application server.	Not TOE
A IBM DB2 database.	Not TOE

Note: Although delivered together with the TOE, the user and administrator tools, the WebSphere Application server and the DB2 database as well as GSKit, Installation and Configuration Tools are all excluded from the TOE. They are considered to be part of the environment. **The TOE is the LDAP server and the administration daemon executables only.**
The TOE environment can also include applications that are not delivered with the IBM Tivoli Directory Server, but are used as unprivileged tools, for example the Netscape browser needed to administrate the TOE or the Adobe Acrobat Reader to access the supplied online documentation.

The TOE can be subdivided into two major components:

- The LDAP Server executable
- and the LDAP Server Administration Daemon executable.

The LDAP server may be partitioned again into two parts: the front-end and the back-end. The front-end is the network interface to LDAP clients and the back-end is the interface to a DB2 database. The Administration Daemon provides an LDAP interface to clients, used for the administration of the LDAP server. For more details refer to chapter 5.

To install and configure the TOE in an certification conformant configuration the user has to follow the guidance documentation provided in [8], [11] and [12] for installation, and in [10] for configuration. The Security Guide [10] provides guidance on how to configure the TOE in accordance with the Security Target [6]. For the secure operation of the TOE document [9] has to be followed.

3 Security Policy

The TOE is an implementation of the Lightweight Directory Access Protocol (LDAP). Its main purpose is to provide identification and authentication, access control and audit functionality. This is supplemented by management and non-bypassability.

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 password policy constraints).
- FDP_ACC.2 and FDP_ACF.1 defining the Directory Access Control SFP, a Security Policy that controls access to directory entries protected by the TOE.

A detailed description/definition of the Security Policy enforced by the TOE is given in the Security Target [6], chapter 5.1.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the Organisational Security Policy to which the TOE complies the following usage assumption exist (for the detailed and precise definition refer to [6], chapter 3.3):

- Of the information under the control of the TOE, only information classified as public information should be made available to unauthenticated or anonymous users (P.PUBLIC).

Based on personnel assumptions defined in [6] the following usage conditions exist:

- The Administrators of the TOE (i.e. Directory Administrators and Members of the Administrative Group) and its environment are trustworthy to perform discretionary actions in accordance with security policies and not to interfere with the abstract machine (A.NOEVIL). Whereas abstract machine means the hardware and operating system software the TOE runs on.
- The TOE and its environment are competently installed and administered (A.ADMIN).
- Authorised users are expected to act in a co-operating manner in a benign environment (A.COOP).

For a detailed description of the usage assumptions refer to the Security Target [6], especially chapter 3.1.

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 [6], chapter 3.1):

- The TOE is operated in a physically secure environment (A.PHYSICAL).
- Communication links between TOE and LDAP clients (on external systems) are protected against modification and disclosure of transmitted data (A.COMM).
- A reliable time function is provided by the environment (A.TIME).

Please consider also the requirements for the evaluated configuration specified in chapter 8 of this report.

4.3 Clarification of scope

The environmental threats listed below are not averted by the TOE. Additional support from the operating environment of the TOE is necessary (for detailed information about the threats and how the environment covers them refer to the Security Target [6], chapter 3.2.2 and chapter 8.1).

TE.USAGE:

The TOE may be configured, used and administered in an insecure manner, allowing an illegitimate user gaining access to resources or information protected by the TOE.

TE.CRASH:

Human error or a failure of software, hardware, power supply, or an accidental event may cause an abrupt interruption to the TOE operation, resulting in loss or corruption of data.

TE.SOPHISTICATED:

An unauthorised individual may gain access to TOE resources or information by using sophisticated technical attack, using IT security-defeating tools applied to the TOE or the underlying system components.

TE.PASS:

An attacker may bypass the TOE to access resources or resources protected by the TOE by attacking the underlying operating system or database, in order to gain access to TOE resources and information.

5 Architectural Information

General overview

The target of evaluation is the IBM Tivoli Directory Server Version 5.2 (ITDS). ITDS is an implementation of the Lightweight Directory Access Protocol (LDAP), which is compliant with the Internet Engineering Task Force (IETF) LDAP Version 2 specifications, i.e. RFC 1777 and Version 3 specifications, i.e. RFC 2251 - 2256.

The server is a software only product and can be installed and operated on a variety of hardware/software platforms (refer to chapter 7).

LDAP essentially provides access to and management of a specialised database where the update operation is less frequent and dedicated to the common goal within the enterprise on consolidating and unifying the management of identity.

IBM Tivoli Directory Server is built for identity management with role support, fine-grained access control and entry ownership. It provides the foundation for improved security, rapid development and deployment of Web applications.

