Security Target

IBM Tivoli Directory Server Version 6.2

Version:	2.2
Status:	Release version
Last update:	2009-02-11

Copyright ©IBM 2005, 2006, 2007, 2008,2009

Document History

Version	Date	Changes	Summary	Author
0.1	2004-03-23	Initial version	Initial version produced for IBM	Staffan Persson
0.2	2004-03-30		Initial review comments/updates	Mark McConaughy
0.3	2004-04-13		Updates based on the review	Staffan Persson
0.4	2004-04-26		Remove proxy server and update of TOE summary specification.	Staffan Persson
0.5	2004-06-02		Update after internal review and review from Watson Lab	Staffan Persson
0.6	2004-07-05	Final draft	Clarifications after internal review to the descriptions of Proxy Authorization Control and Group Control.	Staffan Persson
1.0	2004-07-12	First version	Update of description for Group and Proxy Authorization Control.	Kristin M Hazlewood and Staffan Persson
1.1	2004-11-08		Clarification of replication, ACLs and of the audit functionality	Staffan Persson
1.2	2004-11-15		Updated due to evaluator findings	Staffan Persson
1.3	2004-11-22		Updated with Master DN role	Staffan Persson
1.4	2004-12-08		Addressed comments from QA, fixed some typos	Staffan Persson
1.5	2005-02-14		Updated due to evaluator findings mainly of SFR and passwd policy.	Kristin M Hazelwood and Staffan Persson
1.6	2005-03-01		Minor corrections on the password policy and access control	Staffan Persson
1.7	2005-09-19		Updated description of replication, use of Fix Pack 1 and removed support for Digest	Kristin M Hazelwood and Staffan Persson
1.7.1	2005-10-17		Updated reference name of TOE with Interim Fix 1	Staffan Persson
1.7.2	2005-12-16		Updated reference name of TOE with Interim Fix 5	Staffan Persson
1.7.3	2006-01-06		Updated the TOE environment and the minor issues in the TSS	Staffan Persson
1.8	2006-11-29		Initial update for TDS v6.1.	Scott Chapman
1.8.1	2007-01-23		Updated CC version. Added partial replication text to 2.1.3. Improved description of Fig 5. Improved “non-hostile” description in 3.2. Improved text in FAU_GEN.1 & FAU_GEN.2.	Scott Chapman
1.8.2	2007-02-15		Partially added one-way encryption.	Scott Chapman
1.8.3	2007-02-15		Completed encryption addition.	Scott Chapman
1.8.4	2007-02-23		Fixed minor inconsistencies found by the evaluator.	Scott Chapman
1.8.5	2007-02-23		Fixed evaluator comments in FIA_AFL.1b, added RFC2831 ref., updated 2.2.3 System attributes.	Scott Chapman
1.8.6	2007-02-26		Updated FPT_STM.1. Typo in 8.3.1.	Scott Chapman

Copyright ©IBM 2005, 2006, 2007, 2008,2009

1.8.7	2007-03-07		Updated section 2.1 packages and added exops to table 2.	Scott Chapman
1.8.8	2007-03-14		Added Log Mgmt to table 2.	Scott Chapman
1.8.9	2007-05-01		Updated Section 5.2.2, ER.ROUTE. Table 2 Password policy bind Initialize and verify. Updated F.MANAGEMENT.1 & 4. Updated platforms.	Scott Chapman
1.9	2007-05-04		Updated 2.2.2 (Gbl AGM) and F.MANAGEMENT.1. Updated password policy info.	Scott Chapman
1.9.1	2007-05-11		Updated replication under F.ACCESS_CONTROL. Updated app note under FDP_ACF.1.2. Updated DirDataAdmin & ReplicAdmin role descriptions.	Scott Chapman
1.9.2	2007-05-18		PasswdAdm cannot change GAGM passwords nor can they change failed login attempts.	Scott Chapman
1.9.3	2007-07-24		PasswdAdm can only unlock LDAP User accounts (F.MNGMNT.1). Grp & individual passwd policies must be disabled (F.MNGMNT.2). Prepended 'Local' to all Adm Grp Mbrs. Updated table 3 with the new Command Reference doc.	Scott Chapman
1.9.4	2007-07-31		Modified DirDataAdmin and NoAdmin definition in F.MNGMNT.1. Added SrvCnfgGrpMbr to section 2.1.3, FDP_ACF.1.2, FMT_MSA.1.1f, and F.ACCESS_CONTROL.	Scott Chapman
1.9.5	2007-08-01		Updated FMT_MSA.1, F.MNGMNT.1, and F.ACCESS_CONTROL to match final design.	Scott Chapman
1.9.6	2007-09-04		Added "Enterprise Edition" to section 1.2.	Scott Chapman
1.9.7	2007-09-19		Modified attribute access class definition in section 2.2.3.	Scott Chapman
1.9.8	2008-02-01		Clarified that MD5 is in the env in 2.3. Updated A.ENCRYPT, O.AUTHORIZE, OE.ENCRYPT. Updated F.ACCESS_CONTROL & F.I&A.	Scott Chapman
2.0	2008-02-29		Initial update for TDS 6.2.	Scott Chapman
2.1	2008-03-10		Removed HP-UX. Updated F.MANAGEMENT.2 and section 2.1.	Scott Chapman
2.1.1	2008-04-01		Changed supported OS versions.	Scott Chapman
2.1.2	2008-04-02		Clarified in section 2.2.3 that RNG and SHA-1 are in the TOE env.	Scott Chapman
2.1.3	2008-04-03		Changed modifyDN to modDN	Scott Chapman

			and modifyRDN to modRDN.	
2.1.4	2008-04-03		Updated figures 3 & 4.	Scott Chapman
2.1.5	2008-04-08		Added pre-op auditing text to section 2.2.4 and updated FIA_SOS.1 rationale in 8.3.1.	Scott Chapman
2.1.6	2008-04-18		Updated section 2.1 packages list & section 2.3.	Scott Chapman
2.1.7	2008-04-24		More updates to section 2.1 and 2.3.	Scott Chapman
2.1.8	2008-05-13		Added HP-UX Itanium to 1.2. Fixed misspelling 2.3.	Scott Chapman
2.1.9	2008-08-06		Updated FIA_ATD.1, FMT_MOF.1a, Table 2 Server Backup/Restore and Control Server Tracing exops, F.MANAGEMENT.2, and section 8.3.1.	Scott Chapman
2.2	2009-02-11		Removed Windows restriction on server instances.	Scott Chapman

Table hof contents

References

[CC] Common Criteria for Information Technology Security Evaluation, August 2005, Version 2.3, Parts 1 thru 3, CCMB-2005-08-001, CCMB-2005-08-002, CCMB-2005-08-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, August 2005, Version 2.3, CCMB-2005-08-004

[GUIDE] ISO/IEC PDTR 15446 Title: Information technology – Security techniques – Guide for the production of protection profiles and security targets, ISO/IEC JTC 1/SC 27 N 2449, 2000-01-04

[FIPS140-2] FIPS PUB 140-2: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, Issued May 25, 2001, including CHANGE NOTICES (12-03-2002)

[FIPS180-2] FIPS PUB 180-2: Specification for the SECURE HASH STANDARD, including Change Notice to include SHA-224, August 1, 2002

[FIPS186-2] FIPS PUB 186-2: DIGITAL SIGNATURE STANDARD (DSS) including Change Notice, January 27, 2000

[PSEARCH] IETF Internet-Draft, Persistent Search: A Simple LDAP Change Notification Mechanism < http://www.ietf.org/proceedings/01aug/I-D/draft-ietf-ldapext-psearch-03.txt>

[RFC1274] The COSINE and Internet X.500 Schema, RFC 1274

[RFC1777] Lightweight Directory Access Protocol, RFC 1777

[RFC1778] String Representation of Standard Attribute Syntax's, RFC 1778

[RFC1779] String Representation of Distinguished Names, RFC 1779

[RFC1823] LDAP Application Program Interface (V2), RFC 1823

[RFC2052] A DNS RR for specifying the location of services (DNS SRV), RFC 2052

[RFC2219] Use of DNS Aliases for Network Services, RFC 2219

[RFC2222] Simple Authentication and Security Layer (SASL), RFC 2222

[RFC2247] Using Domains in LDAP/X.500 Distinguished Names, RFC 2247

[RFC2251] Lightweight Directory Access Protocol (v3), RFC 2251

[RFC2252] Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, RFC 2252

[RFC2253] Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names, RFC 2253

[RFC2254] The String Representation of LDAP Search Filters, RFC 2254

[RFC2255] The LDAP URL Format, RFC 2255

[RFC2256] A Summary of the X.500(96) User Schema for use with LDAPv3, RFC 2256

[RFC2596] Use of Language code in LDAP, RFC 2596

[RFC2696] LDAP Control Extension for Simple Paged Results Manipulation, RFC 2696

[RFC2829] Authentication Methods for LDAP, RFC 2829

[RFC2830] (V3) Extension for Transport Layer Security (TLS), RFC 2830

[RFC2831] Using Digest Authenticaiton as a SASL Mechanism, RFC 2831

[RFC2849] The LDAP Data Interchange Format (LDIF) – Technical Specification, RFC 2849

[RFC2891] LDAP Control Extension for Server Side Sorting of Search Results, RFC 2891

1 Introduction

1.1 ST Identification

Title: Security Target for the IBM Tivoli Directory Server Version 6.2

Assurance level: EAL 4 augmented by ALC_FLR.1.

Keywords: Light weight Directory Access Protocol (LDAP), Access Control List (ACL), Password Policy (PP), Audit Service (AS), IBM Tivoli Directory Server (TDS)

1.2 ST Overview

This document is the Security Target (ST) for the IBM Tivoli Directory Server Version 6.2 (6.2.0.0-TIV-ITDS) running on:

- 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 (x86 32-bit)
- SuSE Linux Enterprise Server 10 SP1 (x86 32-bit).

The Security Target has been developed in accordance with the Common Criteria for Information Technology Security Evaluation (CC) version 2.3, for a claimed Evaluation Assurance Level 4 (EAL 4) augmented by ALC_FLR.1.

1.3 IBM Tivoli Directory Server Overview

IBM Tivoli Directory Server version 6.2 (TDS) is an implementation of Lightweight Directory Access Protocol (LDAP), which is compliant with the Internet Engineering Task Force (IETF) LDAP Version 2 specifications, i.e. RFC 1777 and LDAP Version 3 specifications, i.e. RFC 2251-2256. The server is a software only product and can be installed and operated on variety of hardware/software platforms.

LDAP is essentially a specialized database where the update operation is less frequent and dedicated to the common goal within the enterprise on consolidating and unifying the management of identity. TDS is built for identity management with role supports, 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 back end data store, TDS provides high performance, reliability and stability in an enterprise or e-business. As the central repository for data within an enterprise, it is a powerful, secure and standards compliant enterprise directory for corporate intranets and the Internet.

1.4 CC Conformance Claim

The ST is Part 2 conformant and Part 3 conformant to the CC version 2.3, August 2005. This means that it is conformant with the security functional requirements as specified in CC Part 2, and with the security assurance requirements for Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.1, as specified in Part 3 of the CC.

1.5 Strength of Function Claim

The TOE contains one non-cryptographic security function that is realized by a probabilistic or permutational mechanism, i.e. password based authentication. The minimum strength level claimed for this function is **SOF-medium**. Thus, the global minimum strength level claimed for the TOE is also **SOF-medium**.

2 TOE Description

This section describes the Target of Evaluation (TOE) in terms of the class of product, the operational environment, and the provided security functionality. This chapter provides a general description of the product, which also covers the features that are not part of the evaluated configuration. Feature that are not part of the evaluated configuration are explicitly identified as such.

2.1 Product Type

The IBM Tivoli Directory Server Version 6.2 (TDS) is an implementation of the Lightweight Directory Access Protocol (LDAP) and meets the requirements of LDAP Version 3 as defined in RFC 2251–2256 and LDAP Version 2 as defined in RFC 1777. The product consists of two major components: the LDAP Server and the LDAP Server Administration Daemon. The TOE described in this ST includes all of them. The server, which is the core component of the two, may be partitioned into two parts; the Front-end and the Back-end. The Front-end is the network interface to LDAP clients and the Back-end is the interface to the DB2 database. The Administration Daemon provides an interface to clients, used for the administration of the LDAP server.

The TDS Version 6.2 is a software-only product. It is delivered over the Internet and consists of several installation packages. These packages include the:

1. Base Server package
2. Proxy Server package
3. 32 Bit Server package
4. 64 Bit Server package
5. Client packages
6. Web Administration package
7. Language/Message packages
8. Entitlement (Supplied when TDS images are downloaded from Passport Advantage)

Only the following TDS packages contain the TOE:

1. Base Server package (all evaluated platforms)
2. 32 Bit Server package (Windows, Red Hat, and SuSE only)
3. 64 Bit Server package (AIX and Solaris only)

All other packages are excluded from the TOE and are considered part of the TOE environment. The TOE environment also includes applications that are not delivered with the TDS product, but are used as unprivileged tools, for example the web browser needed to administrate the TOE or the Adobe Acrobat Reader to access the supplied online documentation. There is also a secure configuration guide that must be downloaded and used for the installation and management of the TOE.

2.1.1 Defining a Directory

A directory is a collection of information about objects arranged in some order that gives details about each object. It is a specialized database, which stores typed and ordered information about objects. Directories enable users or applications to find resources that have the characteristics needed for a particular task.

If the name of an object is known, its characteristics can be retrieved. If the name of a particular individual object is not known, the directory can be searched for a list of objects that meet a certain requirement. Directories can usually be searched by specific criteria, not just by a predefined set of categories. Directories can be searched once and the results returned, or they can be searched continuously [PSEARCH] with the results returned as new entries matching the search criteria are created or as existing entries matching the criteria are modified.

A directory is a specialized database that has characteristics that set it apart from general purpose relational databases. A characteristic of a directory is that it is accessed (read or searched) much more often than it is updated (written). Because directories must be able to support high volumes of read requests, they are typically optimized for read access. Because directories are not intended to provide as many functions as general-purpose databases, they can be optimized to economically provide more applications with rapid access to directory data in large distributed environments.

A directory can be centralized or distributed. If a directory is centralized, there is one directory server (or a server cluster) at one location that provides access to the directory. If the directory is distributed, there is more than one server, usually geographically dispersed, that provides access to the directory.

When a directory is distributed, the information stored in the directory can be partitioned or replicated. When information is partitioned, each directory server stores a unique and non-overlapping subset of the information. That is, one and only one server stores each directory entry. The technique to partition the directory is to use LDAP referrals. LDAP referrals allow the users to refer Lightweight Directory Access Protocol (LDAP) requests to either the same or different name spaces stored in a different (or same) server. When information is replicated, more than one server stores the same directory entry. In a distributed directory, some information may be partitioned, and some information may be replicated.

2.1.2 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. The client server configuration showing a single server is shown in the picture below.

Figure 1: Configuration showing a client and a single directory server

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).

2.1.3 Replication of directories

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. TDS supports both full replication and partial (branch) replication of the directory tree. Any changes made to the master affecting the replicas, will be transmitted out to them. A user accessing a server may then either go to the master or to any of the replicas.

Replication is enabled as replication agreements between a server and a client. A replication agreement is part of the directory tree of the master. Changes to replication are controlled by the access control. In addition, this has been restricted in the evaluated configuration to the security roles of Primary Directory Administrator, Local Administrative Group Members (with an administrative role of Directory Data Administrator or Replication Administrator or Server Configuration Group Member), and Master Server DN. Only these security roles are able to set up and change replication agreements. (See section 2.2.2 for a description of security roles.)

