Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0535-2009

for

IBM Tivoli Directory Server Version 6.2

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

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0535-2009

IBM Tivoli Directory Server
Version 6.2

from	IBM Corporation
Functionality:	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 accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product 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, 16 March 2009

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

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

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 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- 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-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 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 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 January 2009 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 web site: 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.

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 6.2 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0283-2006.

The evaluation of the product IBM Tivoli Directory Server Version 6.2 was conducted by atsec information security GmbH. The evaluation was completed on 24 February 2009. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the 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 product IBM Tivoli Directory Server Version 6.2 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

This page is intentionally left blank.

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 6.2.

IBM Tivoli Directory Server version 6.2 (TDS) is an implementation of the Lightweight Directory Access Protocol (LDAP), which is compliant with the Internet Engineering Task Force (IETF) LDAP Version 2 specifications (i.e. RFC 1777) and 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 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, rapid development and deployment of Web applications. Using the power of the IBM DB2 Universal Database as a backend 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 IBM Tivoli Directory Server (TDS) is a software product only, delivered over the Internet as a package including the TOE, user and administrative tools, a WebSphere HTTP server, and a DB2 database. The user and administrator tools, the HTTP server and the DB2 database are all excluded from the TOE and are considered part of the 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, and 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 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. Definition of replication agreements is controlled by access control mechanisms in the TOE and is 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 master server that can be concurrently updated, they are not meaningful in the 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 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 EAL4 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
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 group of users is allowed or denied. To make ACLs shorter and more manageable, users with the same access rights are often put into groups. The directory administrator can manage access control by specifying the access rights to objects for individual users or groups.
Auditing	The IBM Tivoli Directory Server can perform auditing of security-relevant events, such as user authentication and modification of 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.

TOE Security Function	Addressed issue
Management	The IBM 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 subset of the rights of the Primary Directory Administrator. The Primary Directory Administrator, the Local Administrative Group Members, and the Global Administrative Group Members all can manage 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 IBM Tivoli Directory Server is designed so 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.

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 'moderate' (SOF-moderate) for specific functions as indicated in the Security Target [6], chapter 1.5 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 TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

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

- Microsoft Windows Server 2003 R2 Enterprise Edition
- IBM AIX 6.1
- Sun Solaris 10 (SPARC)
- HP-UX 11i v3 (Itanium)
- Red Hat Advanced Server 5.1
- SuSE Linux Enterprise Server 10 SP1

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

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 6.2

The following table outlines the TOE deliverables:

No	Type	Identifier	Form of Delivery	TOE/ Not TOE
1	SW	IBM Tivoli Directory Server Version 6.2 • LDAP server • administration daemon executable	Download	TOE
2	SW	IBM Tivoli Directory Server Version 6.2 • Installation and configuration tools version 6.2 • GSKit version 7.0.4.14 (SSL packages only)	Download	Not TOE
3	Doc	Common Criteria Guide, document ID: SC23-9949-00 [9]	Download	TOE
4	SW	IBM Tivoli Directory Server Client SDK version 6.2 Web Administration Tool version 6.1 IBM DB2 database version 9 IBM Tivoli Directory Integrator version 6.1.1	Download	Not TOE

Table 2: Deliverables of the TOE

No hardware is delivered with the product. For further evaluated guidance see section 13.1.

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 reference mediation.

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: OE.MANAGE, OE.ENVMANAGE, OE.PHYSICAL, OE.DATABASE, OE.SOPHISTICATED, OE.BACKUP,OE.COMMUNICATION, OE.ROUTE, OE.TIME and OE.ENCRYPT. Details can be found in the Security Target [6] chapter 4.2.