The IBM DB2 Universal Database is used as back end data store to provide high performance, reliability and stability in an enterprise or e-business.

The IBM Tivoli Directory Server Version 5.2 is a software product only, delivered over the Internet as a package including the TOE, user and administrative tools, a WebSphere Application server, and a DB2 database. The user and administrator tools, the WebSphere Application server and the DB2 database are all excluded from the TOE and are considered part of the environment.

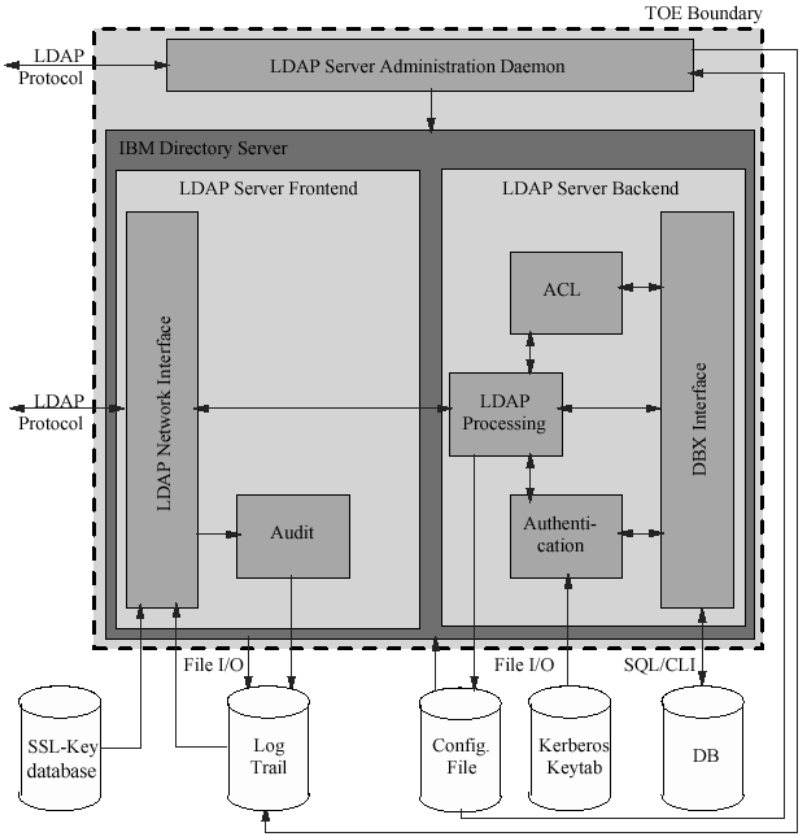
The TOE environment includes applications that are not delivered with the ITDS product, but are used as unprivileged tools, for example the Netscape browser needed to administrate the TOE or the Adobe Acrobat Reader to access the supplied online documentation.

Major structural units of the TOE

The TOE consists of the LDAP Server and the Administration Daemon executables as part of the product IBM Tivoli Directory Server.

User clients are connecting both to the LDAP server and to the administration daemon, using the LDAP protocol, but using different port numbers. The LDAP server component is providing the LDAP functionality to users and administrators, while the administration daemon is only used by the administrator for starting, stopping and querying the status of the TOE.

The following figure provides a more detailed overview of the TOE:



TOE security functionality

Identification and authentication

Identification and authentication are used to determine the identity of the LDAP clients; that is, verifying that users are who they say they are. A user name and password is used as the authentication scheme. This user identity is used for determining access rights and for user accountability. The administrator can manage users, set passwords for users, and place restrictions on user-selected passwords by specifying rules in the password policy managed by the administrator.

Access Control

After users are authenticated, it must be determined whether they have authorisation or permission to perform the requested operation on the specific object. Authorisation is based on access control lists (ACLs). An ACL is a list of authorisations that can be attached to objects and attributes in the directory. An ACL lists what type of access each user or a group of users is allowed or denied. To make ACLs shorter and more manageable, users with the same access rights are often put into groups. The directory administrator can manage access control by specifying the access rights to objects for individual users or groups.

Auditing

The IBM Tivoli Directory Server can perform auditing of security-relevant events, such as user authentication and modification to the directory tree. The audit function provides a means for accountability by generating audit records containing the time, user identity, and additional information about the operation. The behaviour of the audit function, such as selection of auditable events, as well as audit review and clearing of audit files, is managed by the directory administrator.

Management

The IBM Tivoli Directory Server is supporting the roles of Directory Administrator, Members of the Administrative Group and End User, allowing the Directory Administrator to manage the functions for identification and authentication, authorisation and audit. The Members of the Administrative Group have a well-defined sub-set of the rights of the Directory Administrator. Both the Directory Administrator and the Members of the Administrative Group can manage the users and user attributes.