For replication a number of differently configured directory servers may be involved. Any of the following configurations may be used, acting in any of the following ways:

Master/peer — The master/peer server contains the master directory information from where updates are propagated to the replicas. All changes are made and occur on the master server, and the master is responsible for propagating these changes to the replicas. There can be several servers acting as masters for directory information, with each master responsible for updating other master servers and replica servers. This is referred to as peer replication. Peer replication can improve performance and reliability. Performance is improved by providing a local server to handle updates in a widely distributed network. Reliability is improved by providing a backup master server ready to take over immediately if the primary master fails.

1. Master servers replicate all client updates, but do not replicate updates received from other masters.
2. Updates among peer servers can be immediate or scheduled.
3. Updates to the same entry made by multiple servers might cause update conflicts that will be resolved based on update timestamps.

Forwarding — A forwarding or cascading server is a replica server that replicates all changes sent to it. This contrasts to a master/peer server in that a master/peer server only replicates changes that are made by clients connected to that server. A cascading server can relieve the replication workload from the master servers in a network, which contains many widely dispersed replicas.

Gateway — Gateway replication uses gateway servers to distribute replication information effectively across a wide area network. Gateways are servers holding data, but also passing on the updates to other LDAP servers. The primary benefit of Gateway replication is the reduction of network traffic between geographically dispersed groups of LDAP servers.

Replica — An additional server that contains a read-only copy of directory information. The replicas are copies of the master (or the subtree that it is a replica of). The replica provides a backup of the replicated subtree.

These are only different configurations of the directory server and not different types of servers.

The evaluated configuration includes master, forwarding and replica servers, while the gateway server is not part of the evaluated configuration.

In the evaluated configuration, there must not be more than one master for a given entry at any particular point in time. Since gateway servers only serve a purpose in a configuration including more than one concurrently updateable master server they are not meaningful in an

evaluated configuration. Conflict resolution is not included in the TOE. Since an entry can only be updated on one server at any point in time, there should never be any replication conflicts.

In addition, replication must be configured to be single-threaded and use synchronous operations. Operating in this mode makes it easier to guarantee that update operations are executed on the peer or replica in the same order they were on the supplier server.

In replication, all the updates are made between the servers using LDAP operations. Replication means that LDAP requests are made by servers, such as updates initiated by a master server, or operations are passed on from cascading or gateway making these servers act as LDAP clients for other servers.

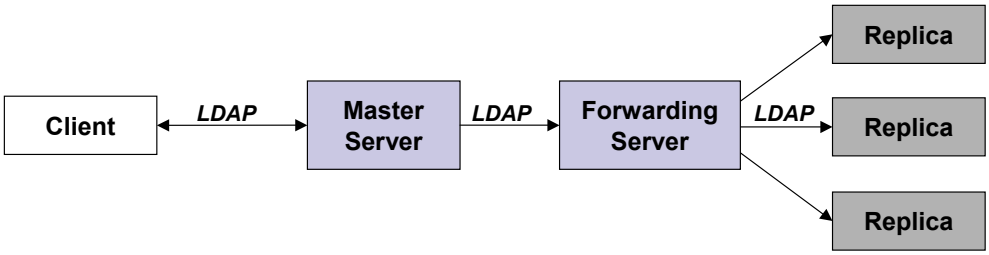

Figure 2: Configuration showing a replication scenario with one master server.

The evaluated configuration using replication contains one master server and may contain one or more forwarding servers with one or more replicas. If there is only one replica there is no need for a forwarding server, as the forwarding server is only there to offload the master.

For redundancy, the master server may send all updates it receives to a peer. The peer is equivalent to a master and may also act as a master in case the initial master no longer is available. This has to be identified by the environment that has to act accordingly, by connecting to the new master. During normal operation the master will send all updates it receives to the peer. The environment must know only to contact the master and not the peer for updates. The normal operation is shown in Figure 3 below showing the master server sending all updates to the peer server.

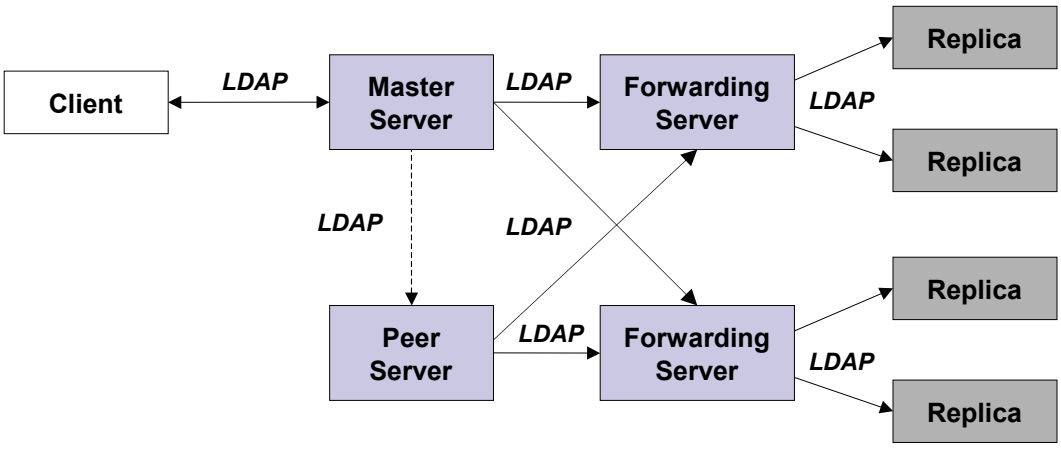

Figure 3: Configuration showing a redundant peer server.

In case the master server no longer is available, the environment must be able to detect this and use the peer server as the new master. Once the original master server is up and running again it will become the peer server with the new master peer will then provide it with all the updates to make them synchronized. This is illustrated in Figure 4 below.

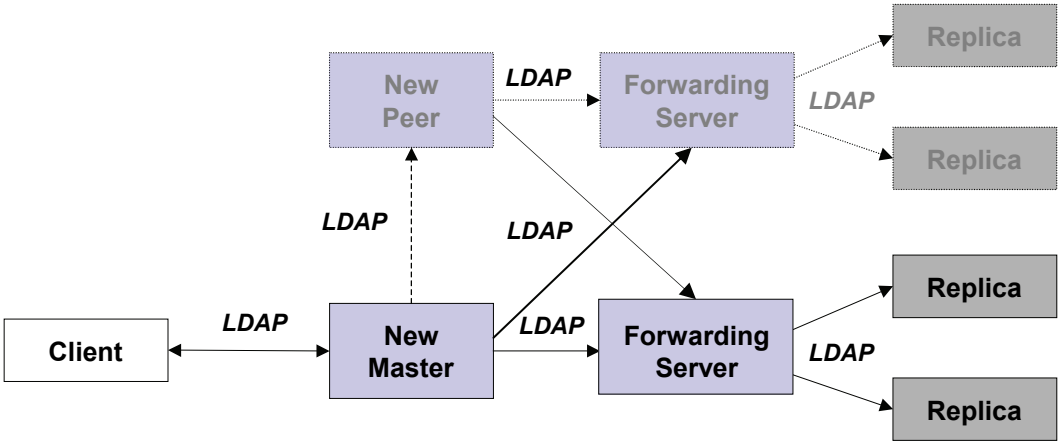

Figure 4: Peer takes over as new master server.

It is assumed that the environment is able to detect and switch over to a peer server and that only requests are sent to the currently active master. Failing to do so will not lead to security problems, but will not provide improvements to availability that the redundancy could bring. The TOE environment must assure that any updates made in a replicated environment only are made to the server currently active as master server. Failing to do so will lead to integrity problems and may lead to security problems as updates may include changes to the security.

With full replication, entire subtrees are replicated to a Replica. The replicated data includes all attributes for each entry in the subtree.

Partial replication allows for the specification of individual entries and attributes that are to be replicated. The specification is performed via filters. Each replication agreement can specify its own filter or specify no filter at all. The agreement can also specify whether missing entries should be created as surrogate entries on the Replica. Surrogate entries may be required if a child entry should be replaced but its parent should not. Having surrogate entries ensures that the access model on the partial Replica remains consistent with the access model on the supplier.

2.1.4 Distributed directory

The concept of a distributed directory is when a directory can be distributed over a number of directory servers. Typically, different branches of a directory tree are handled by different servers, but also a flat tree may be distributed over multiple servers. An LDAP request from an LDAP client is coming in to an LDAP server, the server will then reply to the request either with the result or with a referral to the servers that may be able to provide the result. This means that the client will have to issue the request to the server referred to. How this is performed is based on the entry affected by the request and referrals defining the partitioning of the DIT. Distributed directory is not part of the evaluated configuration.

2.1.5 Directory security

A directory should support the basic capabilities needed to implement a security policy. First, a method is provided to authenticate users. Authentication verifies that users are who they say they are. A user ID and password is used for authentication, using simple bind or the

Simple Authentication and Security Layer (SASL) mechanisms of digest MD5 (SASL is described in section 2.2.4). Once users are authenticated, it must be determined if they have the 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 may be attached to objects and attributes in the directory. An ACL lists what type of access each user or a group of users is allowed or denied. In order to make ACLs shorter and more manageable, users with the same access rights are often put into groups.

2.1.6 Directory Architecture and Operations

LDAP defines the content of messages exchanged between an LDAP client and an LDAP server. The messages specify the operations requested by the client (search, modify, delete, and so on), the responses from the server, and the format of data carried in the messages. LDAP messages are carried over TCP/IP, a connection-oriented protocol; so there are also operations to establish and disconnect a session between the client and server.

The general interaction between an LDAP client and an LDAP server takes the following form:

- The client establishes a session with an LDAP server. This is known as *binding* to the server. The client specifies the host name or IP address and TCP/IP port number where the LDAP server is listening. The client can provide a user name and a password to properly authenticate with the server. Or the client can establish an anonymous session using bind with default access rights. The client and server can also establish a session that uses stronger security methods such as encryption of data.
- The client then performs operations on directory data. LDAP offers both read and update capabilities. This allows directory information to be managed as well as queried. LDAP also supports searching the directory for data meeting arbitrary user-specified criteria. Searching is a very common operation in LDAP. A user can specify what part of the directory to search and what information to return. A search filter that use Boolean conditions, specifies what directory data matches the search. A search can be a one-time search or a persistent (continuous) search [PSEARCH].
- When the client is finished making requests, it closes the session with the server. This is also known as *unbinding*.

Note: Unauthenticated users are users that have not performed a bind, while anonymous users are users that have performed a bind without providing a Distinguished Name (DN) or password. Apart from distinguishing between the two when logging, there is no difference in the way unauthenticated and anonymous users are being treated by the TOE. For this reason we will use the term unauthenticated both for the anonymous and the unauthenticated. The administrator may configure the TOE not to accept any unauthenticated or anonymous users.

2.2 Security Roles and Services

2.2.1 Delivered Core Services

The server allows authorized clients to:

- Add entries to the directory,
- Delete entries from the directory,
- Modify the attributes of an entry,

- Modify the Distinguished Name (DN). For LDAPv2 this operation is called Modify Relative Distinguished Name (RDN),
- Search the directory for entries that meet certain filter criteria,
- Compare to check for presence of attributes with values matching the compare criteria in the specified entry,
- Abandon (terminate) a LDAP operation,
- Extended operations, which are server side enhancements to the LDAP operations as delivered by IBM.

In addition, the server may allow unauthenticated users to perform any operation on any entries or attributes that are not blocked by any ACL. There are a range of extended operation available as part of the core service. One extended operation, event notification, is not supported by the evaluated configuration and must therefore be deactivated by the Primary Directory Administrator in the configuration.

2.2.2 Security Roles

The TDS supports five different security roles: *Primary Directory Administrator, Local Administrative Group Members, Global Administrative Group Members, Master Server DN,* and *LDAP User*. A user account for the TOE operates as one, and only one of these roles. Only by having different accounts a user may act in different security roles, except for the case where administrators can use the Proxy Authorization feature to act as an LDAP User. (Note that Local Administrative Group Members have the Administrative Roles attribute associated with each account which further sub-divides the account's capabilities; thus, there's a distinction between security roles and administrative roles.) The following sections describe the capability of each one.

Note: The TDS has additional roles, which are similar to LDAP groups and should not be confused with the security roles. The only difference between roles and groups is that when a user is assigned to a role, there is an implicit expectation that the necessary authority has already been set up to perform the job associated with that role. With group membership, there is no built-in assumption about what permissions are gained (or denied) by being a member of that group. In this evaluation, the groups and roles are regarded as authorization attributes instead.

Primary Directory Administrator

The Primary Directory Administrator is associated with a specific user account. There is only one Primary Directory Administrator account for the LDAP server. The Primary Directory Administrator has the full rights to manage the LDAP server.

The Primary Directory Administrator is created during product installation. It consists of a user ID and a password and predefined authorization to manipulate the entire directory. The Primary Directory Administrator creates the LDAP User security role. This is an LDAP entry with a specific Distinguished Name (DN), User Password, and other attributes that represent the particular LDAP User. The Primary Directory Administrator also defines the level of authorization each LDAP User will have over entries.

Local Administrative Group Members

Local Administrative Group Members are users that have been assigned a subset of administrative privileges. Each Local Administrative Group Member can have a different set of administrative roles assigned to them by the Primary Directory Administrator (administrative roles are described in section 6.1.4). The Local Administrative Group Members security role is a way for the Primary Directory Administrator to delegate a limited

set of administrative tasks to one or more individual user accounts and maintain accountability of their actions. These users can perform various administrative tasks defined by the administrative roles assigned to them. Excepted are operations affecting the accountability or operations that may increase the privileges of those users, such as changing the password of the Primary Directory Administrator. These Local Administrative Group Members may also be called Administrative Group Members, in contrast to the Global Administrative Group Members, which are described below.

Global Administrative Group Members

Global Administrative Group Members are users that have been assigned the same set of privileges as a Local Administrative Group Member with the administrative role of Directory Data Administrator (see section 6.1.4 for an explanation of administrative roles) when it comes to access to entries in the database backend. However, they have no special privileges or access rights to any other data or operations that are not related to the database backend, such as the configuration file or audit data. All Global Administrative Group Members have the same set of privileges. The Global Administrative Group Members security role is a way for the Primary Directory Administrator to delegate rights in a distributed environment. The Primary Directory Administrator and Local Administrative Group Members with the Directory Data Administrator administrative role may act as Global Administrative Group Members using the proxy authorization.

Master Server DN

The Master Server DN is a security role used by replication that can update the entries under a replica's or a forwarding replica's replication context to which the DN is defined as a Master Server DN. The Master Server DN can create a replication context entry on a replica or forwarding replica if the DN is defined as the Master Server DN to that specific replication context or as a general Master Server DN.

LDAP User

LDAP Users are users without any specific privileges. Each LDAP User is identified with an LDAP entry containing the authentication and authorization information for that LDAP User. The authentication and authorization information may also allow the LDAP User to query and update other entries. The user is authenticated during the bind operation. Once the LDAP User is authenticated, they may access any of the attributes of any entry to which they have permissions.

2.2.3 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 backend and configurable as with the data base back end. The hard coded access rights are very restricted and cannot be changed by anyone, not even the administrator or at installation, while access to LDAP entries stored in the database backend are subject to configuration as described below.

Access is controlled to the LDAP attributes under the control of the TOE. Attributes requiring similar permissions for access are grouped together in five types of access classes. These classes are discrete; access to one class does not imply access to another class.

