Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0806-2013

for

IBM Tivoli Directory Server, Version 6.3

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-0806-2013

Database Management System

IBM Tivoli Directory Server
Version 6.3

from	IBM Corporation
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1

Common Criteria
Recognition
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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, 5 July 2013
For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom.Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition 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 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 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, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

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

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 6.3 has undergone the certification procedure at BSI.

The evaluation of the product IBM Tivoli Directory Server, Version 6.3 was conducted by atsec information security GmbH. The evaluation was completed on 28 June 2013. 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,

[6] Information Technology Security Evaluation Facility

- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual 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 product IBM Tivoli Directory Server, Version 6.3 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://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
Rajiv Gandhi Infotech Pk Phase 2 Plot No Pl.3 Midc,
Hinjewadi, Village Limit Of Marunji Pune, MH411057
India

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 (TOE) is the IBM Tivoli Directory Server Version 6.3 Fix Pack 10. The IBM Tivoli Directory Server (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. RFC1777 [18] and LDAP Version 3 specifications, i.e. RFC2251, RFC2252, RFC2253, RFC2254, RFC2255, RFC2256 [19 - 24]. TDS is a software only product and can be installed and operated on a variety of hardware/software platforms. An LDAP server is a specialized database where the update operations are expected to be less frequent than for a relational database. An LDAP server within an enterprise is often dedicated to the common goal of consolidating and unifying the management of identities. TDS is built for identity management with role support, fine-grained access control, and entry ownership. It provides the foundation for improved security along with rapid development and deployment of Web applications. Using the power of the IBM DB2 Universal Database as a backend data store, the TOE 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 standard compliant enterprise directory for corporate intranets.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) 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 by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functions	Addressed issue
Auditing	The TOE generates audit records for all supported LDAP operations and extended operations except for the LDAP abandon operation. The Administration Server and LDAP Server store their audit records in separate audit logs. The TOE also provides the capability for authorized administrators to review the audit logs through the use of LDAP extended operations. The TOE only allows authorized administrators to clear (delete all audit records in) the audit logs.
Access Control	Access control to LDAP entries is enforced by the directory server back ends in which the entries are maintained. There are two different ways in which access control is implemented, hard coded as with the configuration back end and configurable as with the database back end. The hard coded access rights are very restricted and cannot be changed by anyone, including the administrator or at installation, while access to LDAP entries stored in the database back end are subject to configurable ACLs. This ACL-based access control does not only apply to an LDAP entry but can be specified on attribute level. There are two kinds of ACLs, non-filter based ACLs and filter based ACLs: ● Non-filter based ACLs apply explicitly to the directory object that contains them and may be propagated to none, some, or all its descendant objects

TOE Security Functions	Addressed issue
	as configured. If propagated, the ACL is propagated to all descendant objects that do not contain explicit ACLs. ● Filter based ACLs may apply to the containing object, and some, or all of the objects in the descendant tree. The Access Control Information is applied to an object based on a match with the comparison filter. Filtered ACLs accumulate upward along the ancestor chain in a sub-tree. In addition, selected LDAP strings and binary entries can be one-way encrypted using salted SHA-1 and SHA-2 algorithms to prevent the direct observation of sensitive data.
Identification and Authentication	Users are required to identify and authenticate themselves to the TOE prior to accessing information within the TOE, except when the TOE publishes selected entries as public data. The TOE uses the bind operation to identify and authenticate a user. The bind operation requires the user to supply a Distinguished Name (DN) and password which the TOE uses to verify the validity of the user. The TOE supports the following authentication methods: ● Simple Bind ● Simple Authentication and Security Layer (SASL) using the DIGEST-MD5 SASL authentication mechanism provided by IBM Global Security Kit (GSKit, part of the operational environment)
Security Management	The TOE supports security roles and more fine-grained administrative privileges that separate responsibilities for managing the TOE security functions Auditing, Access Control, and Identification and Authentication.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.1, 3.2 and 3.3.