Reference Mediation

The IBM Tivoli Directory Server is designed that all security policy enforcement functions are invoked and must succeed before any function is allowed to proceed. This means e.g. that any request for access to a directory entry is checked for access according to the rules defined before access is granted.

6 Documentation

The following documentation is provided with the product by the developer to the customer:

IBM Tivoli Directory Server Version 5.2 README Addendum, First Edition (December 2003), [8]

IBM Tivoli Directory Server Administration Guide Version 5.2, SC32-1339-00, First Edition (September 2003), [9]

Common Criteria Compliant Configuration Guide Version 5.2, First Edition (November 2003), [10]

IBM Tivoli Directory Server Installation and Configuration Guide Version 5.2, SC32-1338-00, First Edition (October 2003), [11]

IBM Tivoli Directory Server Version 5.2, Server Readme, [12]

Server Plug-ins Reference Version 5.2, First Edition (September 2003), [13]

C-Client SDK Programming Reference Version 5.2, First Edition (October 2003), [14]

IBM Tivoli Directory Server Version 5.2, Client Readme, [15]

IBM Tivoli Directory Server Performance Tuning Guide, Version 5.2, First Edition (October 2003), [16]

IBM Tivoli Directory Server Version 5.2: Web Administration Tool Readme, First Edition (September 2003), [17]

7 IT Product Testing

Test configuration

The Security Target [6] defines the following platforms for running the TOE:

- Microsoft Windows 2000
- SuSE Linux Enterprise Server 8
- Red Hat Advanced Server 3.0
- IBM AIX 5.2
- Sun Solaris 8
- HPUX 11i

Developer tests have been performed on all platforms, whereas evaluator tests were executed on a sampled subset of those platforms. Each platform was set up in accordance with the Security Target [6] and all the relevant guidance (refer to chapter 6 of this report).

Depth/Coverage of Testing

The security functionality of the TOE as well as all TSFI as detailed in the Functional Specification were completely covered by the developer tests. The developer tests provided for a sufficient depth as required by EAL3. The test areas provided by the developer covered the subsystems as defined in the high-level design documentation of the TOE as well as their interfaces.

Summary of Developer Testing Effort

Test configuration:

Tests have been carried out on the platforms as described above.

Testing approach:

The developer divided the testing effort needed for the TOE into several test areas representing groups of similar functionality. Each test area comprised several function tests that probe for the behaviour of the functions to be tested. For each single test case, the developer provided sufficient information on the setup of the test environment, on the instructions needed to actually run the test, and on the results expected for that test case.

Testing results:

The developer testing for the evaluated configuration of the TOE was performed successfully on all platforms listed above.

Summary of Evaluator Testing Effort

Test configuration

The evaluation lab performed tests on a subset of the platforms listed above. A reasonable argument for the subset chosen was provided. The TOE was setup as required by the Security Target and the respective guidance documentation.

Testing approach:

The evaluator testing effort comprised two test sessions. The first session concentrated on repeating developer test cases, whereas the second session addressed execution of tests devised by the evaluator. These evaluator tests concentrated on features newly introduced since the previous evaluation.

Testing results:

All actual test results obtained by the evaluator matched the expected results.

Evaluator penetration testing:

Within the vulnerability analysis, the evaluator identified potential vulnerabilities and decided to determine their potential of being exploited by devising additional penetration tests probing for ways a potential attacker might circumvent security functions.

The penetration tests did not show any obvious vulnerability which was exploitable in the intended environment.

8 Evaluated Configuration

The Target of Evaluation is called:

IBM Tivoli Directory Server Version 5.2

The IBM Tivoli Directory Server is a software product only, delivered over the Internet as a package including:

Component	TOE / Not TOE
IBM Tivoli Directory Server package	
The LDAP daemon executable and Administration daemon executable.	TOE
Installation and Configuration Tools and GSKit 6 (SSL package only)	Not TOE
User and administrative tools (like the IBM Directory Server Client SDK 5.2 or the Web Administration Tool).	Not TOE
A WebSphere Application Server.	Not TOE
A IBM DB2 database.	Not TOE

Note: Although delivered together with the TOE, the user and administrator tools, Installation and Configuration Tools, the LDAP Client, the replication service, the WebSphere Application Server and the DB2 database as well as GSKit are all excluded from the TOE. They are considered to be part of the environment (refer to [6], chapter 2.3 for further details). **Therefore the TOE comprises the LDAP server and the administration daemon executables only.**

The TOE environment can also include applications that are not delivered with the IBM Tivoli Directory Server, but are used as unprivileged tools, for example the Netscape browser needed to administrate the TOE or the Adobe Acrobat Reader to access the supplied online documentation.