These classes are defined as part of the schema. The schema can only be changed by the Primary Directory Administrator, Local Administrative Group Members, and the Master Server DN security roles, in the case of replication.

Permissions are set with regard to the attribute access class as a whole. The permissions set on a particular attribute class apply to all attributes within that access class unless individual attribute access permissions are specified. The following for access classes exists:

- *System* attributes can only be changed by the directory server itself and cannot be changed by any user, except through the Server Administration Control. They can only be modified by the Primary Directory Administrator using the Server Administration Control with the modify operation. Examples of such attributes are time stamps.
- *Restricted* attributes can only be changed by the attribute owner and not by anyone else. By default all users have read access to the restricted attributes but only the entry owner can create, modify, and delete these attributes. Examples of such attributes are the ACLs controlling access to attributes.
- *Critical, sensitive* and *normal* are the classifications used for user created attributes. The default class for attributes created by a user is normal. The access class of an attribute may be changed (by an administrator that can modify the schema) to sensitive or critical to assign specific (more limited) access. A user can specify the access rights for the different access classes used in the user‘s entries. While normal may be used for any information, sensitive may for example be used for private information and or critical for even more sensitive information.

In addition, it is possible to specify access rules for individual entries or parts of the directory tree using access control lists.

In addition to the access control given to users based on the subjects DN, users may also be given proxied authorization by becoming a member of a proxied authorization group. The members of the proxied authorization group can assume any identities except the Primary Directory Administrator or Local Administrative Group Members. These administrators will be granted proxied authorization right by default, without explicitly being a member of a proxied authorization group.

There are two kinds of ACLs, non-filtered based ACLs and filtered 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 as configured. If propagated, the ACL is propagated to all descendant objects that do not contain explicit ACLs. If a descendant object contains an explicit propagating ACL, then that propagation supersedes the one initiated by the ancestor object. If a descendant object contains an explicit non-propagating ACL, then that object is skipped over, and the ancestor's propagation process continues for the rest of the descendant objects.

  Because of this propagation behavior, it is inconvenient to achieve fine ACL granularity, without having to specify explicit ACLs for many of the objects in a sub-tree. The finer the ACL granularity desired, the more cumbersome the process becomes.

- 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. Accumulation means that matching filter ACLs defined in the ancestor chain are collectively applied to the target object. Filter based ACLs have the advantage of convenience when finer ACL granularity is needed, and they provide for hierarchical refinement of access permissions through accumulation.

  Filtered ACL's provide the option of defining all ACL's at the base of the directory tree, and using the filters to select the entries that various ACL's should be applied

to. Conversely, if you wish to apply different access rules to different entries within the tree when using non-filtered ACL's, then they must be dispersed within the tree.

In addition, selected LDAP string and binary entries can be one-way encrypted using salted SHA-1 to prevent the direct observation of sensitive data. If an LDAP entry is selected to be one-way encrypted, an add or a modify operation will automatically encrypt the value provided in the request and store the encrypted value. Each LDAP entry contains its own random salt value that's used in the encryption of the LDAP entry in order to thwart simple dictionary attacks. The unencrypted value is not stored by the server. For search and compare operations, the value provided to the operation is first one-way encrypted using the salt of the LDAP entry to which it's being compared, then the result compared to the one-way encrypted LDAP entry. The Primary Directory Administrator and Local Administrative Group Members with the Schema Administrator administrative role (administrative roles are described in section 6.1.4) can specify which LDAP entries are to be encrypted. (The SHA-1 algorithm and the random number generation for the salt value are provided by the TOE environment.)

2.2.4 Auxiliary Services

In addition to the implementation of Lightweight Directory Access Protocol (LDAP), the TDS also includes enhancements added by IBM in functional and performance areas. This version uses the IBM DB2 as the backing store to provide per LDAP operation transaction integrity, high performance operations, and data backup and restore capability. It interoperates with the IETF LDAP V3 and V2 based clients. Besides supporting the standard LDAP operations, it additionally includes a number of features listed below. These features are all included in the evaluated configuration unless explicitly stated.

- Administration and configuration for the IBM Tivoli Directory Server is provided by LDAP clients being either a Web browser-based GUI or command line clients. The administration and configuration functions allow the administrators to:
    - Perform the initial setup of the directory
    - Change configuration parameters and options
    - Manage the daily operations of the directory

  The administrative tasks of the TOE are mainly done through LDAP operations on the TDS. For starting, stopping, restarting and querying the status of the TDS, LDAP operations are performed on the administration daemon, which then will carry out the operations on the directory server.
- A dynamically extensible directory schema – This means that administrators can define new attributes and object classes to enhance the directory schema. Users may dynamically modify the schema content without restarting the directory server. Since the schema itself is part of the directory, schema update operations are done through standard LDAP APIs. The following functions are provided by the TDS to determine the status of the server and the LDAPv3 dynamic extensible schema:
    - Query of the schema information through LDAP APIs
    - Dynamic schema changes through LDAP APIs
    - Server rootDSE can be queried for status information of the server
    - Dynamic configuration changes using LDAP APIs
- UTF-8 (Universal Character Set Transformation Format) – The TDS supports data in multiple languages, and allows users to store, retrieve and manage information in a native language code page.

- Simple Authentication and Security Layer (SASL) – This support provides for additional authentication mechanisms, which is a plug-in facility to allow different authentication methods to be used. Only the SASL mechanism of digest MD5 is part of the TOE (note that the MD5 algorithm of the SASL implementation is provided by the TOE environment) and may be used in the evaluated configuration in addition to the simple bind (user ID and password) authentication scheme. The passwords selected by LDAP Users, the Local Administrative Group Members, Global Administrative Group Members, Master Server DNs, and the Primary Directory Administrator are subject to a password policy. The password policy for the LDAP User and Global Administrative Group Members is determined by the Global Administrative Group Members, Master Server DNs, Local Administrative Group Members with the Directory Data Administrator administration role, or the Primary Directory Administrator. The password policy of the Master Server DN, Local Administrative Group Members, and Primary Directory Administrator can only be determined by the Primary Directory Administrator.
- The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) provide encryption of data and authentication using X.509v3 public-key certificates. A server may be configured to run with or without TLS or SSL support. However, TLS and SSL support is not part of the TOE but part of the TOE environment.
- Replication – Replication is supported, which makes additional read-only copies of the directory available, improving performance and reliability of the directory service.
- Referrals – Support for LDAP referrals, allowing directories to be distributed across multiple LDAP servers where a single server may only contain a subset of the whole directory data. Although distributed directory is not part of the evaluated configuration the feature of referral is available and is used for replication purposes.
- Access Control Model – A powerful, easy-to-manage access control model on LDAP objects (entries or attributes) is supported through ACLs.
- Change log – Changes made to the LDAP data are logged in a separate database in the LDAP server to support meta-directories or client queries to monitor directory updates.
- Security audit logging – Auditing of the LDAP operations is provided by the security auditing logging.
- A dynamic tracing facility is provided, which can be activated and deactivated by the Primary Directory Administrator and Local Administrative Group Members using extended operations. The dynamic tracing facility must not be activated as part of the evaluated configuration of the TOE.
- Proxy Authorization Control – An LDAP control is provided to allow administrators or trusted users (as specified in the Proxy Authorization Group), to perform individual LDAP operations on behalf of other end users. When this control is included, all access control decisions made for the operation are based on the user id specified in the control. LDAP Users and Global Administrative Group Members may not use this control to assume a security role. Primary Directory Administrators and Local Administrative Group Members may use this control to assume an LDAP User, or Global Administrator security role.
- Group Authorization Control – An LDAP control is provided to allow administrators or trusted users (as specified in the Proxy Authorization Group), to perform individual LDAP operations as a member of the set of asserted groups. When this control is included, all access control decisions made for the operation are based on the groups specified in the control.

- Tombstones – An LDAP feature is provided that allows for deleted entries to be stored in a separate retention area. This allows for the restoration of accidentally deleted entries. Only the Primary Directory Administrator and Local Administrative Group Members with the Server Configuration Group Member administrative role can enable/disable this feature. This feature must be disabled as part of the evaluated configuration of the TOE.
- Virtual List View – An LDAP control is provided to control the flow of search results returned by a search when a search generates large amounts of data. It also allows for the server to perform forward and backward scrolling through the search results so that a graphical user interface doesn't have to allocate space to hold all the data. Only the Primary Directory Administrator and Local Administrative Group Members with the Server Configuration Group Member administrative role can enable/disable this feature. This feature must be disabled as part of the evaluated configuration of the TOE.
- Remote Server Backup/Restore – An LDAP feature is provided that allows for a remote Primary Directory Administrator to initiate a backup/restore of the LDAP server. This feature must be disabled as part of the evaluated configuration of the TOE.
- Pre-Operation Auditing – An LDAP feature is provided that allows for pre-operation and post-operation auditing. This feature must be disabled as part of the evaluated configuration of the TOE.

2.3 TOE Boundary

The TOE can be illustrated as in Figure 5, showing the basic client/server based TDS architecture. The rectangle represented by the dashed lines indicates the TOE boundary, i.e. the standalone directory server with the administration daemon is the Target of Evaluation. Those, out of the scope of evaluation, are listed as below:

- The underlying hardware and operating system of the Directory Server
- The database, which serves as the back end data store of the directory
- The LDAP client
- The TLS/SSL module, which provides:
    - trust path between LDAP client and TDS,
    - trust path among replication servers,
    - encryption/hash and random number generation support for salted SHA-1 encryption of LDAP entries
    - encryption/hash generation support for MD5 for the SASL mechanism using MD5.

The underlying hardware and operating system, the database, the LDAP client and the TLS/SSL module are part of the TOE environment. 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.

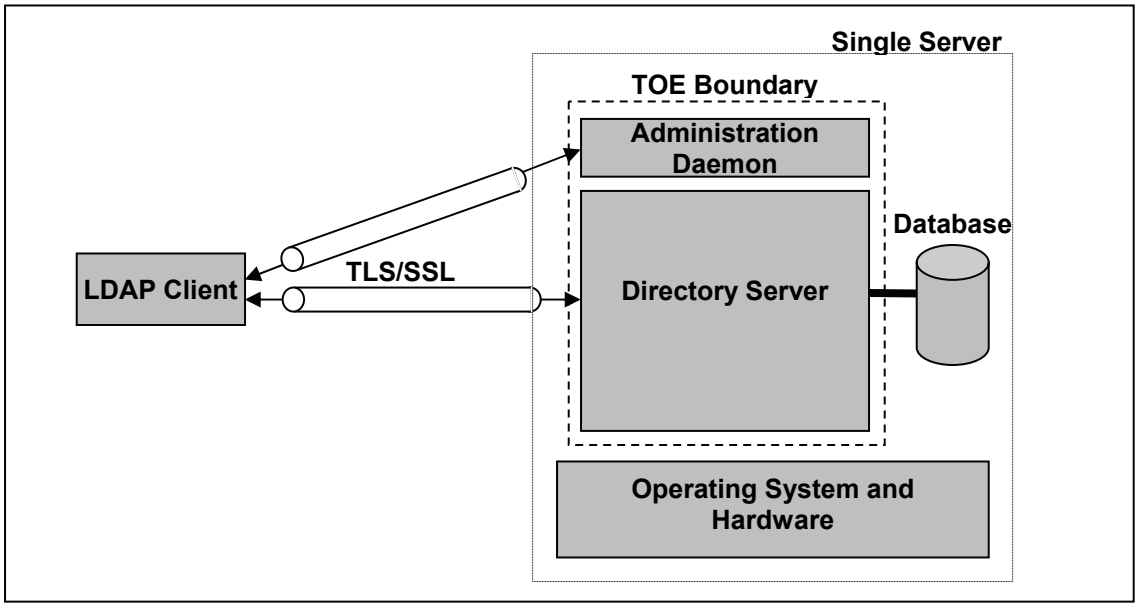

Figure 5: IBM Tivoli Directory Architecture and TOE Boundary

Figure 5 provides a high-level overview of the components showing that the Directory Server and Administration Daemon are inside the TOE boundary and the remaining components are outside the TOE boundary. It shows that the Administrative Daemon, Directory Server, Database, and Operating System can reside on a Single Server. It also shows that the LDAP Clients can exist on systems other than the system containing the TOE.

The figure shows that the LDAP Clients can communicate to both the Directory Server and the Administrative Daemon through TLS/SSL connections. It also shows that the Directory Server is the only component out of the ones shown that uses the Database. To avoid obfuscating this high-level figure, lines have been purposefully left out which show that all operations between all components must pass through the operating system and/or hardware.

LDAP clients may connect either to the LDAP server (shown in the picture above as the Directory Server) or to the administration daemon, using the LDAP protocol but using different port numbers. The directory server is providing the LDAP functionality to LDAP Users, the Local Administrative Group Members, the Global Administrative Group Members, the Master Server DN, and the Primary Directory Administrator, while the administration daemon is only used by the Local Administrative Group Members with the Server Start/Stop Administrator administrative role (administrative roles are described in section 6.1.4) and the Primary Directory Administrator for the primary purpose of starting, stopping and querying the status of the TDS. Figure 5 shows the simplest configuration of the TDS as a single server.

The hardware, operating system, and database that TDS uses are part of the TOE environment. The TOE assumes a secured communication link between itself and the client.

The evaluated configuration of TDS supports multiple server instances on a single operating system.

When using replication, both master/peer server, forwarding and replicas may be included which means that more than a single server will be used. Each server will have its own administration daemon, directory server and database, as in the single server configuration. However, the different servers will interact with each other and not just with an LDAP client.

3 TOE Security Environment

3.1 Secure Usage Assumptions

The following conditions are assumed to exist in the TOE operational environment. These assumptions include essential environmental constraints on the secure use of the TOE.

A.PHYSICAL The TOE is operated in a physically secure environment.

A.ADMIN The TOE Administrators (i.e. the Primary Directory Administrator, the Local Administrative Group Members, and the Global Administrative Group Members) are trustworthy to perform discretionary actions in accordance with security policies and not to interfere with the abstract machine, making sure that the TOE is competently administered.

A.TOEENV The TOE Environment Administrators are trustworthy to perform discretionary actions in accordance with security policies, assuring that the TOE environment is competently installed and administered.

A.COMM It is assumed that any communication links between the TOE and external systems are protected against unauthorized modification and disclosure of communication data.

A.COOP Authorized LDAP Users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

A.ROUTE It is assumed that in a replicated environment, all the update requests are made to the master server only. It is also assumed that all replicas are under the same administration and the protection in the TOE environment is as for the TOE (master server).

A.TIME It is assumed that a reliable time function is provided by the TOE environment to support the generation of audit records.

A.ENCRYPT It is assumed that the TOE environment provides one-way encryption and random number generation functions for the TOE.

3.2 Threats to security

The threats are categorized as those addressed by the TOE and those addressed by the environment.

The assets held in the TOE are information and resources under the control of the TOE, such as directory entries and TSF data. It is assumed that an attacker is either an unauthorized user of the TOE, or an authorized user of the TOE who has been granted rights to access the information or resources held by the TOE.

The threat agents are assumed to originate from a well-managed user community in a non-hostile working environment, and hence the product protects against threats of inadvertent or casual attempts to breach the system security. The TOE is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. The TOE in accordance with the strength of function claimed protects against straightforward or intentional breach of TOE security by attackers possessing a low attack potential.

3.2.1 Threats addressed by TOE

The TOE addresses the threats discussed below.

T.ENTRY A user could gain unauthorized, malicious access to resources or information, other than public information, protected by the TOE.

T.ACCESS A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or performs operations for which no access rights have been granted, via user error, system error, or other actions.

