Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0428-2008

for

IBM Tivoli Directory Server 6.1

from

IBM Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0428-2008

IBM Tivoli Directory Server 6.1

from	IBM Corporation
Functionality:	Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1 - Basic flaw remediation

Common Criteria
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by CEM supplementation “ALC_FLR – Flaw remediation”, Version 2.3, August 2005 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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.

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.

Bonn, 22. April 2008

For the Federal Office for Information Security

IT
Security
Certified

SOGIS - MRA

Irmela Ruhrmann
Head of division

L.S.

This page is intentionally left blank.

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

The parts A to D contain the pages 1 to 36.

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective 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). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

[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 07 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

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 6.1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0283-2006. Specific results from the evaluation process BSI-DSZ-CC-0283-2006 were re-used.

The evaluation of the product IBM Tivoli Directory Server 6.1 was conducted by atsec information security GmbH. The evaluation was completed on 22. April 2008. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: IBM Corporation

The product was developed by: IBM Corporation

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. 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 and in the Security Target.

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

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The productIBM Tivoli Directory Server 6.1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] IBM Corporation
11501 Burnet Road
Internal mail drop 9015F000
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.

1 Executive Summary

The target of evaluation is the Tivoli Directory Server Version 6.1.

Tivoli Directory Server version 6.1 (TDS) is an implementation of Lightweight Directory Access Protocol (LDAP), which is compliant with the Internet Engineering Task Force (IETF) LDAP Version 2 specifications, i. e. RFC 1777 and LDAP 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.

LDAP is essentially a specialized 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. TDS is built for identity management with role support, finegrained access control and entry ownership. It provides the foundation for improved security, rapid development and deployment of Web applications. Using the power of the IBM DB2 Universal Database as back end data store, TDS provides high performance, reliability and stability in an enterprise or e-business. As the central repository for data within an enterprise, it is a powerful, secure and standards compliant enterprise directory for corporate intranets and the Internet.

The Tivoli Directory Server (TDS) 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,
- a WebSphere HTTP server and
- a DB2 database.

Note: Although delivered together with the TOE, the user and administrator tools, the HTTP server and the DB2 database are all excluded from the TOE and are considered part of the TOE environment.

The TOE environment must also include applications that are not delivered with the TDS product, but are used as unprivileged tools, for example the Internet Explorer or Firefox browser needed to administrate the TOE via the web GUI, or the Adobe Acrobat Reader to access the supplied online documentation.

Directory clients and servers

Directories are usually accessed using the client-server model of communication. The client and server processes might or might not be on the same machine. A server is capable of serving many clients. An application that wants to read or write information in a directory does not access the directory directly. Instead, it calls a function or application programming interface (API) that causes a message to be sent to another process. This second process accesses the information in the directory on behalf of the requesting application. The results of the read or write are then returned to the requesting application.

An API defines the programming interface a particular programming language uses to access a service. The format and contents of the messages exchanged between client and server must adhere to an agreed upon protocol. LDAP defines a message protocol used by directory clients and directory servers. There is also an associated LDAP API for the C language and ways to access the directory from a Java application using the Java Naming and Directory Interface (JNDI).

In order to improve performance and availability, directories may be replicated. This means that one master directory may be replicated to a number of copies allowing improved availability to read accesses. Any changes made to the master affecting the replicas, will be transmitted out to them. A user accessing a server may then either go to the master or to any of the replicas.

Replication is enabled as replication agreements between a server and a client. A replication agreement is part of the directory tree of the master. Access to the replication agreements and associated replication configuration information in the directory is limited. This has been restricted in the evaluated configuration to the security roles of Primary Directory Administrator, Local Administrative Group Members (with an administrative role of Directory Data Administrator or Replication Administrator or Server Configuration Group Member), and Master Server DN. Only these security roles are able to set up and change replication agreements.

In the evaluated configuration, there must not be more than one master for a given entry at any particular point in time. Since gateway servers only serve a purpose in a configuration including more than one concurrently updateable master server they are not meaningful in an evaluated configuration. Conflict resolution is not included in the TOE. Since an entry can only be updated on one server at any point in time, there should never be any replication conflicts.