This certification covers the following configurations of the TOE:
The evaluated configuration of the TOE consists of the IBM Tivoli Directory Server Version 6.3 with Fix Pack 10. For details refer to chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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, Version 6.3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1.	SW	IBM Tivoli Directory Server	6.3	Secure Download
2.	SW	IBM Tivoli Directory Server v6.3 Fix Pack 10	FP10	Secure Download
3.	DOC	IBM Tivoli Directory Server Version 6.3 Fix Pack 10 Common Criteria Guide [8]	GC27-2757-00	Secure Download
4.	DOC	IBM Tivoli Directory Server Version 6.3 What's New for This Release [9]	GC27-2746-00	Secure Download
5.	DOC	IBM Tivoli Directory Server Version 6.3 Quick Start Guide [10]	GI11-9351-00	Secure Download
6.	DOC	IBM Tivoli Directory Server Version 6.3 System Requirements [11]	SC27-2755-00	Secure Download
7.	DOC	IBM Tivoli Directory Server Version 6.3 Installation and Configuration Guide [12]	SC27-2747-00	Secure Download
8.	DOC	IBM Tivoli Directory Server Version 6.3 Administration Guide [13]	SC27-2749-00	Secure Download
9.	DOC	IBM Tivoli Directory Server Version 6.3 Command Reference [14]	SC27-2753-00	Secure Download
10.	DOC	IBM Tivoli Directory Server Version 6.3 Programming Reference [15]	SC27-2754-00	Secure Download
11.	DOC	IBM Tivoli Directory Server Version 6.3 Problem Determination Guide [16]	GC27-2752-00	Secure Download
12.	DOC	IBM Tivoli Directory Server Version 6.3 Messages Guide [17]	GC27-2751-00	Secure Download

Table 2: Deliverables of the TOE

The complete TOE (the base release and the Fix Pack) is delivered via a secure download (HTTPS) from the IBM Passport Advantage web portal (http://www.ibm.com/software/passportadvantage[8]). This requires the use of the Download Director which is an applet provided on the IBM web page once the TOE has been chosen for download.

The guidance can be obtained from the IBM support page (http://www.ibm.com/support). Specifically, the Common Criteria Guide [8] can be found by searching for GC27-2757-00, and should then be downloaded securely choosing the Download Director option. The Common Criteria Guide contains more details on the secure delivery for the TOE components and the fix pack mentioned above.

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 audit functionality, access control, identification and authentication and security management.

[8] IBM Passport Advantage requires an account IBM account.

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:

- The communication links between the TOE and LDAP clients on external systems and replicas are protected from unauthorized modification and disclosure of communication data.
- The database used to store the TSF and user data is configured and managed in a secure way that prohibits unauthorized access and tampering with the TSF data and user data of the TOE.
- The Operational Environment must provide functions for support of one-way encryption of sensitive data and random number generation to the TOE.
- Those responsible for the Operational Environment must ensure that the underlying operating system and hardware are configured and managed in a secure way.
- Those responsible for the TOE must ensure that the TOE is installed, and managed in a secure manner, which maintains the security of the TOE, TSF data and user data of the TOE.
- Those responsible for the TOE must ensure that the TOE and its underlying hardware and software are physically protected from unauthorized physical access and tampering.
- The Operational Environment must ensure that in a replicated environment all the update requests are made to the master server only. It must also ensure that all replicas are under the same administration and have the same protection as is required for the TOE (master server).
- The Operational Environment must provide a reliable time source.

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The TOE is illustrated in Figure 1 in the ST [6], showing the basic client/server based TDS architecture. The rectangle represented by the dashed lines indicates the TOE boundary of the two major TOE components, i.e. the standalone LDAP Server with the Administration Server.

Figure 1 in the ST [6] provides a high-level overview of the components showing that the LDAP Server and Administration Server are inside the TOE boundary and the remaining components are outside the TOE boundary. It shows that the Administration Server, LDAP Server, Database, and Operating System reside on a Single Server. It also shows that the LDAP Clients exist on systems other than the system containing the TOE.

The LDAP Clients can communicate to both the LDAP Server and the Administration Server through TLS/SSL connections. The LDAP Server is the only component out of the ones shown that uses the Database.

The LDAP Server design architecture is further broken down into the following subsystems:

● LDAP Network Interface Subsystem: This subsystem receives all LDAP requests (including standard LDAP operations like bind or modify, but also extended operations, and any controls associated with an LDAP request) from network clients, and performs sanity checks on the data. It then forwards the requests to the LDAP Processing subsystem.