A legitimate user is someone who is:

- authenticated uniquely by the TDS, or
- unauthenticated, and appears as an anonymous user.

T.ACCOUNT Security relevant actions occur without awareness by Primary Directory Administrator. Lack of accountability of security relevant events of user or system processes may lead to failure in identifying possible security violations and holding those responsible accountable.

T.BYPASS An attacker may bypass TOE security functions to gain access to resources or information protected by the TOE.

3.2.2 Threats addressed by the operating environment

The threats discussed below must be countered in order to support the TOE security capabilities but are either:

- not addressed by, or
- only partly addressed by the TOE

Such threats must therefore be addressed in conjunction with the operating environment.

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

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

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

3.3 Organizational Security Policies

The TOE complies with the following organizational security policies:

P.PUBLIC Of the information under the control of the TOE, only information classified as public information should be made available to unauthenticated or anonymous users, if such users are given access to the TOE.

P.ENCRYPT Sensitive data may be stored one-way encrypted to prevent direct

observation. Administrators determine which entries will be encrypted.

4 Security Objectives

This section defines the security objectives for the TOE and its environment respectively.

4.1 TOE Security Objectives

The following lists the security objectives that the TOE meets.

O.AUTHENTICATE The TOE must ensure that all users are identified and authenticated before being granted access to the TOE mediated resources except for allowing unauthenticated users to perform some operations on public data. Such limited access to the TOE is configured by the Primary Directory Administrator, Local Administrative Group Members, and Global Administrative Group Members and should be compliant with the security policy of the organization responsible for the operation of the TOE.

O.AUTHORIZE The TOE must provide the ability to specify and manage access rights to objects and services by user and system process. The TOE also must enable access control to sensitive data through the optional use of salted one-way encryption.

O.ACCOUNT The TOE must ensure that all TOE users can subsequently be held accountable for their security relevant actions, except for unauthenticated users, who may be granted limited access to TOE.

O.BYPASS The TOE security policy enforcement functions must be invoked and succeed before access to TOE objects and services are allowed.

4.2 Environmental Security Objectives

Some security needs are beyond the capability of the TOE to be adequately satisfied without support from the TOE operational environment. Those security needs derive environmental security objectives, which are listed as below:

OE.MANAGE 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.

OE.ENVMANAGE Those responsible for the TOE environment must ensure that the underlying operating system and hardware is configured and managed in a secure way.

OE.PHYSICAL 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.

OE.DATABASE 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.

OE.SOPHISTICATED The TOE environment must sufficiently counter the threat of an individual (other than an authorized user) gaining unauthorized access via sophisticated technical attack.

OE.BACKUP The TOE environment must provide backup facility for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecure status. This includes the provisions necessary to ensure the availability of the TSF data and user data stored outside of the TOE.

Copyright ©IBM 2005, 2006, 2007, 2008,2009

OE.COMMUNICATION	The communication links between the TOE and LDAP clients on external systems and replicas are protected from unauthorized modification and disclosure of communication data.
OE.ROUTE	The TOE environment must ensure that in a replicated environment all the update requests are made to the master server only. It must also ensure that that all replicas are under the same administration and has the same protection as is required for the TOE (master server).
OE.TIME	The TOE environment must provide a reliable time source.
OE.ENCRYPT	The TOE environment must provide functions for support of one-way encryption of sensitive data and random number generation to the TOE.

5 IT Security Requirements

This section contains the security functional requirements (SFRs) and security assurance requirements (SARs) that must be satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and Evaluation Assurance Level (EAL) 4 assurance components from Part 3 of the CC, augmented with ALC_FLR.1 for flaw remediation.

5.1 TOE Security Functional Requirements

This section identifies and specifies the SFR components that the TOE, is intended to meet for the purposes of this CC evaluation. All of these SFR components are chosen from Part 2 of the CC to directly or indirectly (i.e., via a functional component dependency) satisfy the security objectives for the TOE, summarized in Table 1.

Operations that are completed on the SFR components are indicated throughout this section through the use of Bold Italic text. The iteration operation has been performed for FIA_AFL.1, FIA_SOS.1 and FMT_MOF.1. The two SFR components are identified by adding the letter a and b after the SFR as for FMT_MOF.1a and FMT_MOF.1b.

Table 1: Summary of Security Functional Requirements for the TOE

SFR Components	
Identifier	**Name**
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_STG.1	Protected audit trail storage
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FIA_AFL.1a	Authentication failure handling (for the LDAP Users)
FIA_AFL.1b	Authentication failure handling (for the administrators)
FIA_ATD.1	User attribute definition
FIA_SOS.1a	Verification of secrets (for the LDAP Users)
FIA_SOS.1b	Verification of secrets (for the administrators)
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MOF.1a	Management of security functions behavior
FMT_MOF.1b	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-bypassability of the TSP

5.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***not specified*** level of audit; and

c) ***Including the following events:***

- ***Bind (LDAP v2 and v3)***
- ***Unbind (LDAP v2 and v3)***
- ***Search (LDAP v2 and v3)***
- ***Add (LDAP v2 and v3)***
- ***Modify (LDAP v2 and v3)***
- ***Delete (LDAP v2 and v3)***
- ***ModDN (LDAP v3) and ModRDN (LDAP v2) operations***
- ***Compare (LDAP v2 and v3)***
- ***Event notification (LDAP v3)***
- ***Extended operations (LDAP v3)***

Application Note: All supported LDAP operations performed on the server or administration daemon are audited. The list above shows the full set of LDAP operations supported by the server. However, the administration daemon only supports a limited set of LDAP operations, i.e.: bind, unbind, search, and extended operations. Therefore, the administration daemon only audits the following events: start-up, shutdown, bind, unbind, search, and extended operations. All other LDAP operations will be rejected by the administration daemon and will therefore not be audited by the administration daemon. Note that the operation event notification, although listed above is not considered part of the evaluated configuration

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST: ***none***

Application Note: The subject identity for unauthenticated or anonymous users assigned will be the one of the unauthenticated or anonymous user identity. The subject identity for the start-up and shutdown of the audit function is not being audited.

5.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note: The unauthenticated or anonymous users will be assigned the unauthenticated or anonymous user identity. The subject identity for the start-up and shutdown of the audit function is not being audited.

5.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide the ***authorized administrators*** with the capability to read ***all audit information*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: The authorized administrators for this function are the Primary Directory Administrator and the Local Administrative Group Members with either the Audit Administrator or Server Configuration Group Member administrative roles.

5.1.4 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Application Note: Only the Primary Directory Administrator and the Local Administrative Group Members have read access. Local Administrative Group Members must have the Audit Administrator and/or Server Configuration Group Member administrative role to perform this function.

5.1.5 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to ***prevent*** unauthorized modifications to the audit records.

Application Note: Only the Primary Directory Administrator and the Local Administrative Group Members with the Audit Administrator administrative role have the privilege to delete audit records. This is done by deleting the whole content of an audit file.

5.1.6 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the ***Directory Access Control SFP*** on ***users as subjects and directory entries and attributes as objects*** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Application Note: Access rights may be attached to users, groups and roles. Subjects that can access directory entries or attributes are users, but the decision if to grant the requested access takes the user's membership in groups and the user's role into account. For proxied authorization, the user assumes the proxied identity and the ACL restrictions for the proxied identity. Users using the group control assume group membership in the asserted set of groups and the ACL restrictions for the asserted groups.

5.1.7 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***Directory Access Control SFP*** to objects based on ***three attributes sets:***

1. ***Entry Owner Information:***
   - ***entryOwner: defines entry owner.***
   - ***ownerPropagate: indicates whether to propagate the ownership of the entry to all descendant entries.***

2. ***Access Control Information (ACI)***
   - ***Non-filter based***
     - ***aclEntry: defines the access control information.***
     - ***aclPropagate: indicates whether to propagate access control information of the entry to all descendant entries.***
   - ***Filter based***
     - ***ibm-filterAclEntry: defines filter-based access control information.***
     - ***ibm-filterAclInherit: indicates whether to terminate accumulation of access control information.***
3. ***Encryption Information:***
   - ***ENCRYPT: defines the encryption type if the value is encrypted.***

FDP_ACF.1.2 The TSF shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed ***in the following evaluation order:***

1. ***By comparing the subject's bind DN with the effective entryOwner attribute values. The entry owner has full access to the target entry.***
2. ***If the subject does not possess the entry ownership, the check for access continues by comparing the subject's DN with the effective ACI of the target entry. Depending on the ACI type two access control modes are possible:***
   - ***I. In non filter-based ACL this means matching the subject DN with the subject of the ACI information. If a match on the subject is found the permissions defined in the corresponding ACI are enforced.***
   - ***II. In filter-based ACL this means matching the subject DN and the requested object, with the subject and object of the ACI information. If a match on both the subject and the object is found the permissions defined in the corresponding ACI are enforced.***
3. ***If no ACI information is found for the target object either explicitly or through inheritance, then default access is given.***

Application Note: The Primary Directory Administrator, the Local Administrative Group Members with the Directory Data Administrator administrative role, and the Global Administrative Group Members are the entryOwners for all objects in the directory by default, and this entryOwnership cannot be removed from any object. For proxied authorization, the user assumes the proxied identity and the ACL restrictions for the proxied identity. It is not possible to gain the rights of Primary Directory Administrator or Local Administrative Group Members by using proxied authorization with one exception. The Primary Directory Administrator and Local Administrative Group Members with the Directory Data Administrator administrative role can become Global Administrative Group Members by using the proxied authorization. Entries under the "cn=Configuration" suffix are not subject to configurable access control. In general, these server configuration settings may only be read or updated by the Primary Directory Administrator and the Local Administrative Group Members with the Server Configuration Group Member administrative role. Only the Primary Directory Administrator and Local Administrative Group Members with the Audit Administrator

administrative role can modify the auditing configuration settings. Global Administrative Group Members and LDAP Users have no access to the server's configuration. In the evaluated configuration, access to replication related objects are restricted to the rights related to the Primary Directory Administrator, the Local Administrative Group Members with the Replication Administrator, Server Configuration Group Member, and/or Directory Data Administrator administrative roles, and to the Master Server DN only.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***any subject may be allowed access to public information.***

Application Note: Anonymous users may only have access to public information if the Primary Directory Administrator configured anonymous binds to the TOE to be allowed.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the ***following rule:***

- ***if an object is one-way encrypted by the TOE, an operation on the object will not return the unencrypted value of the object.***

Application Note: Section 6.1.2 defines the rather complex rules for access control defined in FDP_ACF.1. A later version of this Security Target may try to express those rules in FDP_ACF.1.

5.1.8 FIA_AFL.1a Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***3*** unsuccessful authentication attempts occur related to ***consecutive authentication attempts of the same End User.***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall ***prohibit further login of that End User until an authorized administrator has reset that End User's password.***

Application Note: The number of unsuccessful authentication attempts can be specified by the Primary Directory Administrator, Local Administrative Group Members with an administrative role of Directory Data Administrator, a Global Administrative Group Members, or Master Server DN as referred to by the term "authorized administrator" above. The value of three unsuccessful attempts is the one selected for the evaluated configuration. The authentication failure handling applies to all LDAP Users and Global Administrative Group Members as referred to by the term "End User" above, but not to the Primary Directory Administrator, to the Local Administrative Group Members, or to the Master Server DN. For these administrative users, the FIA_AFL.1b applies.

5.1.9 FIA_AFL.1b Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***3*** unsuccessful authentication attempts occur related to ***consecutive authentication attempts of the Administrator.***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall ***prohibit further login of that Administrator from any host other than the one on which the directory server is running. After a successful local login, or a restart of the directory server, the Administrator's account is restored to normal access.***

Application Note: This authentication failure handling only applies for the Primary Directory Administrator, Local Administrative Group Members, or Master Server DN, as referred to by the term "Administrator" above. The number of unsuccessful authentication attempts can be specified by the Primary Directory Administrator or Local Administrative Group Members with the Server Configuration Group Member administrative role. The value of three is the one selected for the evaluated configuration.

Local login is only possible for the Primary Directory Administrator. In case of a blocked account, the Local Administrative Group Members and Master Server DN cannot log on until the Primary Directory Administrator changes their password.

5.1.10 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- ***Distinguished Name of the user***
- ***User password***
- ***pwdChangedTime: it specifies the last time the user's password was changed***
- ***pwdFailureTime: it holds the times of the consecutive authentication failures, which are internally maintained by the directory.***
- ***pwdAccountLockedTime: it holds the time that the user's account was locked***
- ***pwdReset: it holds a flag to indicate whether the user password has been reset and therefore must be changed by the user on next authentication***

Application Note: In addition to these attributes, there are several other user attributes, which are not considered to be security attributes. All these attributes are maintained for LDAP Users and for Global Administrative Group Members. All of these attributes except pwdChangedTime and pwdReset are maintained for the Primary Directory Administrator, for the Local Administrative Group Members, and for the Master Server DN.

5.1.11 FIA_SOS.1a Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***the password policy constraints, defined by the following attributes:***

- ***Minimum length of 8 characters***
- ***Minimum number of 2 non-alphabetic characters***
- ***Minimum of 4 alphabetic characters***
- ***Maximum of 2 identical characters***
- ***Maximum age of 90 days***
- ***Minimum time of 1 day to expire before a password can be changed again***

Application Note: The Primary Directory Administrator, Local Administrative Group Members with the Directory Data Administrator administrative role, Global Administrative Group Members, and Master Server DN have the ability to specify different values than those listed above. The above listed values are those that are considered for a secure configuration. The claimed SOF for the authentication mechanism is SOF-medium. This claim is based on the setting above for the verification of secrets, when using simple bind and using the SASL mechanism with MD5. The Primary Directory Administrator's, Local Administrative Group Members', or Master Server DN's passwords are not subject to these constraints. They are subject to the constraints in FIA_SOS.1b described below.

5.1.12 FIA_SOS.1b Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***the password policy constraints, defined by the following attributes:***

- ***Minimum length of 8 characters***
- ***Minimum of 2 non-alphabetic character***
- ***Minimum of 4 alphabetic characters***
- ***Maximum of 2 identical characters***

Application Note: The Primary Directory Administrator, Local Administrative Group Members, and Master Server DNs are subject to these constraints, when using the simple bind and using the SASL mechanism with MD5. The above listed values are those that are considered for a secure configuration. The claimed SOF for the authentication mechanism is SOF-medium. This claim is based on the setting above for the verification of secrets, when using simple bind and using the SASL mechanism with MD5.

5.1.13 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow ***limited operations as assigned by authorized administrators in compliance with the security policy*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The Primary Directory Administrator and the Local Administrative Group Members with the Server Configuration Group Member administrative role are the authorized administrators and may allow unauthenticated users to perform operations on public information, without a previous authentication if anonymous bind is allowed and the ACLs are allowing this. The bind/unbind is part of the user authentication and abandon is an allowed operation also for unauthenticated users.

5.1.14 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow ***limited operations as assigned by authorized administrators in compliance with the security policy*** on behalf of the user to be performed before the user is identified**.**

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The application note for FIA_UAU.1 also applies for the identification since this is performed as one bind operation.

5.1.15 FMT_MOF.1a Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***modify the behavior of*** the functions ***authentication mechanism*** to ***authorized administrators***.

Application Note: Only the Primary Directory Administrator, Local Administrative Group Members with the Directory Data Administrator administrative role, Global Administrative Group Members, and the Master Server DN are authorized to perform this function.

5.1.16 FMT_MOF.1b Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***disable, enable, and modify the behavior of*** the functions ***audit service*** to ***authorized administrators***.