The TOE provides the following evaluated 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 a basic 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. Both end users and administrators are subject to the password policy.

Access control

After users are authenticated, it must be determined whether they have authorization or permission to perform the requested operation on the specific object. Authorization is often based on access control lists (ACLs). An ACL is a list of authorizations 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 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 Tivoli Directory Server supports the roles of Primary Directory Administrator, Local Administrative Group Members, Global Administrative Group Members, Master DN and LDAP User, allowing the Primary Directory Administrator to manage the functions for identification and authentication, authorization and audit. The Local Administrative Group Members and the Global Administrative Group Members have a well-defined sub-set of the rights of the Primary Directory Administrator. Both the Primary Directory Administrator, the Local Administrative Group Members, and the Global Administrative Group Members can manage the users and user attributes. The master server DN is a role used for replication between LDAP servers. Finally, LDAP Users do not have any administrative rights.

Reference mediation

The 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 that any request for access to a directory entry is checked for access according to the rules defined before access is granted.

To ensure a secure usage, a set of guidance documents is provided together with TDS. 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 Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C or [1], part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC part 2 conformant.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.2.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	**Addressed issue**
F.AUDIT	Audit Generation
ACCESS_CONTROL	Access control to particular LDAP operations
F.I&A	Identification & authentication of TOE user
F.MANAGEMENT	Management of the behaviour of Roles, authentication functionality, authorisation on directory entries and audit functionality
F.REF_MEDIATION	Non-bypassability of the TSF

Table 1: TOE Security Functions

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

The claimed TOE's strength of functions 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 1.5 and 8.3.2 is confirmed.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6], chapter 3.

The Security Target defines six different platforms as configuration requirements for running the TOE:

- Microsoft Windows Server 2003 R2 Enterprise Edition
- IBM AIX 5.3
- Sun Solaris 10
- HP-UX 11i v2
- Red Hat Advanced Server 5.0
- SuSE Linux Enterprise Server 10

No explicit restrictions on the usable hardware were made in the Security Target [6]. For details refer to chapter 8.

The following constraints concerning the operating environment are made in the Security Target. They are based on the assumptions defined in the ST [6], chapter 3.1 and are summarised in the following table:

Assumption Name	**Summary**
A.PHYSICAL	The TOE is operated in a physically secure environment.
A.ADMIN	The TOE Administrators (i.e. the Primary Directory Administrator, the Local Administrative Group Members, and the Global Administrative Group Members) are trustworthy to perform discretionary actions in accordance with security policies and not to interfere with the abstract machine, making sure that the TOE is competently administered.
A.TOEENV	The TOE Environment Administrators are trustworthy to perform discretionary actions in accordance with security policies, assuring that the TOE environment is competently installed and administered.
A.COMM	It is assumed that any communication links between the TOE and external systems are protected against unauthorized modification and disclosure of communication data.
A.COOP	Authorized LDAP Users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
A.ROUTE	It is assumed that in a replicated environment, all the update requests are made to the master server only. It is also assumed that all replicas are under the same administration and the protection in the TOE environment is as for the TOE (master server).
A.TIME	It is assumed that a reliable time function is provided by the TOE environment to support the generation of audit records.
A.ENCRYPT	It is assumed that the TOE environment provides one-way encryption and random

Assumption Name	Summary
	number generation functions for the TOE.

Table 2: Assumptions on the TOE environment

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 Directory Server 6.1

The Tivoli Directory Server is a software product only, delivered over the Internet (secure download procedure offered by IBM has to be used) as a package including:

No	Type	Identifier	Release	Form of Delivery	TOE/ Not TOE
1	SW	- LDAP Base Server and LDAP Server Administration Daemon Package	6.1	Download	TOE
2	SW	– LDAP Client Packages – Web Administration Package – LDAP Proxy Server Package – LDAP RDBM Server Package	6.1	Download	Not TOE

Table 3: Deliverables of the TOE

3 Security Policy

The security policy is expressed by the set of security functional requirements and implemented by the TOE. It covers the following issues:

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

4 Assumptions and Clarification of Scope

The assumptions defined in the Security Target and some aspects of threats and organisational security policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment. The following topics are of relevance.