● LDAP Processing Subsystem: The LDAP Processing Subsystem is the core of the LDAP functionality as it implements the hierarchical semantics of the data. It is therefore responsible for either applying the LDAP read or write operations on the LDAP tree, or for forwarding requests to replicas. The subsystem also verifies whether the LDAP data matches the scheme before performing any changes to the DIT. Operations that relate to the database back end undergo a conversion phase to match the database structure when updating the database or to match the tree structure when retrieving data from the database. The subsystem delegates authentication and password policy processing to the Authentication and Password Policy subsystem when receiving bind requests or operations on data that is affected by password policies. The subsystem further delegates authorization decisions to the ACL subsystem while processing database operations, and enforces the decisions returned by the ACL Subsystem. For handling audit review extended operations, it communicates with the Audit Subsystem.

● Authentication and Password Policy Subsystem: This subsystem performs the actual authentication based on the bind requests. It further handles the Password Policy processing, which not only applies to bind operations but also to any LDAP operations that target password or password policy data.

● ACL Subsystem: The ACL Subsystem is responsible for evaluating access requests, based on the type of operation (e.g., ldapadd), the requester (subject), the target data (objects), and the access control lists that apply to the targeted data. It returns the evaluation result (permit or deny) to the calling subsystem.

● DBX Interface Subsystem: This subsystem works as a link between the TOE and the database that stores most of the LDAP tree data. It provides a wrapper interface that is used by the other subsystems when accessing the LDAP database back end data.

● Audit Subsystem: The Audit subsystem is responsible for generating and writing audit events to audit log files, and returns audit logs when requested through LDAP audit extended operations.

The LDAP Server Administration Daemon Subsystem implements a small subset of the interface provided by the LDAP Networking Interface Subsystem. Its main purpose is to allow administrators to query the configuration and to perform a few basic management operations like starting or stopping the LDAP Server. It authenticates any requests that requires administrative privileges.

6 Documentation

The evaluated documentation as outlined in table 2 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.

7 IT Product Testing

7.1 Developer Testing

Test Effort

The developer used an automated test framework which included about 300 perl test scripts. From these, about 160 tests cases were relevant for the evaluation. The test environment was specifically designed to create, remove, and start/stop TOE instances during the test execution to ensure independence between several different test runs, and to support the seamless creation of multiple TOE instances to also test functions that require more than one instance (e.g. for replication). The tests were designed such to provide a detailed test result log for each test within one test case script as well as a test execution summary that displays the overall result of a test run.

Test Configuration

All developer tests were performed on all but the RHEL 6 platform. Due to the identical code base of SLES11 and RHEL 6, only the former platform was tested. Each platform was set up in accordance with the Security Target and all the relevant guidance.

Test Approach and Depth

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. All security-relevant functionality of the TOE was covered by those test areas.

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 expected results for that test case.

The developer used a subsystem-to-test mapping to ensure that:

- all SFRs are tested
- that all subsystems are tested

Test Results

The developer testing was performed successfully by the developer on all tested platforms. The actual test results were made available to the evaluator via the Test Tracking Tool database used by the developer. All actual test results did match the expected results for the respective test case as documented in the developer test documentation. The developer’s philosophy on testing was taken into account by the evaluator. The developer stated in the test plan that testing is only completed when 95% of the test cases have been successfully executed. Therefore the evaluator verified that still 100% all of the security-relevant test cases were executed without failures.

7.2 Evaluator Independent Testing

Test Effort

The evaluator chose three developer test scripts to be executed on the developer test system. Each of the tests was run on another test platform. Two of the tests were run twice: first using the original test case, and a second time with modified parameters.

The evaluator ran 16 automated test cases on two of the supported platforms.

The evaluator created 18 new manual tests on two of the supported platforms.

Most of the tests used the user interface provided through the client utilities to communicate with the TOE (client command-line tools), while one test used the client C-libraries to create a C-program which then sends requests to the TOE.

Test Configuration

The developer tests chosen by the evaluator were performed on an AIX 7.1, a Windows Server 2008 R2 (64-bit), and a SLES 11 (64-bit) installation.

The evaluator tests were performed on a Windows Server 2008 32-bit and a RHEL 6 installation. The evaluator created several instances on the RHEL6 installation for the replication tests.

In both cases, the evaluated configuration was followed apart from some exceptions that were merely organizational requirements and which had no impact on the test results.