Application Note: Only the Primary Directory Administrator and Local Administrative Group Members with the Audit Administrator administrative role are authorized to perform this function.

5.1.17 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***Directory Access Control SFP*** to restrict the ability to ***modify, delete, or read*** the security attributes:

a) ***Password – User (account owner), Global Administrative Group Members, Local Administrative Group Members (with Directory Data Administrator or Password Administrator administrative role), or Primary Directory Administrator***

b) ***Password policy – The attributes of the user password policy for users defined in the database can be read by everybody, but only changed by the Primary Directory Administrator, Local Administrative Group Members (with Directory Data Administrator administrative role), Global Administrative Group Members, or Master Server DN***

c) ***Entry Owner Information – LDAP User (entry owner), Primary Directory Administrator, Local Administrative Group Members (with Directory Data Administrator administrative role), or Global Administrative Group Members***

d) ***Access Control Information – LDAP User (entry owner), Primary Directory Administrator, Local Administrative Group Members (with Directory Data Administrator administrative role), or Global Administrative Group Members***

e) ***Audit options – Can be read by Primary Directory Administrator and all Local Administrative Group Members, but only modified by the Primary Directory Administrator or Local Administrative Group Members (with Audit Administrator administrative role)***

f) ***Replication behavior – Changes to the replication behavior in the configuration file can only be made by the Primary Directory Administrator, the Local Administrative Group Members (with Directory Data Administrator or Replication Administrator or Server Configuration Group Member administrative role), and the Master Server DN***

g) ***Administrative roles – Can be read by Primary Directory Administrator and all Local Administrative Group Members, but only modified by the Primary Directory Administrator***

h) ***Encryption Information – Can be read and modified by Primary Directory Administrator or Local Administrative Group Members (with Schema Administrator administrative role)***

to ***those users or roles as identified above.***

Application Note: Local Administrative Group Members cannot modify the password of the Primary Directory Administrator or other Local Administrative Group Members. Local Administrative Group Members with Password Administrator administrative role can modify LDAP User passwords. The passwords cannot be read as clear text, since they are stored in an encrypted form in the evaluated configuration of the TOE.

5.1.18 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Application Note: This requirement applies only to the Encryption Information security attributes.

5.1.19 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the ***Directory Access Control SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***Primary Directory Administrator, the Local Administrative Group Members, Global Administrative Group Members, Master Server DN or authorized LDAP Users with roles of proper privileges*** to specify alternative initial values to override the default values when an object or information is created.

Application Note: Restrictive attributes apply to the privileges and rights granted to new users and to new attributes created. This is interpreted so that new users will not be assigned any special privileges. However, by default all users have read access rights to normal, system, and restricted attributes. The ability of a Local Administrative Group Members account to perform these actions depends on the Administrative Roles assigned to the account.

5.1.20 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to ***modify*** the ***TOE security configuration made in the schema file and in the configuration file*** to ***authorized administrators***.

Application Note: The Primary Directory Administrator can modify both the schema file and configuration file. Local Administrative Group Members with the Schema Administrator administrative role can modify the schema file. Local Administrative Group Members with the Server Configuration Group Member administrative role can modify most of the configuration file, though there are some exceptions for example the audit entries and other user's passwords. Local Administrative Group Members with Audit Administrator administrative role can modify the audit related entries in the configuration file.

5.1.21 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

- ***a) Password management***
- ***b) Password policy management***
- ***c) User management***
- ***d) Access control management***
- ***e) Audit management***
- ***f) Replication management.***

5.1.22 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles ***Primary Directory Administrator, Local Administrative Group Members, Global Administrative Group Members, Master Server DN and LDAP User.***

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.23 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2 TOE Environment Security Functional Requirements

This section identifies and specifies the environmental SFR components that the environment of the TOE is intended to meet for the purposes of this CC evaluation. All of these SFR components are chosen to directly or indirectly (i.e., via a functional component dependency) satisfy the environmental security objectives for the TOE.

5.2.1 IT Security Requirements for the underlying Operating System

FCS_COP.1a Cryptographic salt operation

FCS_COP.1.1 The ***IT environment*** shall perform ***generation of random numbers*** in accordance with a specified cryptographic algorithm ***Universal Software Base True Random Number Generator algorithm*** and cryptographic keys sizes ***none*** that meet the following:

- ***conformant to FIPS 186-2 [FIPS186-2], Appendix 3.2 as required in FIPS 140-2 annex C [FIPS140-2]***

FCS_COP.1b Cryptographic hash operation

FCS_COP.1.1 The ***IT environment*** shall perform ***digest generation and digest verification*** in accordance with a specified cryptographic algorithm ***SHA-1*** and cryptographic keys sizes ***none*** that meet the following:

- ***conformant to the Secure Hash Standard (SHS) as defined in FIPS 180-2 [FIPS180-2]***

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The ***IT environment*** shall be able to provide reliable time stamps for **use by the TSF**.

5.2.2 Non-IT Security Requirements for the TOE Environment

The following requirements for the non-IT environment of the TOE need to be satisfied:

ER.ATTACK – Sophisticated Attacks

The TOE as well as the database needs to be protected against sophisticated attacks by appropriate measures in the TOE environment if such protection is required by the operational policy. This includes also potential denial-of-service attacks when the functions of the TOE are used for time critical applications.

Note that this requirement may be satisfied by physical / organizational controls, IT controls or a combination of both. This Security Target does not prescribe how the required protection is achieved.

ER.BACKUP – Backup and Recovery

Backup of the TSF data and the TOE user data have to be taken which allow to restore the TOE with its TSF data and user data in a known and secure state. Backup frequency and strategy must be defined in the security policy of the organization responsible for the operation of the TOE. Backup data needs to be adequately protected to prevent loss, unauthorized access or modification.

ER.COMMUNICATION – Protection of the Communication

Communication links between the TOE and LDAP clients on external systems need to guarantee the authenticity of the communication partner and need to be protected from unauthorized access to and modification of communication data.

ER.OS-MANAGE – Management of the Operating System Environment

The operating system and hardware used to run the TOE on must be configured and managed by competent and trustworthy personnel in a way that ensures the security, preventing unauthorized access to the TOE, TSF data and user data.

Note that this requirement may be satisfied by physical / organizational controls, IT controls, or a combination of both. This Security Target does not prescribe how the required protection is achieved.

ER.MANAGE – Management of the TOE

The TOE must be installed and managed by competent and trustworthy personnel in a way that ensures the security, preventing unauthorized access to the TOE, the TSF data and user data.

ER.DATABASE – Management of the Database

The database used to store the TSF and user data must be protected from unauthorized access, tampering and loss of data. The database must be configured and managed by competent and trustworthy personnel to ensure this protection at all operational stages.

ER.ROUTE – Routing of LDAP Requests

In an environment using replication, all LDAP update (add, delete, modify, modDN, modRDN) requests must be routed to the currently active master server. This is to avoid the possibility of a replication conflict occurring because the same entry was updated on two peer servers at about the same time, leading to potential inconsistencies. The environment must ensure that that all replicas are under the same administration and has the same protection as the TOE (master server). This applies both to the physical, logical and administrative protection of the server as to the communication with the replication servers.

Copyright ©IBM 2005, 2006, 2007, 2008,2009

5.3 TOE Security Assurance Requirements

The target evaluation assurance level is EAL 4 [CC] augmented by ALC_FLR.1.

6 TOE Summary Specification

This section provides a description of the TOE security functions and assurance measures, which meet the TOE security requirements specified in Section 5.

6.1 TOE Security Functions

The TOE security functions are described as follows:

6.1.1 F.AUDIT

The TOE provides audit generation service; the administration daemon and the server each have a separate **audit log file**. In the audit log file, audit entries are written in chronological order to keep traces of users' activities and to keep track of any changes made to the audit function.

The audit log files are stored as text files, which are managed and reviewed using the audit review as part of F.MANAGEMENT.4.

Audit Generation (F.AUDIT)

The audit service will generate at least one audit log entry for each valid LDAP request received by the server, when configured to do so. The entry is generated when the administration daemon and the server is about to return the corresponding LDAP response to the client, i.e., when the result of the processing is known.

The following administrators are authorized to manage auditing:

- Primary Directory Administrator
- Local Administrative Group Members with the Audit Administrator administrative role.

There are three versions of the audit function that can be selected by an authorized administrator, version 1, 2 or 3. Only version 3 must be used in an evaluated configuration, since only version 3 is able to audit the operations as required.

In addition to the LDAP operations, audit events are also generated by the audit service for starting or stopping of the audit service, or any changes made of the audit configuration options. These messages will be logged in the audit log as well as in the error log. This is to cover the case that the audit log is full and no more entries could be added.

The audit log will grow and requires an authorized administrator to manage (delete, save, or replace) the content of the audit log (as part of the TOE environment). In case the administration daemon or the server is not able to write to the audit log file, i.e. the device is out of space, an error message will be written in the corresponding error log file; the TDS will continue to operate, but the auditing function will no longer generate audit entries into the audit log file.

To accurately track a user's activity, each message entry contains the following information:

- time when the activity occurs,
- the user's identity or unauthenticated and anonymous for unauthenticated and anonymous users respectively,
- the activity, and
- the result of the activity.

The format of each audit version 3 message entry generated by the administration daemon, and the server will be:

```
AuditV3 -- Timestamp1 -- message text
```

Each non-message entry will contain a header (general information) and operation specific data. The header will be in the following format:

```
AuditV3 -- Timestamp1 -- Version number + [TLS] [SSL] +
[unauthenticated or anonymous] Operation—bindDN: server
encoded DN string -- client:Client IP address:Port number --
ConnectionID: xxxx -- received: Timestamp2 -- Result or
Status string
[Unique ID]
[Control String]
```

Where:

Timestamp 1
Is the local time the entry is logged (i.e., when the processing of the request is done).

Version number +[TLS] [SSL]+[unauthenticated or anonymous] Operation
Shows the LDAP request that was received and processed. Version number is V3, in the evaluated configuration. TLS or SSL indicates whether TLS or SSL was used. Unauthenticated indicates whether the request was sent by an anonymous or unauthenticated client. If the client was anonymous or unauthenticated the text "authenticated" or "anonymous" will be shown before the Operation. For authenticated requests, this will be omitted and the bindDN user ID will be shown as described below.

bindDN: server encoded DN string
Shows the bind DN. The encoding done by the server is to hide the DN from trivial viewing. The server will provide a decoding function through an LDAP search of special audit related attributes. For V3 unauthenticated or anonymous requests, this field will not be shown.

client:Client IP address:Port number
Shows the client's IP address and port number.

ConnectionID: xxxx
Shows the connection identification number used to tie all the entries of a connection together (i.e. all events between a Bind and an Unbind).

received: Timestamp 2
Is the local time when the request was received, or more precisely, the beginning time when the request was processed. Its format is the same as Timestamp 1.

Result or Status string
Shows the result or status of the LDAP operation. The result is a text message like "success" or "operationsError".

Unique ID
This identifier is sent from the client to the server in its own control, it is for example used for proxied authorization, i.e. when a user is performing an operation on behalf of another user id. In such an environment the unique ID is passed along with the operation to any other servers that are chained to. The other servers also include the ID in their audit logs as part of auditing the control that carried the ID, to allow the operations to be correlated in audit logs from multiple servers.

Control String
This section contains an OID and appropriate content related to any control that was included with the operation being logged.

For the LDAP operation a message will follow the header and display the operation specific data of that LDAP operation. The following lists the operation specific data for each auditable operation.

The following information is associated with the individual operations:

Bind

name – the DN of the client authenticating to the server; **authenticationChoice** – the authentication choice (simple authentication, SASL or Kerberos, but only simple and SASL using MD5 are part of the evaluation); **authenticationMechanism** – the authentication mechanisms used, but only in case a SASL mechanism is being used.

Unbind

No operation specific data.

Search

base – the base DN for the search; **scope** – the scope of the search; **derefAliases** – the dereferencing option supplied by the client indicating how aliases dereferencing should be done in the request (either never, always, when searching, or dereferenced only when locating the base object for the search); **typesOnly** – a Boolean flag indicating whether the client wants to have the attribute types and values, or the attributes types only; **filter** – the filter string used for the search request; **attributes** – and finally the list of all attributes that are requested, provided they are specified by the client in the search request.

Add

entry – the DN that is added to the DIT (directory information tree); **attributes** – the list of attributes the added attribute contains.

Modify

object – the DN of the entry subject to modification; **operation** – and the operation type (add, delete or replace) and attribute subject to the operation. This entry is repeated for each operation/attribute pair affected by the request from the client.

Compare

entry – the DN of the entry involved in the compare; **attribute** – the name of the attribute type whose value is being compared.

Delete

entry - the DN of the entry requested to be deleted.

ModDN (for LDAP v2, this is called ModRDN)

entry – the DN of the entry subject to renaming; **newrdn** - the new DN after the renaming; **deleteoldrdn** – a Boolean value indicating if the old DN is being deleted (or copied); **newSuperior** – the name of the new parent DN for the new entry.

Event notification extended operation: registration

eventID – the event notification ID created by the server during registration; **base** – the base entry containing the baseDN, at which the notification starts in the DIT (directory information tree); **scope** – the cope of the operation; **type** – the type of event for which the client is requesting event notification. Note that this operation is not supported as part of the evaluated configuration.

Event notification extended operation: unregister

eventID – the event notification ID created by the server during registration. Note that this operation is not supported as part of the evaluated configuration.

Extended operation (with exception of event notification)

OID – the OID value for the extended operation[1].

6.1.2 F.ACCESS_CONTROL

Permission to perform a particular LDAP operation on a specified target object is granted or denied based on the subject's DN (Distinguished Name), established by the bind operation. Users, who have not performed a bind or an anonymous bind, will have an empty DN (NullDN) and are called unauthenticated or anonymous. There is no difference between the access rights given to unauthenticated and anonymous user.

In addition to the authorization given to users based on the subjects DN, users may also be given proxied authorization by becoming a member of a proxied authorization group. The members in the proxied authorization group can assume any authenticated identity except the Primary Directory Administrator or Local Administrative Group Members or Global Administrative Group Members. The proxied authorization control for specifying an authorization identity is on a per LDAP operation basis instead of a whole LDAP session basis. To use proxied authorization, user being a member of a proxied authorization group will have to pass control data along with each LDAP request, stating the proxied DN which will be the subject DN under which the operation will be performed.

The members of the proxied authorization group can assume any identities except the Primary Directory Administrator or Local Administrative Group Members. The Primary Directory Administrator, Local Administrative Group Members, or Global Administrative Group Members will be granted proxied authorization right by default, without explicitly being a member of a proxied authorization group. The Primary Directory Administrator and Local Administrative Group Members with the Directory Data Administrator administrative role are able to proxy to Global Administrative Group Members.

Each entry within the LDAP directory contains the distinguished name of the entry as well as a set of attributes and their corresponding values. Each entry has a list of entry owners kept in the attribute entryOwner. In addition each entry has a set of associated ACIs (Access Control Information). When determining access, the entryOwner information and the ACI information are used.

The access control using the ACI information is either filter-based or non filter-based. The attributes are mutually exclusive within a single containing directory entry. However, both types can co-exist in the directory tree in separate entries. The ACI type of the target entry ACI determines the mode of calculation. In filter based mode, non-filter based ACLs are ignored in effective access calculation, and vice versa.

The ACIs for an entry is determined in the following way:

a) If there is a set of explicit access control attributes at the entry, then the entry's ACI applies.

b) If there is no explicitly defined access control attributes, then traverse the directory tree upwards until an ancestor node is reached with a set of propagating access control attributes.

c) If no such ancestor node is found, the default access rights will apply. The default access rights are predefined and cannot be changed by the Primary Directory Administrator.