5 Architectural Information

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

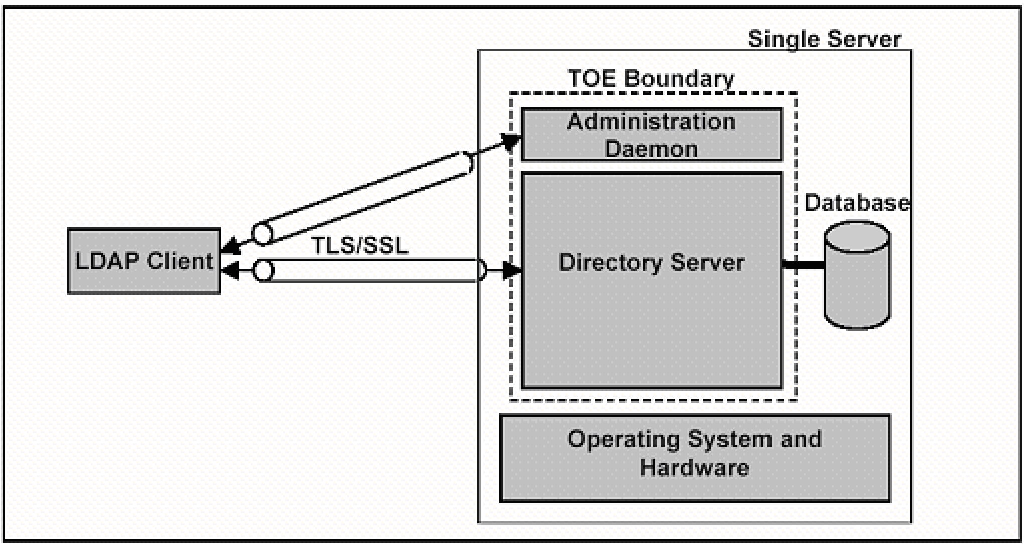

Figure 1: IBM Tivoli Directory Architecture and TOE Boundary

The IBM Tivoli Directory Server provides a rich set of security features. The security functions that were evaluated are summarized in the following list:

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

For further details refer to table 1 in this report or the ST [6], chapter 6.1.

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 and guidance documents as listed in section 13.1 of this report have to be followed.

7 IT Product Testing

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

- Microsoft Windows Server 2003 R2 Enterprise Edition
- IBM AIX 6.1
- Sun Solaris 10 (SPARC)
- HP-UX 11i v3 (Itanium)
- Red Hat Advanced Server 5.1
- SuSE Linux Enterprise Server 10 SP1

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

7.1 Report on the Developer Testing Effort

Test Configuration

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 and all the relevant guidance.

Testing Approach

The developer provided evidence that the security functionality of the TOE was tested. All security-relevant functionality of the TOE was covered by those tests.

Testing Results

The developer testing was performed successfully on all platforms comprising the evaluated configuration of the TOE as listed above. The evaluator was able to verify this for a sample of test cases chosen by the evaluator when inspecting the actual test results. All actual test results did match the expected results for the corresponding test case as documented in the developer test documentation.

Test Coverage/ Test Depth

The evaluator determined that the security functionality of the TOE as well as all except one TSFI as detailed in the Functional Specification were completely covered by those tests. The evaluator created an own test to verify that the Configuration Data Interface (environment variables) are honored by the TOE. The developer's philosophy on testing was taken into account by the evaluator.

The developer stated that testing is only completed when 95% of the test cases have been successfully executed. The evaluator verified that these 95% of the test cases contain all security-relevant test cases.

The evaluator was able to verify that developer tests provide for a sufficient depth as required by EAL4.

7.2 Report on the Evaluator Testing Effort

TOE Test Configuration

The evaluator performed the subset of developer tests on remote test machines provided by the developer in Pune, India. Furthermore, the evaluator performed his own tests on one test machine within the ITSEF testing facilities in Munich.

Test session one was performed on platforms Windows 2003 R2 Enterprise Edition, RedHat Advanced Server 5.1, and HP-UX 11iv3, on systems provided by the developer. Test session two was performed on Sun Solaris 10.

Summary of Evaluator Test Results

The evaluator tests were performed as planned using the selected platforms listed above. All actual test results obtained by the evaluator 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.

Summary of the 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., the evaluator could not determine any way by which the security functionality of the TOE can be breached.

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:

Component	**TOE / Not TOE**
The IBM Directory Server: The LDAP server and administration daemon executable, being the core part of the TDS.	TOE
It also contains installation and configuration tools as well as the GSKit 7.0.4.14 (SSL packages only).	Not TOE
The IBM Tivoli Directory Server Client SDK 6.2: The client package provides the tools required to develop LDAP applications, including client executables, libraries, sample programs in source code form, header files and documentation for the C language APIs.	Not TOE
Web Administration Tool: The Web-based GUI for administering the directory, including the IBM WebSphere Application Server Express, Version 6.1.	Not TOE
IBM DB2 database: The IBM DB2 Universal Database version 9 used for storing the LDAP entries.	Not TOE
IBM Tivoli Directory Integrator: Enables SNMP, Active Directory synchronization, and the use of the idssupport server utility, Version 6.1.1.	Not TOE

Table 3: Components of the TOE

Only the following components from the IBM Tivoli Directory Server program package form the TOE:

- **the LDAP server and**
- **the administration daemon executable.**

All other parts of the IBM Tivoli Directory Server such as the installation and configuration tools as well as the GSKit are considered to be part of the TOE environment. All other components listed in the table above are also part of 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. As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL4 package as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0283-2006, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on new versions of the underlying platforms as well as on new features like the restriction of the maximum number of consecutively repeated characters for the password management .