Operating System	Developer	Evaluator
SLES11	+	(+)
AIX 7.1	+	(+)
RHEL 6	-	+
Solaris 10	+	-
Windows Server 2008 32-bit	+	+
Windows Server 2008 64-bit (R2)	+	(+)

Table 3: Tested Platforms[9]

Test Approach and Depth

The evaluator witnessed the developer testing via a web conference, where the developer started the automated tests based on the evaluator's choice. Finally, modifications were made to observe respective failures to occur in the tests (verifying that the developer test framework properly catches and displays test failures).

The evaluator tests focused on the remotely accessible interfaces (the LDAP interface of the LDAP Server and the Administration Server). On these interfaces, the tests exercised mostly the access control and security management functions, but also included a few I&A tests targeting the DIGEST-MD5 authentication. Because the developer already performed extensive testing, the evaluator tests often involved non-standard situations as follows:

- the TOE is in configuration mode
- only the Administration Server is available
- use controls in unintended ways
- test TSFs while the TSF data changes

Test Results

The following test result deviations were observed:

- The Digest-MD5 tests failed for the Administration Daemon. The developer clarified that the Administration Daemon is not designed to support this authentication type. This has

[9] (+) denotes example execution of developer tests

been subsequently clarified in the guidance and in the Security Target. Based on this, it is not considered a deviation from the expected results.

- A minor guidance documentation error had been found for the Dynamic Group control function, which has no impact on the evaluation.

All other tests ran as expected.

7.3 Evaluator Penetration Testing

Test Effort, Approach and Depth

The evaluator used the CVE portal and Google searches to find publicly documented vulnerabilities. From the understanding that the evaluator gained from this, further vulnerability considerations in the area of LDAP request parsing (which deals with properly decoding BER-encoded ASN.1 messages) have been performed. The goal was to detect coding flaws, also by using automated tests (Java code) to exercise a broad combination of request data as input.

These parsing tests were also the focus of the vulnerability analysis and the respective tests, combining random input tests (fuzzing) with targeted ill-formed ASN.1 attribute length tests. To support this test approach, the evaluator used a custom Java LDAP clients based on the SUN LDAP client implementation as follows:

- for specific ASN.1 encoding modifications, individual Java files from the SUN LDAP client had been modified and integrated into the test suite. This was necessary because the normal client implementation does not provide control over individual bytes of the request buffer
- for more complex LDAP communication tests (for example for sending more than one message over the same connection), the complete SUN LDAP client implementation had been modified and replaced when constructing the LDAP client objects through the standard Java API

For testing the IBM-specific extended operations, the evaluator used the developer's LDAP programming reference to create a C test program that exercised these interface function. For this he deliberately deviated from the programming reference which defines a certain order of client operations, e.g. he left out the binding step prior to actual operation to determine that the TSF do not depend on the client behaviour.

The evaluator also tested the more complex feature of Persistent Search under specific conditions.

Another area of tests were functions that are not directly related to the security functionality, like DN normalization or referrals, but which could in the worst case have a negative impact on the security of the TOE.

The evaluator also used publicly available tools to identify additional network interfaces (using nmap) and the PROTOS LDAP implementation test suite to identify potential vulnerabilities of the TOE.

The following list summarizes the tested areas:

- General network interfaces introduced on a TOE installation.
- LDAP protocol implementation tests (especially ill-formed LDAP request to test for coding flaws). An error may affect any of the TOE security functions, i.e. any SFR.
- File transfer functions and their authorization enforcement (FMT_SMR.1).

- Persistent search operations under specific conditions and their authorization enforcement (FDP_ACC.2).
- Check for sensitive information in publicly available directory entry.
- Access control and authentication for referrals and their target entries, and behaviour of user referrals (FIA_UID.1 / FIA_UAU.1).
- DN normalization side-effects on access control and authentication (FIA_UID.1 / FIA_UAU.1).
- General access control of available naming contexts and their data backends (FMT_ACC.2, FMT_SMR.1).

Test Configuration

The tests were performed on the TOE that was installed on the Windows Server 2008 32-bit installation. The test configuration concerning in terms of the evaluated configuration settings and software versions was the same than for the evaluator's independent testing.

Results

None of the penetration tests performed by the evaluator revealed an exploitable or residual vulnerability of the TOE.

8 Evaluated Configuration

This certification covers the following configurations of the TOE: The evaluated configuration of the TOE consists of the IBM Tivoli Directory Server Version 6.3 with Fix Pack 10.