It is possible to grant access to groups by associate multiple subject DNs to DNs representing a group. The LDAP server also maintains dynamic groups called pseudo DNs. These group DNs can be granted rights, which will apply to all group members.

The ACI information applicable to an entry is compiled and used in the following way:

[1] Some extended operations include parameters in addition to the OID that are logged here.

1. Specificity Rule
   a) The rights assigned to the owner DN dominate over the right of the group DN.
   b) Within the same entry, individual attribute permissions dominate over the attribute class permissions.
   c) Within the same attribute or attribute class, deny dominates over grant.
2. Combinatory Rule
   - For each entry the permissions granted to subjects of equal importance, as described under a), b) and c) above are combined.
   - If the access cannot be determined within the same specificity level, the access definitions of a less specific level are used.
   - If the access is not determined after defined ACIs are applied, the access is denied.

Order of Evaluation

When determine access, processing stops as soon as access can be determined based on access evaluation order, evaluation mode and evaluation rules as described below:

1. The first check for access is done by comparing the subject's bind DN with the effective entryOwner attribute values. The entry owner has full access to the target entry. The Primary Directory Administrator is always the owner of all entries in the directory tree.
2. If the subject does not possess the entry ownership, the check for access continues by comparing the subject's DN with the effective ACI of the target entry. Depending on the ACI type two access control modes are possible:
   i. In non filter-based ACL this means matching the subject DN with the subject of the ACI information. If a match on the subject is found the permissions defined in the corresponding ACI are enforced.
   ii. In filter-based ACL this means matching the subject DN and the requested object, with the subject and object of the ACI information. If a match on both the subject and the object is found the permissions defined in the corresponding ACI are enforced.
3. If no ACI information is found for the target object either explicitly or through inheritance, then default access is given.

Encryption

String and binary LDAP entries may be one-way encrypted using salted SHA-1 to prevent direct viewing of the values. The Primary Directory Administrator and Local Administrative Group Members with the Schema Administrator administrative role can select which entries are encrypted by the server. The unencrypted values are not maintained by the server, but comparisons can be made to the encrypted entries by first performing the salted SHA-1 encryption on the comparison value using the entry's random salt value, then comparing the encrypted comparison value to the encrypted entry value to see if they match. Each encrypted entry has its own random salt value to deter simple dictionary attacks.

Access Control Attributes

The TOE controls access to all directory entry objects based on the following security attributes:

- Entry Owner Information

  - entryOwner – identifying the DN of the owner of the entry
  - ownerPropagate – specifying the inheritance of ownership in case no entry owner is specified in descendants
- Access Control Information (ACI)
  - non filter-based
    - aclEntry – specifying the access control for the non filter-based ACI
    - aclPropagate – specifying the inheritance of access control rights in case no ACI is specified in descendants
  - filter-based
    - ibm-filterAclEntry – specifying the access control for the filter-based ACI
    - ibm-filterAclInherit – specifying the inheritance of access control rights in case no ACI is specified in descendants
- Encryption Information
  - ENCRYPT – specifying the encryption type if the value is to be one-way encrypted.
- Groups and roles

Replication objects

Replication objects located in the configuration backend are controlling replication agreements and are subject to access control as other objects. In the evaluated configuration, modify access to replication objects is restricted to the Primary Directory Administrator, the Local Administrative Group Members with the Directory Data Administrator administrative role or the Replication Administrator administrative role or the Server Configuration Group Member administrative role, and to the Master Server DN. No other roles will be able to modify/add/delete/modDN/modRDN to any replication related objects.

6.1.3 F.I&A

User Authentication (F.I&A)

In order to give the users access rights to other than operations on public data, the TOE requires each user to be successfully identified and authenticated. The subject's DN is established by the identification and authentication using a bind operation. There two possible authentication methods available for the evaluated configuration. The TOE either uses a simple user ID / password authentication method to authenticate users as defined in RFC 2251, or the authentication is made using the SASL mechanisms for message digest authentication as defined in RFC 2831. Users are maintained in the directory.

The authentication mechanism is selected by the administrator and the behavior of the authentication mechanism is, in the case of simple bind and the SASL mechanism, controlled by the password policy specified by the Primary Directory Administrator (see F.MANAGEMENT.2 below).

The administrator can also specify, for simple bind and the SASL mechanism, that a user has to change his password after it has been initially set or after it has been reset by the administrator. The administrator can also define the number of consecutive failed authentication attempts after which the following happens:

- the user will not be able to log in until the administrator has reset the user's password

6.1.4 F.MANAGEMENT

The TOE allows the Primary Directory Administrators to manage the behavior of the following functions:

- Authentication function
- Authorization function
- Audit function

The TOE allows Primary Directory Administrators to configure the following security attributes:

- Password policy (Authentication function)
- Entry Owner Information (Authorization function)
- Access Control Information (Authorization function)
- Encryption Information (Authorization function)
- Audit options (Audit function)

Roles (F.MANAGEMENT.1)

The TOE supports five security roles: Primary Directory Administrator, Local Administrative Group Members, Global Administrative Group Members, Master Server DN, and LDAP User.

All five roles are defined within the TOE. While the ordinary LDAP Users and the Master Server DN have no administrative rights, the Primary Directory Administrator has the ability to define groups and other “roles” to assist in the management of access rights and privileges. Those administrator defined groups and roles are not considered to be roles in the sense of the CC requirement FMT_SMR.1 but are just ways to manage access rights more easily.

The Primary Directory Administrator also has the ability to define Local Administrative Group Members, which will have a limited set of the administrative rights of the Primary Directory Administrator.

The administrative rights can be divided into two categories, ability to make changes to the configuration of the TOE and ability to perform certain extended operations. Local Administrative Group Members have the same rights as the Primary Directory Administrator with the difference that they cannot make configuration changes to the administrative group (cn=admingroup, cn=configuration) or to change the DN or password of the Primary Directory Administrator. (The ability of a Local Administrative Group Members account to perform these actions depends on the Administrative Roles assigned to the account.)

The Primary Directory Administrator or Local Administrative Group Members with the Directory Data Administrator administrative role also have the ability to define Global Administrative Group Members, which will have administrative access to all entries in the directory except the configuration file entries (all entries under cn=configuration).

Local Administrative Group Members or Global Administrative Group Members also cannot perform some extended operations (see table below).

Table 2: Extended Operations and Security Roles

Extended operation, Short name, description and OID	Primary Directory Administrator	Local Administrative Group Members	Global Administrative Group Members	Master Server DN	LDAP User
Start TLS Request - Request to start Transport Layer Security. OID = 1.3.6.1.4.1.1466.20037	Yes	Yes	Yes	Yes	Yes
Event Notification Registration Request - Request registration for notification events. OID = 1.3.18.0.2.12.1	Yes	Yes	Yes	Yes	Yes
Event Notification Unregister Request - Request Unregister for events that were registered for using an Event Notification Registration Request. OID = 1.3.18.0.2.12.3	Yes	Yes	Yes	Yes	Yes
Begin Transaction Request - Begin a Transactional context for SecureWay V3.2 OID = 1.3.18.0.2.12.5	Yes	Yes	Yes	Yes	Yes
End Transaction Request - End Transactional context (commit/rollback) for SecureWay V3.2 OID = 1.3.18.0.2.12.6	Yes	Yes	Yes	Yes	Yes
Cascading Control Replication Request - This operation performs the requested action on the server it is issued to and cascades the call to all consumers beneath it in the replication topology. OID = 1.3.18.0.2.12.15	Yes	Yes	Yes	Note 3	Note 4
Control Replication Request - This operation is used to force immediate replication, suspend replication, or resume replication by a supplier. This operation is allowed only when the client has update authority to the replication agreement. OID = 1.3.18.0.2.12.16	Yes	Yes	Yes	Note 3	Note 4
Control Replication Queue Request - This operation marks items as "already replicated" for a specified agreement. This operation is allowed only when the client has update authority to the replication agreement. OID = 1.3.18.0.2.12.17	Yes	Yes	Yes	Note 3	Note 4
Quiesce or Unquiesce Server Request - This operation puts the subtree into a state where it does not accept client updates (or terminates this state), except for updates from clients authenticated as primary directory administrators where the Server Administration control is present. OID = 1.3.18.0.2.12.19	Yes	Yes	Yes	Note 3	Note 4
Clear Log Request - Request to Clear log file. OID = 1.3.18.0.2.12.20	Yes	Yes	--	--	--
Get Lines Request - Request to get lines from a log file. OID = 1.3.18.0.2.12.22	Yes	Yes	--	--	--
Get Number of Lines Request - Request number of lines in a log file. OID = 1.3.18.0.2.12.24	Yes	Yes	--	--	--
Start, Stop Server Request - Request to start, stop or restart an LDAP server. OID = 1.3.18.0.2.12.26	Yes	Yes	--	--	--
Update Configuration Request - Request to update server configuration for IBM Directory Server. OID = 1.3.18.0.2.12.28	Yes	Yes	--	Yes	--
DN Normalization Request - Request to normalize a DN or a sequence of DNs. OID = 1.3.18.0.2.12.30	Yes	Yes	Yes	Yes	Yes
Event Update Request – Request to reinitialize the event notification configuration OID = 1.3.18.0.2.12.31 (this operation can only be initiated by the server, not any user)	No	No	No	No	No
Log Access Update Request – Request to reinitialize the log access plugin configuration OID= 1.3.18.0.2.12.32 (this operation can only be initiated by the server, not any user)	No	No	No	No	No
Kill Connection Request - Request to kill connections on the server. The request can be to kill all connections or kill connections by bound DN, IP, or a bound DN from a particular IP. OID = 1.3.18.0.2.12.35	Yes	Note 2	Note 2	--	--
User Type Request - Request to get the User Type of the bound user. OID = 1.3.18.0.2.12.37	Yes	Yes	Yes	Yes	Yes

Copyright ©IBM 2005, 2006, 2007, 2008,2009

Extended operation, Short name, description and OID	Primary Directory Administrator	Local Administrative Group Members	Global Administrative Group Members	Master Server DN	LDAP User
Control Server Tracing Request - Activate or deactivate tracing of the LDAP Server. OID = 1.3.18.0.2.12.40	Yes	No	No	No	--
LDAP Trace Facility Request – Execute remote trace facility commands including turning tracing on and off. OID = 1.3.18.0.2.12.41	Yes	Yes	Yes	No	No
Unique Attributes Request – Enforce attribute uniqueness. OID = 1.3.18.0.2.12.44	Yes	Yes	Yes	Yes	No
Attribute Type Request – Get attributes by supported capability. OID = 1.3.18.0.2.12.46	Yes	Yes	Yes	Yes	Yes
Group Evaluation Request – This operation is used in a distributed directory environment to determine all groups that a particular DN is a member of. OID = 1.3.18.0.2.12.50.	Yes	Yes	Yes	Yes	--
Replication Topology Request – This operation is used to replicate the objects that define the topology of a particular replication context, such as the replication agreements for that context. Any user with update rights to the Replication Group Entry of the context is allowed to issue this extended operation. OID = 1.3.18.0.2.12.54.	Yes	Yes	Yes	Yes	Note 4
Replication Error Log Request – Maintain the replication error table. OID = 1.3.18.0.2.12.56	Yes	Yes	Yes	No	No
Account Status Request – This operation is used to determine if an account is locked by password policy. OID = 1.3.18.0.2.12.58	Yes	Yes	Yes	No	No
Prepare Transaction Request – Execute the transactions. OID = 1.3.18.0.2.12.64	Yes	Yes	Yes	Yes	Yes
Log Management Request – Start, stop, and provide status for the log management of TDS. OID = 1.3.18.0.2.12.70	Yes	Yes	No	No	No
Get File Request – Retrieve an LDAP file. OID = 1.3.18.0.2.12.73	Yes	No	No	No	No
Online Backup Request – Backup the DB2 database instance. OID = 1.3.18.0.2.12.74	Yes	Yes	No	No	No
Effective Password Policy Request – Retrieve a user's effective password policy. OID = 1.3.18.0.2.12.75	Yes	Yes	Yes	Note 1	Note 1
Password Policy Bind Initialize and Verify Request – Provide password policy pre-bind initialization and verification for use by the Proxy Server. OID = 1.3.18.0.2.12.79	Yes	Yes	Yes	No	No
Password Policy Finalize and Verify Bind Request – Provide password policy post-bind processing for use by the Proxy Server. OID = 1.3.18.0.2.12.80	Yes	Yes	Yes	No	No
Server Backup/Restore Request – Backup/restore the server's directory data and configuration data or suspend/resume a scheduled backup. OID = 1.3.18.0.2.12.81	Yes	Yes	No	No	No

Note 1: Can only retrieve their own password policy.

Note 2: Any connection can be killed, except connections associated with the Primary Directory Administrator and Local Administrative Group Members.

Note 3: Any DN defined as either the Master Server DN for that particular replication context or as the general Master Server DN can issue these extended operations (for that particular replication context).

Note 4: Any user who has "write" access granted in the ACL's on the Replication Group Object can issue any of these extended operations for that particular replication context.

Administrative Roles

Only the Local Administrative Group Members security role can have different administrative roles assigned to each member's account. Administrative roles control the amount of administrative privilege an account has. Only the Primary Directory Administrator can assign administrative roles to a Local Administrative Group Members account.

At a minimum, all administrative roles (including No Administrator) have:

- Read access to the schema backend
- Read access to the configuration file (including audit settings) except for the credentials of other users defined in the configuration file.

The following is a list of administrative roles supported by TDS:

- Audit Administrator (AuditAdmin) – This administrative role enables an account to gain unrestricted access to audit logs, audit log settings, and default log management settings. This means that the account is able to turn the audit settings ON and OFF and clear the audit logs as well.
- Directory Data Administrator (DirDataAdmin) – This administrative role enables an account to gain unrestricted access to all the entries in the RDBM backend. However, for setting the password attributes of RDBM entries, they still have to follow the normal password policy rules that are in effect. This role can also perform the tasks of the Replication Administrator administrative role.
- No Administrator (NoAdmin) – This administrative role disables all other administrative roles assigned to this account.
- Replication Administrator (ReplicationAdmin) – This administrative role has unlimited access to update replication topology objects (located in the database backend). This role's access rights will not be affected by ACLs or any other configuration file settings.
- Schema Administrator (SchemaAdmin) – This administrative role enables unrestricted access to the schema backend only.
- Server Configuration Group Member (ServerConfigGroupMember) – This administrative role has restricted update access to the configuration backend. In general, this role cannot modify the audit log settings or the audit log, but it can review audit logs. It cannot modify the Primary Directory Administrator credentials or the Local Administrative Group Members credentials. It contains many more restrictions that prevent the role from performing many of the actions of the other administrative roles listed here.
- Server Start/Stop Administrator (ServerStartStopAdmin) – This administrative role enables an account to start and stop both the directory server and the administrative daemon.
- Password Administrator (PasswordAdmin) – This administrative role authorizes an account to unlock LDAP User accounts and to change account passwords of LDAP User accounts without following password policy constraints that would normally be in effect.

Authentication Function (F.MANAGEMENT.2)

User Authentication Management

The user password policy which applies to LDAP Users and Global Administrative Group Members is a combination of up to 3 password policies:

- Global password policy - The default password policy if an explicit group or user password policy does not exist for that user.
- Group password policy – An optional password policy for users assigned to a specific group.
- Individual password policy – An optional password policy assigned to a user.