4.1 Usage Assumptions

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

- The Administrators of the TOE are trustworthy to perform discretionary actions in accordance with security policies and not to interfere with the abstract machine (A.ADMIN). Whereas abstract machine means the hardware and operating system software the TOE runs on.
- The TOE Environment Administrators are trustworthy to perform discretionary actions in accordance with security policies, assuring that the TOE environment is competently installed and administered (A.TOEENV).
- 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 external systems are protected against modification and disclosure of transmitted data (A.COMM).
- In a replicated environment all the update requests are made to the master server only. Furthermore it is assumed that all replicas are under the same administration and the protection in the TOE environment as for the master server (A.ROUTE).
- 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 threats listed below must be countered in order to support the TOE security capabilities but are either (i) not addressed by, or (ii) only partly addressed by the TOE. These threats must therefore be addressed in conjunction with the operating environment. Please refer to the Security Target [6], chapter 3.2.2 and chapter 8.1 for more details.

Threat name	Summary
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.

Table 4: Threats addressed by the operating environment

5 Architectural Information

Major structural units of the TOE

The TOE consists of two components: the directory server component and the administration daemon. User clients are connecting both to the LDAP server and to the administration daemon, using the LDAP protocol, but using different port numbers. The directory server 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 Tivoli Directory Server. Figure 1 below provides a more detailed overview of the TOE:

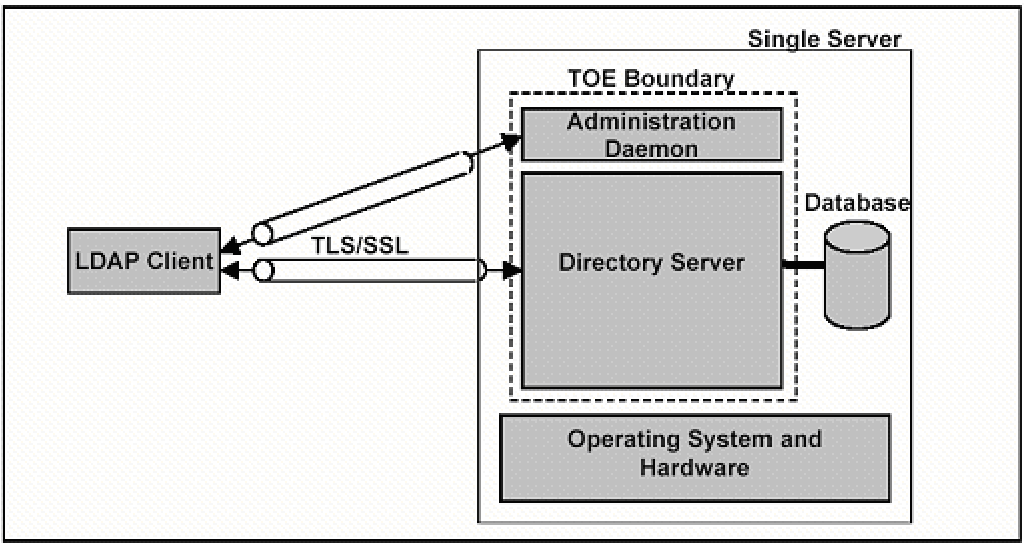

Figure 1: Tivoli Directory Architecture and TOE Boundary

6 Documentation

The evaluated documentation as outlined in table 3 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed. The following documentation is provided with the product by the developer to the customer:

[AdminGuide]	IBM Tivoli Directory Server Version 6.1, Administration Guide, GC32-1564-00, 02.04.2008
[C4Guide]	IBM Tivoli Directory Server Version 6.1, Common Criteria Guide, GC32-1570-00, 02.04.2008
[CommandRef]	IBM Tivoli Directory Server Version 6.1, Command Reference, SC23-7834-00, 02.04.2008
[InstGuide]	IBM Tivoli Directory Server Version 6.1, Installation and Configuration Guide, GC32-1560-00, 02.04.2008
[MsgsGuide]	IBM Tivoli Directory Server Version 6.1, Messages Guide GC32-1567-00, 24.08.2007
[New]	IBM Tivoli Directory Server Version 6.1, What's New for This Release, SC23-6539-00, 24.08.2007
[PDGuide]	IBM Tivoli Directory Server Version 6.1, Problem Determination Guide, GC32-1568-00, 02.04.2008
[PlugIn]	IBM Tivoli Directory Server Version 6.1, Server Plug-ins Reference, GC32-1565-00, 24.08.2007
[ProgRef]	IBM Tivoli Directory Server Version 6.1, Programming Reference, SC23-7836-00, 02.04.2008
[QuickStart]	IBM Tivoli Directory Server Version 6.1, Quick Start Guide, GI11-8172-00, 24.08.2007
[SysReq]	IBM Tivoli Directory Server Version 6.1, System Requirements, SC23-7835-00, 24.08.2007
[TuningGuide]	IBM Tivoli Directory Server Version 6.1, Performance Tuning and Capacity Planning Guide , SC23-6540-00, 24.08.2007

Table 5: Supporting documents

7 IT Product Testing

The Security Target defines six different platforms for running the TOE:

- Microsoft Windows Server 2003 R2 Enterprise Edition
- IBM AIX 5.3
- Sun Solaris 10
- HP-UX 11i v2
- Red Hat Advanced Server 5.0
- SuSE Linux Enterprise Server 10

Developer tests have been performed on all platforms, whereas evaluator tests were executed on a sampled subset of those platforms.

Report on the Developer Testing Effort

For details on the developer tests that go beyond the summary presented here, please refer to the Single Evaluation Report on Testing [ETE]. All developer tests were performed on all the platforms listed above. Due to the identical code base for the two Linux versions only one Linux platform was tested. Each platform was set up in accordance with the Security Target [6] and all the relevant guidance.

Testing Results

The developer testing was performed successfully by the developer on all platforms comprising the evaluated configuration of the TOE as listed above. All actual test results did match the expected results for the respective test case as documented in the developer test documentation.

7.1 Test Coverage/Test Depth

A complete coverage was achieved for all the TOE security functions as provided by the developer. The security functionality of the TOE as well as all TSFIs as detailed in the Functional Specification were completely covered by those tests.

The developer tests provide for a sufficient depth as required by EAL4. The test areas provided by the developer cover the subsystems as defined in the high-level design documentation of the TOE as well as their internal interfaces, whereas the single test cases be applicable for the lowlevel design as well, thus exceeding the scope of this evaluation.

7.2 Summary of Evaluator Testing Effort

The evaluation lab decided to devise independent evaluator tests in order to gain confidence on the behaviour of security functionality of the TOE and to check for exploitability of identified potential vulnerabilities.

Based upon the test cases provided by the developer and on the observation from the vulnerability analysis, the evaluation lab designed test cases, each either probing for potential vulnerabilities or extending the scope of an available developer test case to an aspect of the tested security function that the evaluator considered had not been covered appropriately by developer tests.

The tests of the evaluation lab were performed as planned using the selected platforms listed above. All actual test results obtained matched the expected results as documented in the evaluator test descriptions.

Report on the 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. Those penetration tests were performed as part of the evaluator independent testing. These tests did not reveal any exploitable vulnerability.

Evaluator Penetration Testing

By performing the penetration tests as part of the independent evaluator testing, the evaluator was able to clarify open issues with respect to his analysis of potential vulnerabilities. All penetration tests passed, i.e. it could be positively verified by the evaluator that the TOE behaved as expected not providing for potential ways to breach its security functionality. The actual test results obtained by the evaluator matched the expected test results as documented in the evaluator test descriptions.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

IBM Tivoli Directory Server 6.1

The IBM Tivoli Directory Server is a software product only, delivered over the Internet (secure download procedure offered by IBM has to be used) as a package including:

Component	**TOE / Not TOE**
IBM Tivoli Directory Server 6.1 package The LDAP daemon executable and Administration daemon executable.	TOE
Installation and Configuration Tools and GSKit, Version 7.0.3.30 (SSL package only)	Not TOE
User and administrative tools (like the IBM Directory Server Client SDK 6.1 or the Web Administration Tool).	Not TOE
Java Client (Java runtime version 1.5 and Java utilities)	Not TOE
A WebSphere Application server (IBM WebSphere Application Server Express, Version 6.1.0.7).	Not TOE
An IBM DB2 database.	Not TOE

Table 6: Product/ TOE components

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 web browser that may be used to administrate the TOE or the Adobe Acrobat Reader to access the supplied online documentation.