The operational environment includes the following software products:

- IBM DB2 Universal Database
- IBM Global Security Kit (GSKit), version 8.0.14.14

The operational environment consists of the following hardware platforms and operating systems:

- Microsoft Windows Server 2008 Enterprise Edition (32-bit)
- Microsoft Windows Server 2008 R2 Enterprise Edition (AMD64/EM64T 64-bit)
- IBM AIX 7.1
- Sun Solaris 10 (SPARC)
- Red Hat Advanced Server 6 (AMD64/EM64T 64-bit)
- SuSE Linux Enterprise Server 11 (AMD64/EM64T 64-bit)

Apart from the software products and hardware systems mentioned above, the following functionality is out of scope of the evaluation:

- The LDAP Client
- The TLS/SSL module (GSKit), which provides:
  - Protected communication between an LDAP Client and TOE
  - Protected communication among replication servers

- Encryption/hash and random number generation support for salted SHA-1 and salted SHA-2 encryption of LDAP entries
- Encryption/hash generation support for MD5 for the DIGEST-MD5 SASL authentication mechanism
- Authentication using X.509v3 public-key certificates

The TOE and the DB2 database will run on the same machine. In case of replication, when different instances of the TOE run on different machines, they will all have their own DB2 databases running on their respective machine.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

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

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.1

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

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 documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and

techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

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

ACL Access Control List

AIS Application Notes and Interpretations of the Scheme

AIX Advanced Interactive eXecutive

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

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

DN Distinguished Name

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

GSKIT Global Security Kit

IETF Internet Engineering Task Force

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

LDAP Lightweight Directory Access Protocol

PP Protection Profile

RHEL Red Hat Linux Enterprise

SAR Security Assurance Requirement

SASL Simple Authentication and Security Layer

SFP Security Function Policy

SFR Security Functional Requirement

SLES SuSE Linux Enterprise Server

ST	Security Target
TDS	Tivoli Directory Server
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[10].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0806-2013, Version 1.12, 2013-02-25, IBM Tivoli Directory Server Version 6.3 Fix Pack 10 Security Target, IBM Corporation

[7] Evaluation Technical Report, Version 4, 2013-05-08, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

13.1 Guidance Documentation

[8] IBM Tivoli Directory Server Version 6.3 Fix Pack 10 - Common Criteria Guide, GC27-2757-00, 2013-04-09

[9] IBM Tivoli Directory Server Version 6.3 - What's New for This Release, GC27-2746-00

[10] IBM Tivoli Directory Server Version 6.3 - Quick Start Guide, GI11-9351-00

[11] IBM Tivoli Directory Server Version 6.3 - System Requirements, SC27-2755-00

[12] IBM Tivoli Directory Server Version 6.3 - Installation and Configuration Guide, SC27-2747-00

[13] IBM Tivoli Directory Server Version 6.3 - Administration Guide, SC27-2749-00

[14] IBM Tivoli Directory Server Version 6.3 - Command Reference, SC27-2753-00

[15] IBM Tivoli Directory Server Version 6.3 - Programming Reference, SC27-2754-00

[16] IBM Tivoli Directory Server Version 6.3 - Problem Determination Guide, GC27-2752-00

[17] IBM Tivoli Directory Server Version 6.3 - Messages Guide, GC27-2751-00

13.2 RFC References

[18] RFC1777, Lightweight Directory Access Protocol, Authors: W. Yeong, T. Howes, S. Kille, 1995-03-01

[19] RFC2251, Lightweight Directory Access Protocol (v3), Authors: M. Wahl, T. Howes, S. Kille, 1997-12-01

[10] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[20] RFC2252, Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, Authors: M. Wahl, A. Coulbeck, T. Howes, S. Kille, 1997-12-01

[21] RFC2253, Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names, Authors: M. Wahl, S. Kille, T. Howes, 1997-12-01

[22] RFC2254, The String Representation of LDAP Search Filters, Author: T. Howes, 1997-12-01

[23] RFC2255, The LDAP URL Format, Authors: T. Howes, M. Smith, 1997-12-01

[24] RFC2256, A Summary of the X.500(96) User Schema for use with LDAPv3, Author: M. Wahl, 1997-12-01

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 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 7 of this CC 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.