The TOE contains a global password policy that defines the required password rules for these users. Additionally, an administrator can create and assign a password policy to a group and/or to an individual user. The system determines the user's effective password policy by starting with the individual password policy of the user if one exists, combining the group password policies (for the groups associated with the user) if any exist with the previous result, and then combining the global password policy with the previous result. In all cases, the combining process chooses the values that maintain or potentially increase the password strength. Additionally, the TOE can globally enable and disable support for the optional group and individual password policies. When disabled, only the global password policy will apply to these users. The evaluated configuration requires the group password policy and the individual password policy to be disabled.

The password policies consist of the following password criteria which can be specified by the Primary Directory Administrator, Local Administrative Group Members with the Directory Data Administrator administrative role, Global Administrative Group Members, and the Master Server DN to enhance the quality of the passwords selected by the LDAP Users:

- Minimum length of passwords
- Minimum number of alphabetic characters
- Minimum number of non-alphabetic characters
- Maximum number of repeated characters
- Maximum number of consecutively repeated characters
- Maximum lifetime of a password
- Minimum lifetime of a password

The Primary Directory Administrator, Local Administrative Group Members with the Directory Data Administrator administrative role, Global Administrative Group Members, and the Master Server DN can also specify that a user has to change his password after it has been initially set or after it has been reset by the administrator. The Primary Directory Administrator can also define the number of consecutive failed authentication attempts after which the following happens:

- the user will not be able to log in until the administrator has reset the user's password

The Primary Directory Administrator or Local Administrative Group Members with the Directory Data Administrator administrative role, Global Administrative Group Members, and the Master Server DN can also specify if the user is allowed to change his own password.

The following section defines the password security policy settings that are considered for the evaluated configuration:

- pwdCheckSyntax – 1 (activate the password checking mechanism)
- Minimum length of passwords (pwdMinLength) – default for secure configuration is 8 characters
- Minimum number of alphabetic characters (passwordMinAlphaChars) – default for secure configuration is 4

- Maximum number of repeated characters (passwordMaxRepeatedChars) – default for secure configuration is 2
- Maximum number of consecutively repeated characters (passwordMaxConsecutiveRepeatedChars) – default for secure configuration is 0 (where 0 means disabled)
- Minimum number of non-alphabetic characters (passwordMinOtherChars) – default for secure configuration is 2
- Maximum lifetime of a password (pwdMaxAge) – default for secure configuration is 90 days (7776000 seconds)
- Minimum lifetime of a password (pwdMinAge) – default for secure configuration is 1 day (86400 seconds)
- Maximum number of consecutive failed login attempts (PwdMaxFailure) – default for secure configuration is 3
- Action to be taken when PwdMaxFailure is reached or exceeded – default for secure configuration is: LDAP User cannot log in until the administrator has reset the password (pwdLockout – TRUE and pwdLockoutDuration – 0)
- LDAP User must change his password after initialization and after reset by the Primary Directory Administrator (pwdMustChange – TRUE)
- LDAP Users are allowed to change their own password (pwdAllowUserChange – TRUE)
- pwdSafeModify – TRUE
- ibm-pwdpolicy – TRUE

Administrative User Authentication Management

Administrative users (i.e., the Primary Directory Administrator, Local Administrative Group Members and Master Server DN) have only one password policy which all administrators defined in the configuration file must follow. Only the Primary Directory Administrator can configure the behavior of the authentication function for the administrative users by setting the following values, common to all administrators:

- Minimum length of passwords – default for secure configuration is 8
- Minimum number of alphabetic characters (passwordMinAlphaChars) – default for secure configuration is 4
- Maximum number of repeated characters (passwordMaxRepeatedChars) – default for secure configuration is 2
- Maximum number of consecutively repeated characters (passwordMaxConsecutiveRepeatedChars) – default for secure configuration is 0 (where 0 means disabled)
- Minimum number of non-alphabetic characters (passwordMinOtherChars) – default for secure configuration is 2
- Maximum number of consecutive failed login attempts (PwdMaxFailure) – default for secure configuration is 3
- Action to be taken when PwdMaxFailure is reached or exceeded – default for secure configuration is: Administrator cannot log in from a remote host until the server is restarted or the administrator successfully logs in on the local host (pwdLockout – TRUE and pwdLockoutDuration – 0)

Authorization Functions (F.MANAGEMENT.3)

With the exception of the user password entry and the system attributes, the entry owners have full access rights for an entry and are able to use the authorization function to modify the authorization information on an entry.

The Primary Directory Administrator and Local Administrative Group Members with the Directory Data Administrator administrative role are the entryOwners for all objects in the directory by default, and this entryOwnership cannot be removed from any object.

The following functions for management of security attributes are available:

- **Entry owner information** – the entry owner information (entryOwner) of an entry can be set by the entry owner. This means that the entry owner can give away an entry to any other user. The entry owner information is either inherited from an ancestor or directly specified for each entry.
- **Access Control Information (ACI)** – the access control information can be specified by the entry owner. This means that these users can specify explicit access rights by specifying the access control mode and the associated attributes. These are:
    - **Non filter-based ACL** – containing the aclEntry defining the access control information and aclPropagate indicating whether to propagate the ACL information to descendants.
    - **Filter-based ACL** – containing the ibm-filterAclEntry defining the filter-based access control information, and aclPropagate indicating whether to propagate the ACL information to descendants.
- **Encryption Information –** the encryption information can be specified by the Primary Directory Administrator and by Local Administrative Group Members with the Schema Administrator administrative role. This means that these users can specify if an entry is encrypted and what the encryption type is. Additionally, they specify the proper configuration of the encryption module.

There are attributes, so-called system attributes that can only be changed by the system itself, and neither by the LDAP User nor by the Primary Directory Administrator nor the Local Administrative Group Members. An example for these attributes is pwdChangedTime, specifying the last time the user's password was changed.

Changes to the user password entries are not only subject to the access control, as described above, but in addition subject the constrains of the password policy.

Access to entries under the "cn=configuration" suffix are subject to a hard coded access control and not configurable access control by any user or administrator.

Audit Function (F.MANAGEMENT.4)

The audit management is divided into management of the audit function and audit file management. The following administrators are authorized to manage auditing:

- Primary Directory Administrator
- Local Administrative Group Members with the Audit Administrator administrative role.

Audit function management

Authorized administrators can perform the following management functions:

- The audit subsystem can be enabled and disabled.

- The audit file name can be specified.
- The auditable events can separately be activated or deactivated for the following events: bind, unbind, search, add, modify, delete, modDN (including modRDN), compare, groups on the group control, attributes on the group evaluation operation, the event notification extended operation: registration and unregistration, and all other extended operations.
- Select that only operations that failed are to be audited, or both failed and successful operations.

Note: The modDN and modRDN are indistinguishable by the audit function such that they will both be audited as modDN and also cannot be configured individually. Also note that the event notification is not part of the evaluated configuration.

Audit file management

There are three different extended operations available to authorized administrators for managing the log files. With the extended operation LDAP requests, the audit file can be queried, read, or deleted as follows:

- **Get number of lines request** – inquiry of how many lines are in the log file
- **Get lines request** – request to view a subset of the log file
- **Clear log request** – request to clear the log file

While also the Local Administrative Group Members with the Server Configuration Group Member administrative role can query the number of lines and view audit records, the Server Configuration Group Member administrative role cannot clear the audit log file. Only the authorized administrators specified above can clear the audit log file.

The LDAP server reads the lines of the log file and truncates a line down to 400 characters in case the line is larger before sending it to the client. This is set to prevent the server from sending endless lines.

Each of the extended operations must contain at least the type of the requested log file.

6.1.5 F.REF_MEDIATION

The TOE is designed such that all security policy enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. Any request for access to a directory entry the TOE receives is checked for access according to the rules defined for the TOE.

6.1.6 TOE Security Functions rationale

For a justification of the TOE security functions to meet the security functional requirements is provided in TOE Security Functional Rationale, section 8.3.1.

6.2 Assurance Measures

The assurance requirements are met by this TOE by the following assurance measures. These assurance requirements provide, primarily via review of supplied evidence, independent confirmation that these actions have been competently performed. They also include the following independent, third-party analysis:

a) Confirmation of effective configuration management

b) Confirmation of product delivery and installation procedures

c) Conformation of the life-cycle security in the development environment and in the flaw remediation

d) Confirmation that the guidance documentation is adequate

e) Confirmation that the development documentation is correct and complete

f) Verification of a sample of the vendor functional testing

g) Verification of the developers analysis for vulnerabilities and resistance against obvious penetration attacks

h) Independent functional testing

To define the assurance measures claimed to satisfy the security assurance requirements specified in section 5.3, a mapping is provided between the Assurance Requirements and the Assurance Measures, which are intended to satisfy the Assurance Requirements. As shown in Table 3, the Assurance Measures are provided in the form of description of the relevant processes and appropriate documentation associated with each requirement.

Table 3: Assurance Measures

CC Assurance Component	***Assurance Measure***
ACM_AUT.1	M.AUT Configuration Management Version Control (CMVC) is the tool used to manage configuration items of the TOE. The configuration management procedures and tools are identical to the ones used for previous versions of TDS that have been evaluated under the CC scheme. The procedures are described in separate documents.
ACM_CAP.4	M.CAP Configuration Management Version Control (CMVC) is used to manage configuration items of the TOE. Lotus team rooms are only used for distribution of documentation and for non-TOE documents that are not subject to changes, such as protocols from meetings.
ACM_SCP.2	M.SCP In addition to the previous evaluation, all documentation will be under the control of the CMVC too or in a Notes Teamroom Database, including the test results.
ADO_DEL.2	M.DEL The software along with all documentation will be delivered via the Internet using a secure download mechanism as defined in the Download Director Specification, as described in the previous evaluation.
ADO_IGS.1	M.IGS This process will be described in the document: IBM Tivoli Directory Server Version 6.2 Installation and Configuration Guide and in the IBM Tivoli Directory Server and in the Security Guide.
ADV_FSP.2	M.FSP The functional specification will be provided in the document IBM Tivoli Directory Server Version 6.2 Functional Specification.
ADV_HLD.2	M.HLD The high level design will be described in the documents IBM Tivoli Directory Server Version 6.2 High Level Design.
ADV_IMP.1	M.IMP The full source code of the TOE is provided for the evaluation.
ADV_LLD.1	M.LLD The low-level design documentation is provided for all subsystems that

CC Assurance Component	*Assurance Measure*
	implement TSF. These are new design documents developed for this release describing new components of TDS 6.2 making up the TOE.
ADV_RCR.1	M.RCR Correspondence demonstration will be provided in a separate document that maps the TOE Summary Specification to the Functional Specification and the Functional Specification to the High Level Design.
ADV_SPM.1	M.SPM A separate document describing the Security Policy Model is provided to the evaluation facility.
AGD_ADM.1	M.ADM The administrator guidance will be provided with the IBM Tivoli Directory Server Version 6.2: • Administration Guide • Command Reference
AGD_USR.1	M.USR The user guidance will be provided with the IBM Tivoli Directory Server Version 6.2: • C-Client SDK Programming Reference • Command Reference
ALC_DVS.1	M.DVS The security procedures on the development site are described in general documents that apply for IBM as a whole as well as site specific documents and specific documents for the LDAP development.
ALC_FLR.1	M.FLR Flaw remediation measures are implemented by offering well-defined points of contact to its customers for reporting potential security flaws. Defects and their status are tracked within the support chain as well as in the CM system for the implementation representation. A dedicated website notifies customers of updates to the TOE that implement corrections due to identified flaws.
ALC_LCD.1	M.LCD The life cycle security maintained by corporate security procedures along with specific Tivoli Software Group procedures addressing the software development process and description of the tools and how they are used for development.
ALC_TAT.1	M.TAT See above.
ATE_COV.2	M.COV Detailed test plans are produced to test the functions of the TOE. Those test plans include an analysis of the test coverage, an analysis of the functional interfaces tested and an analysis of the testing against the high-level design
ATE_DPT.1	See above
ATE_FUN.1	M.FUN Testing will be performed on a range of platforms as defined by the ST. Test results are documented such that the test can be repeated.

CC Assurance Component	*Assurance Measure*
ATE_IND.2	M.IND Independent testing will be performed by the evaluation facility
AVA_MSU.2	M.VLA The misuse analysis will be provided as an update to the vulnerability analysis made for the EAL 4 evaluation.
AVA_SOF.1	M.SOF A Strength of Functional analysis will be provided for the password mechanism, based on the Strength of Function Analysis made for the previous evaluation.
AVA_VLA.2	M.VLA A vulnerability analysis will be provided that describes IBM's approach to identify vulnerabilities of TDS 6.2 as well as the results of the findings.

7 Protection Profile Claims

7.1 PP Reference

This Security Target does not claim conformance with any Protection Profile that has been registered and / or evaluated.

8 Rationale

8.1 Security Objectives Rationale

Table 4 provides a mapping of TOE security objectives to threats and assumptions. Then it is followed by rationale of how each threat, assumption and organizational security policy is addressed by the corresponding security objectives.

Table 4: Mapping of Security Objectives to Threats, Assumptions and Policies

	T.ENTRY	T.ACCESS	T.ACCOUNT	T.BYPASS	TE.SOPHISTICATED	TE.CRASH	TE.PASS	A.PHYSICAL	A.ADMIN	A.TOEENV	A.COMM	A.COOP	A.ROUTE	A.TIME	A.ENCRYPT	P.PUBLIC	P.ENCRYPT
O.AUTHENTICATE	X		X														
O.AUTHORIZE		X														X	X
O.ACCOUNT			X														
O.BYPASS				X													
OE.MANAGE									X	X		X					
OE.ENVMANAGE							X		X	X							
OE.PHYSICAL							X	X									
OE.DATABASE		X					X		X	X							
OE.SOPHISTICATED					X												
OE.BACKUP						X											
OE.COMMUNICATION		X									X						
OE.ROUTE		X											X				
OE.TIME														X			
OE.ENCRYPT															X		

T.ENTRY — O.AUTHENTICATE ensures that all users are identified and authenticated before being granted access to TOE mediated resources except for allowing unauthenticated users to perform some operations on public data, configured by administrators. The administrators may also configure the TOE to reject any anonymous or unauthenticated users. It prevents unauthenticated users from access to TOE resources and services.

T.ACCESS — O.AUTHORIZE provides the capability to specify and manage access rights to TOE resources and services. Thus it prevents any user from access to data or performing operations without proper permissions.