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
- The following TOE Security Functions fulfil the claimed Strength of Function: moderate FIA_SOS.1 Verification of secrets.

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 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.

Especially at least the latest fixes, updates, or patches which were available up to end of February 2009 must be installed on the operating systems that are considered for EAL4 evaluation.

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
BSIG	BSI-Errichtungsgesetz
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

Assets – Information or resources to be protected by the countermeasures of a TOE.

Assignment – The specification of an identified parameter in a component.

Assurance – Grounds for confidence that an entity meets its security objectives.

Attack potential – The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Augmentation – The addition of one or more assurance component(s) from Part3 to an EAL or assurance package.

Authentication data – Information used to verify the claimed identity of a user.

Authorised user – A user who may, in accordance with the TSP, perform an operation.

Class – A grouping of families that share a common focus.

Component – The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Connectivity – The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Dependency – A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Element – An indivisible security requirement.

Evaluation – Assessment of a PP, an ST or a TOE, against defined criteria.

Evaluation Assurance Level (EAL) – A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Evaluation authority – A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

Evaluation scheme – The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Extension – The addition to an ST or PP of functional requirements not contained in Part2 and/ or assurance requirements not contained in Part 3 of the CC.

External IT entity – Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Family – A grouping of components that share security objectives but may differ in emphasis or rigour.

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

Human user – Any person who interacts with the TOE.

Identity – A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

Informal - Expressed in natural language.

Internal communication channel – A communication channel between separated parts of TOE.

Internal TOE transfer – Communicating data between separated parts of the TOE.

Inter-TSF transfers – Communicating data between the TOE and the security functions of other trusted IT products.

Iteration – The use of a component more than once with varying operations.

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

Organisational security policies – One or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

Package – A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

Product – A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

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

Reference monitor – The concept of an abstract machine that enforces TOE access control policies.

Reference validation mechanism – An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.

Refinement – The addition of details to a component.

Role – A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret – Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Security attribute – Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Security Function (SF) – 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 Function Policy (SFP) – The security policy enforced by an SF.

Security objective – A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.

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

Selection – The specification of one or more items from a list in a component.

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

Strength of Function (SOF) – 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.

System – A specific IT installation, with a particular purpose and operational environment.

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

TOE resource – Anything usable or consumable in the TOE.

TOE Security Functions (TSF) – 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 Functions Interface (TSFI) – A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

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

TOE security policy model – A structured representation of the security policy to be enforced by the TOE.

Transfers outside TSF control – Communicating data to entities not under control of the TSF.

Trusted channel – A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted path – A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

TSF data – Data created by and for the TOE, that might affect the operation of the TOE.

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

User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data – Data created by and for the user, that does not affect the operation of the TSF.

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.[8]

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

[6] Security Target BSI-DSZ-0535-2009, Version 2.2, 11.02.2009, IBM Tivoli Directory Server Version 6.2, IBM Corporation

[7] Evaluation Technical Report, Version 3, 24.02.2009, atsec information security GmbH (confidential document)

13.1 Guidance documentation

[8] IBM Tivoli Directory Server Version 6.2, Administration Guide (SC23-9941-00)

[9] IBM Tivoli Directory Server Version 6.2, Common Criteria Guide (SC23-9949-00)

[10] IBM Tivoli Directory Server Version 6.2, Command Reference (SC23-9945-00)

[11] IBM Tivoli Directory Server Version 6.2, Installation and Configuration Guide (SC23-9939-00)

[12] IBM Tivoli Directory Server Version 6.2, Messages Guide (GC23-9943-00)

[13] IBM Tivoli Directory Server Version 6.2, What's New for This Release (SC23-9938-00)

[14] IBM Tivoli Directory Server Version 6.2, Problem Determination Guide (GC23-9944-00)

[15] IBM Tivoli Directory Server Version 6.2, Server Plug-ins Reference (GC23-9942-00)

[16] IBM Tivoli Directory Server Version 6.2, Programming Reference (SC23-9946-00)

[17] IBM Tivoli Directory Server Version 6.2, Quick Start Guide (GI11-8731-00)

[18] IBM Tivoli Directory Server Version 6.2, System Requirements (SC23-9947-00)

[19] IBM Tivoli Directory Server Version 6.2, Performance Tuning and Capacity Planning Guide (GC23-9940-00)

[8] specifically

- AIS 14, Version 4: Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC, Stand 02.04.2007
- AIS 19, Version 3: Gliederung des ETR, Stand 02.04.2007
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

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.