To install and configure the TOE in a certification conformant configuration the user has to follow the guidance documentation as listed in chapter 6. The Security Guide [9] 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.

According to the Security Target, the TOE can be run on

- Microsoft Windows Server 2003 R2 Enterprise Edition
- IBM AIX 5.3
- Sun Solaris 10
- HP-UX 11i v2
- Red Hat Advanced Server 5.0
- SuSE Linux Enterprise Server 10

No explicit restrictions on the usable hardware were made in the Security Target [6]. The Administrators 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 the TOE and external systems) are protected against modification and disclosure of transmitted data. A reliable time is provided by the TOE environment.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used. It was supplemented by the methodology for “ALC_FLR – Flaw remediation”, Version 2.3, August 2005.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented by ALC_FLR.1 – Basic flaw remediation and the class ASE for the Security Target evaluation) are summarised in the following table.

- All components of the EAL 4 augmented package as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 augmented for this TOE evaluation.

This is a re-certification based on BSI-DSZ-CC-0283-2006. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0283-2006 were re-used. In comparance to the former certificate the Level of Assurance has been increased and new functionality was subject to analysis (refer to the ST [6] for details). The focus of this re-evaluation was on the introduction of administrative roles, to allow for more specific administrative roles. Additionally features introduced are new interfaces to the server through extended operations, controls and environment variables. The encrypted attributes feature allows administrators the ability to add an additional layer of security to the data.

The evaluation has confirmed:

- for the functionality: Common Criteria Part 2 conformant
- for the assurance: Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1 - Basic flaw remediation
- The following TOE Security Functions fulfil the claimed Strength of Function : medium FIA_SOS.1 Verification of secrets

The results of the evaluation are only applicable to the IBM Tivoli Directory Server 6.1 IBM Tivoli Directory Server 6.1 as outlined in chapter 2 and 8 of this report.

For specific evaluation results regarding the development and production environment see annex B in part D 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.

9.2 Results of cryptographic assessment

The TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Security Target

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

12 Definitions

12.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
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

12.2 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.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

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

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

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

[6] Security Target BSI-DSZ-CC-0428, Version 1.9.9, 2008-04-02, IBM Tivoli Directory Server Version 6.1, IBM Corporation

[7] Evaluation Technical Report, Version 3, 2008-04-15, atsec information security GmbH (confidential document)

13.1 User Guidance Documents

[8] IBM Tivoli Directory Server Version 6.1, Administration Guide, GC32-1564-00, 02.04.2008

[9] IBM Tivoli Directory Server Version 6.1, Common Criteria Guide, GC32-1570-00, 02.04.2008

[10] IBM Tivoli Directory Server Version 6.1, Command Reference, SC23-7834-000, 2.04.2008

[11] IBM Tivoli Directory Server Version 6.1, Installation and Configuration Guide, GC32-1560-00, 02.04.2008

[12] IBM Tivoli Directory Server Version 6.1, Messages Guide GC32-1567-00, 24.08.2007

[13] IBM Tivoli Directory Server Version 6.1, What's New for This Release, SC23-6539-00, 24.08.2007

[14] IBM Tivoli Directory Server Version 6.1, Problem Determination Guide, GC32-1568-00, 02.04.2008

[15] IBM Tivoli Directory Server Version 6.1, Server Plug-ins Reference, GC32-1565-00

[16] IBM Tivoli Directory Server Version 6.1, Programming Reference, SC23-7836-00, 02.04.2008

[17] IBM Tivoli Directory Server Version 6.1, Quick Start Guide, GI11-8172-00, 24.08.2007

[18] IBM Tivoli Directory Server Version 6.1, System Requirements, SC23-7835-00, 24.08.2007

[19] IBM Tivoli Directory Server Version 6.1, Performance Tuning and Capacity Planning Guide , SC23-6540-00, 24.08.2007

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

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

- **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:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

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

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA. 2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.