To install and configure the TOE in an certification conformant configuration the user has to follow the guidance documentation provided in [8], [11] and [12] for installation, and in [10] for configuration. The Security Guide [10] provides guidance on how to configure the TOE in accordance with the Security Target [6]. For the secure operation of the TOE document [9] has to be followed.

The TOE can be run on the following Operating Systems:

- Microsoft Windows 2000
- SuSE Linux Enterprise Server 8

- Red Hat Advanced Server 3.0
- IBM AIX 5.2
- Sun Solaris 8
- HPUX 11i

No restriction on the usable hardware was made in the Security Target [6].

The Administrators and members of the administrative group of the TOE and its environment are seen as trustworthy to perform discretionary actions in accordance with security policies. The TOE and its environment is competently installed and administered. Authorised users are expected to act in a co-operating manner in a benign environment.

The TOE is operated in a physically secure environment. Communication links (between TOE and LDAP clients on external systems, and between the TOE and external systems) are protected against modification and disclosure of transmitted data. A reliable time is provided by the TOE environment.

For setting up / configuring the TOE all guidance documents have to be followed (refer to chapter 6 of this report).

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Common Evaluation Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE. This certification is a re-certification of BSI-DSZ-CC-0207-2003. The TOE includes additional functionality and is certified at a higher Evaluation Assurance Level.

The verdicts for the CC, Part 3 assurance components (according to EAL3 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-basic for the password based user authentication (SFR FIA_SOS.1).

Please note that:

- The **SOF-claim only applies for the non-administrative users** of the TOE. According to the Security Target [6], chapter 5.1.9, TOE Administrators and Administrative Group members are not subject to the Password Policy enforced by the TOE
- The **SOF-Claim is only valid if the English language is chosen** for the TOE.

Please refer to chapter 10 for more details and further comments and recommendations.

The vulnerability assessment performed during evaluation revealed potential vulnerabilities. None of them were either obvious or exploitable in the intended environment.

The results of the evaluation are only applicable to the product IBM Tivoli Directory Server Version 5.2 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [6] 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 following recommendations/comments are given by the Certification Body:

R1 The guidance documentation with respect to administrative passwords has to be followed. Because TOE Administrators and Members of the Administrative Group are not subject to the password policy enforced by the TOE, these administrative users have to choose strong passwords and to change them every 90 days.

R2 The English language has to be chosen for the TOE to ensure that the TOE's password policy is fully applied and the SOF-Claim is valid.

C1 According to A.ADMIN it is assumed that the TOE and its IT environment (e.g. the DB2 database back-end) is installed and administered by competent personnel. It has to be pointed out that the fulfilment of this assumption is crucial for the overall security.

C2 According to A.NOEVIL it is assumed that Administrators and Administrative Group Members are trustworthy. It has to be pointed out that the fulfilment of this assumption is crucial for the overall security, because administrative users are allowed to erase the audit records (refer to [6], chapter 5.1.4).

C3 The TOE is delivered via the Internet. The secure download method offered by IBM has to be used to obtain an un-manipulated copy of the TOE.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

ACL Access Control List

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

IT Information Technology

LDAP Lightweight Directory Access Protocol

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

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

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

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

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

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

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

[6] Security Target BSI-DSZ-CC-0235, Version 1.5, 2003-11-10, Security Target IBM Tivoli Directory Server Version 5.2, IBM Corporation

[7] Evaluation Technical Report BSI-DSZ-CC-0235, Version 1.3, 2004-02-08

User Guidance Documentation:

[8] IBM Tivoli Directory Server Version 5.2 README Addendum, First Edition (December 2003).

[9] IBM Tivoli Directory Server Administration Guide Version 5.2, SC32-1339-00, First Edition (September 2003)

[10] Common Criteria Compliant Configuration Guide Version 5.2, First Edition (November 2003)

[11] IBM Tivoli Directory Server Installation and Configuration Guide Version 5.2, SC32-1338-00, First Edition (October 2003)

[12] IBM Tivoli Directory Server Version 5.2, Server Readme

[13] Server Plug-ins Reference Version 5.2, First Edition (September 2003)

[14] C-Client SDK Programming Reference Version 5.2, First Edition (October 2003)

[15] IBM Tivoli Directory Server Version 5.2, Client Readme

[16] IBM Tivoli Directory Server Performance Tuning Guide, Version 5.2, First Edition (October 2003)

[17] IBM Tivoli Directory Server Version 5.2: Web Administration Tool Readme, First Edition (September 2003)

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

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

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

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

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

plus one of the following:

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

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

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

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

CC Part 3:

Assurance categorisation (chapter 2.5)

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

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 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.“