Unauthorized access during communication and while stored in the

	external database needs to be ensured by measures in the TOE environment and are addressed by the objectives OE.DATABASE and OE.COMMUNICATION.
T.ACCOUNT	O.AUTHENTICATE ensures that all users are identified and authenticated before being granted access to the TOE mediated resources except for allowing unauthenticated users to perform some operations on public data. Such limited access to the TOE is configured by the administrators and should be compliant with the security policy of the organization responsible for the operation of the TOE. Based on the identity information, O.ACCOUNT enforces that any security related events can be further associated with those accountable for such activities. Note that unauthenticated users and anonymous users are granted limited access to public data. For those audit entries for activities performed by unauthenticated users or anonymous users, no identity information is kept in such entries. The administrators may also configure the TOE to reject any anonymous or unauthenticated users. The two objectives together prevent security relevant actions from occurring without traceability of those accountable for such actions.
T.BYPASS	O.BYPASS enforces that the TOE security policy enforcement functions must always be invoked and succeed before access to TOE objects and services are allowed. It prevents the user from circumventing the TOE security functions.
TE.SOPHISTICATED	OE. SOPHISTICATED ensures that the TOE environment have sufficient capabilities to counter the threat of illegal users gaining unauthorized access via sophisticated attacking tools applied to the underlying system.
TE.CRASH	OE.BACKUP requires that TOE environment have the backup services. Hence, upon human error, software/hardware failure, etc. which result in data loss or corruption, the system is still able to restore to a previous secure state.
TE.PASS	OE.PHYSICAL, OE.ENVMANAGE and OE.DATABASE requires that the hardware and software is physically protected, that the underlying operating system and hardware is configured and managed in a secure manner and that the database is configured and managed in a secure way, preventing the bypassing of the TOE security functions.
A.PHYSICAL	OE.PHYSICAL requires that TOE and its underlying hardware and software are physically protected from unauthorized physical modification and from technical attacks at the hardware and operating system level. Hence, this assumption is maintained.
A.ADMIN	OE.MANAGE, OE.ENVMANAGE and OE.DATABASE require that TOE and the TOE environment is managed and administered in a secure manner. Assuming that the administrators should be trusted to perform discretionary actions in accordance with security policies.
A.TOEENV	OE.MANAGE, OE.ENVMANAGE and OE.DATABASE requires that TOE and the underlying OS and HW, and database is managed and administered in a secure manner, which implies that TOE and TOE environment are competently installed and administered.

A.COMM	OE.COMMUNICATION requires that communication links between the TOE and LDAP clients on external systems are protected to against unauthorized modification and disclosure of communication data.
A.COOP	OE.MANAGE requires that the TOE is managed in a secure manned to maintain the security of the TSF data and user data. Including the protection of user passwords and setting of the access control rights under the control of the individual users.
A.ROUTE	OE.ROUTE requires that all the updates in a replicated environment are made to the current master server and not to any other server. It is also assumed that all replicas are under the same administration and that the same protection as required by the TOE (master server).
A.TIME	OE.TIME requires that the TOE environment provides a reliable time function.
A.ENCRYPT	OE.ENCRYPT requires that the TOE environment provides one or more encryption algorithms.
P.PUBLIC	O.AUTHORIZE provides the capability to specify and manage the access rights to TOE resources and services. Thus, preventing users from access to data or performing operations without proper permissions by only making public information available to any user.
P.ENCRYPT	O.AUTHORIZE requires that the TOE provides the ability to encrypt sensitive data in order to prevent direct observance of that data.

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements Rationale

Table 5 shows a mapping of Security Functional Requirements to TOE Security Objectives and Security Objectives for the TOE environment. Following such a mapping, further discussion is given on how each Security Objective is addressed by the corresponding Security Functional Requirements.

The *italic text* used in the table represents those functional components that are met by the TOE environment.

Table 5: Mapping of Security Functional Requirements to TOE Security Objectives

	O.AUTHENTICATE	O.AUTHORIZE	O.ACCOUNT	O.BYPASS	OE.MANAGE	OE.ENVMANAGE	OE.PHYSICAL	OE.DATABASE	OE.SOPHISTICATED	OE.BACKUP	OE.COMMUNICATION	OE.ROUTE	OE.TIME	OE.ENCRYPT
FAU_GEN.1			X											
FAU_GEN.2			X											

	O.AUTHENTICATE	O.AUTHORIZE	O.ACCOUNT	O.BYPASS	OE.MANAGE	OE.ENVMANAGE	OE.PHYSICAL	OE.DATABASE	OE.SOPHISTICATED	OE.BACKUP	OE.COMMUNICATION	OE.ROUTE	OE.TIME	OE.ENCRYPT
FAU_SAR.1			X											
FAU_SAR.2			X											
FAU_STG.1			X											
FDP_ACC.2		X												
FDP_ACF.1		X												
FIA_AFL.1a	X													
FIA_AFL.1b	X													
FIA_ATD.1		X												
FIA_SOS.1a	X													
FIA_SOS.1b	X													
FIA_UAU.1	X													
FIA_UID.1	X													
FMT_MOF.1a	X	X												
FMT_MOF.1b			X											
FMT_MSA.1		X												
FMT_MSA.2		X												
FMT_MSA.3		X												
FMT_MTD.1		X												
FMT_SMF.1	X	X	X											
FMT_SMR.1		X												
FPT_RVM.1				X										
FPT_STM.1			X										X	
FCS_COP.1a														X
FCS_COP.1b														X

O.AUTHENTICATE

FIA_AFL.1a for LDAP Users and FIA_AFL.1b for the administrators ensures that an attacker does not have an unlimited number of authentication attempts he could use to guess an LDAP User's and administrator password.

FIA.UID.1 ensures that, except that unauthenticated users and anonymous users are allowed access to public information and services configured by the Primary Directory Administrator or Local Administrative Group Members in accordance with security policies, each user is successfully identified before allowing any

	TSF-mediated actions for that user. FIA_UAU.1 ensures that, except that unauthenticated users and anonymous users are allowed access to public information and services configured by the Primary Directory Administrator or Local Administrative Group Members in accordance to security policies, each user is successfully authenticated before allowing any TSF-mediated actions for that user. FIA_SOS.1a ensures that password rules, for password based identification and authenticated, are enforced against all LDAP Users, preventing the bypassing or circumventing security policies. FIA_SOS.1b ensures that the passwords for administrators are of a certain quality, to prevent easy to guess passwords being used. FMT_MOF.1a ensures that the authentication function is managed by the Primary Directory Administrator or Local Administrative Group Members to enforce the appropriate password rules. FMT_SMF.1 ensures that the TSF is capable of performing management of the authentication function by password management and password policy management. Such security requirements work together to ensure successful identification and authentication prior to any TSF-mediated actions for each user.
O.AUTHORIZE	FDP_ACC.2 ensures that complete access control is enforced on access to TOE resources and services. FDP_ACF.1 ensures that the access control security policy is actually implemented by relevant security functions, based on user security attributes. FIA_ATD.1 ensures that user security attributes are maintained and managed by the TOE to provide supports for access control. FMT_MOF.1a ensures that the TSF behavior is administered and managed by the administrators, so that any change to it is restricted to authorized users. FMT_MSA.1 ensures that the TOE security attributes can only be administered and managed by the administrators authorized users. FMT_MSA.2 ensures that the security attributes related to configuring the encryption algorithms supplied by the TOE environment are appropriately set by the TOE to only use secure values. FMT_MSA.3 ensures that TOE assess control is enforced to restrict the capability to specify default security attributes to authorized users. FMT_MTD.1 ensures that access to TSF data is restricted to the Primary Directory Administrator or Local Administrative Group Members. FMT_SMF.1 ensures that the TSF is capable of performing management of the users and of the access control. FMT_SMR.1 ensures that roles/groups are maintained by the TOE and can be associated with users to facilitate the access control.

	Such security requirements work together to ensure full control and management of user, data, and services, providing authorized user access to resources and functionality.
O.ACCOUNT	FAU_GEN.1 ensures that audit log of security related activity and events are recorded. FAU_GEN.2, which is a security requirement on TOE environment, ensures that each audit event can be associated with the identity of the user that caused the event so that the user can be held accountable for security related action, except for unauthenticated user and anonymous user. However, since ability to bind and access to resources and services is defined by the Primary Directory Administrator and the Local Administrative Group Members in accordance to security policy, it doesn't pose threats to TOE. FPT_STM.1, which is a security requirement on TOE environment, ensures that each audit entry is associated with reliable time stamp. Note that this time stamp is taken from the underlying operating system, which is part of the TOE environment. FAU_SAR.1 provides the Primary Directory Administrator and the Local Administrative Group Members with the capability to review audit log. FAU_SAR.2 restricts the read access to the audit log to users of Primary Directory Administrator role and Local Administrative Group Members. FAU_STG.1 further prevents any other user than the Primary Directory Administrator and Local Administrative Group Members with the Audit Administrator administrative role from manipulating the audit log and thereby preserves the integrity audit log. FMT_MOF.1b ensures that the behavior of the audit function is managed by the Primary Directory Administrator and Local Administrative Group Members with the Audit Administrator administrative role to enforce accountability. Such security requirements, as a whole, ensure that users can be held accountable for their actions. FMT_SMF.1 ensures that the TSF is capable of performing management of the audit function.
O.BYPASS	FPT_RVM.1 ensures that security policy enforcement functions are invoked and succeed before each function is allowed to proceed so the access control is always enforced. These security requirements work together to prevent from bypassing and circumvention of TOE security policy. Note that, although unauthenticated user and anonymous user have limited access to TOE resources and services, such access is defined by the administrators and are under control by TOE security policy, hence it is not regarded as circumvention of security policy.
OE.MANAGE	No dependency to any SFR.
OE.ENVMANAGE	No dependency to any SFR.
OE.PHYSICAL	No dependency to any SFR.

OE.DATABASE	No dependency to any SFR.
OE.SOPHISTICATED	No dependency to any SFR.
OE.BACKUP	No dependency to any SFR.
OE.COMMUNICATION	No dependency to any SFR.
OE.ROUTE	No dependency to any SFR.
OE.TIME	FPT_STM.1 ensures that a reliable timestamp is provided by the TOE environment. The user attribute definition FIA_ATD.1 and verification of secrets FIA_SOS.1a also depends on a reliable timestamp to maintain the user attributes and to enforce the password policy.
OE.ENCRYPT	FCS_COP.1a provides the random salt generation algorithm to the TOE for the salted SHA-1 hash functionality. FCS_COP.1b provides the SHA-1 hash generation algorithm to the TOE for the salted SHA-1 hash functionality.

8.2.2 Dependency Analysis

Table 6 demonstrates that the security functional requirements meet all functional dependencies. The *italic text* used in the table represents those functional components that are met by the TOE environment.

As the assurance components are those standard ones for EAL 4 augmented with ALC_FLR.1, all dependencies for such EAL 4 assurance components are satisfied automatically. For ALC_FLR.1 there are no dependencies to any other requirements.

Table 6: Dependency Mapping of Security Functional Requirements

Component	Name	Dependencies
FAU_GEN.1	Audit data generation	FPT_STM.1
FAU_GEN.2	User identity generation	FAU_GEN.1, FIA_UID.1
FAU_SAR.1	Audit review	FAU_GEN.1
FAU_SAR.2	Restricted audit review	FAU_SAR.1
FAU_STG.1	Protected audit trail storage	FAU_GEN.1
FPT_STM.1	Time stamps	—
FDP_ACC.2	Complete access control	FDP_ACF.1
FDP_ACF.1	Security attribute based access control	FDP_ACC.1, FMT_MSA.3
FIA_AFL.1a	Authentication failure handling	FIA_UAU.1
FIA_AFL.1b	Authentication failure handling	FIA_UAU.1
FIA_ATD.1	User attribute definition	Non explicit to FPT_STM.1
FIA_SOS.1a	Selection of secrets	Non explicit to FPT_STM.1
FIA_SOS.1b	Selection of secrets	—
FIA_UAU.1	Timing of authentication	FIA_UID.1
FIA_UID.1	Timing of identification	—

Copyright ©IBM 2005, 2006, 2007, 2008,2009

Component	Name	Dependencies
FMT_MOF.1a	Management of security functions behavior	FMT_SMF.1, FMT_SMR.1
FMT_MOF.1b	Management of security functions behavior	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1	Management of security attributes	FDP_ACC.1 [or FDP_IFC.1] FMT_SMF.1, FMT_SMR.1
FMT_MSA.2	Secure security attributes	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	Static attribute initialization	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	Management of TSF data	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	Specification of Management Functions	—
FMT_SMR.1	Security roles	FIA_UID.1
FPT_RVM.1	Non-bypassability of the TSP	—
FCS_COP.1a	Cryptographic operation	[*FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 - Unresolved*], *FCS_CKM.4 - Unresolved*, FMT_MSA.2
FCS_COP.1b	Cryptographic operation	[*FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 - Unresolved*], *FCS_CKM.4 - Unresolved*, FMT_MSA.2

8.2.3 Demonstration of Mutual Support Between Security Requirements

The dependency analysis provided in the previous section has shown how supportive dependencies between SFRs are satisfied. This section further demonstrates that the SFRs are mutually supportive by highlighting and discussing the additional supportive dependencies, which ensures that security policies are enforced.

FPT_RVM.1 ensures that SFRs cannot be bypassed.

FIA_UAU.1 provides additional protection as it ensures that access to the TOE cannot be made by impersonate as a different user. FIA_UID.1 ensures that no security mediated functions can be initiated on behalf of a user until the user is uniquely identified to the TOE, except that limited access (to public information) is granted to unauthenticated user and anonymous user prior to identification and authentication. However, such restricted access is defined by Primary Directory Administrators and Local Administrative Group Members in accordance to the organizational security policy. Then, it poses no threats to the TOE.

The FIA_AFL.1a and FIA_AFL.1b provides assurance by preventing password guessing attacks against LDAP User and administrator accounts, by blocking the account after a defined number of failed attempts, thereby supporting the function FIA_UAU.1 that only provides access to properly authenticated users.

FIA_ATD.1 and FIA_SOS.1 have non-explicit dependencies to a reliable time in order to maintain the user attributes and to enforce the user password policy. This is addressed by the TOE IT environment in FPT_STM.1 by providing reliable time stamps.

FCS_COP.1a and FCS_COP.1b support the encryption requirements of FDP_ACF.1. FMT_MSA.2 requires that only secure values are provided by the TOE when using FCS_COP.1a and FCS_COP.1b.

FMT_SMR.1 enforces which roles users may take in the TOE and the conditions associated with assuming the role. Based on FMT_SMR.1, FMT_MOF.1a FMT_MOF.1b restricts the ability of users under specific roles to modify the behavior of functions that control security attributes or configuration data. With the aid of FMT_SMR.1, FMT_MSA.1 restricts the ability to modify security attributes or configuration data, protecting against tampering attacks through unauthorized modification of data. FMT_MSA.3 restricts default security attributes or configuration data controlled under FMT_MOF.1a, FMT_MOF.1b and FMT_MSA.1. Management of the replication relies on the access control FDP_ACC.2 and especially FDP_ACF.1. With the aid of FMT_SMR.1, FMT_MSA.2 restricts the TOE to using only secure values for the encryption algorithms specified by FCS_COP.1a and FCS_COP.1b. This is accomplished by both the configuration data used by the encryption module through controls defined by FMT_MSA.1 and through the programming interfaces of the encryption module used by the TOE. Since FMT_MSA.2 supports FCS_COP.1a and FCS_COP.1b and these FCS SFRs support FDP_ACF.1, the FMT_MSA.2 support for FDP_ACC.2 is implied.

FMT_MTD.1 restricts the ability to modify any other security relevant data, protecting against tampering attacks through unauthorized modification of data.

FMT_SMF.1 specifies the management functions for the security behavior of the authentication function (FMT_MOF.1a) and for the password and password policy (FMT_MSA.1). FMT_SMF.1 also specifies the management functions for the user and access control (FMT_MSA.1 and FMT_MTD.1), as well as for the management of the audit function (FMT_MSA.1).

FDP_ACF.1 controls rules governing user access to objects based on security attribute values and supports FDP_ACC.2. FDP_ACC.2 provides complete access control and enforces access controls on subjects and objects and all operations among the subjects and objects. Furthermore, FCS_COP.1a and FCS_COP.1b in the TOE environment support the encryption aspect of FDP_ACF.1.

FIA_SOS.1a and FIA_SOS.1b reduce the likelihood of successful direct attack aimed at the identification and authentication functions, and thus supports FIA_UAU.1.

FPT_STM.1 support time entries in audit records for FAU_GEN.1, as provided by the TOE environment. The FPT_STM.1 is not subject to any administration by any TOE administrator.

FAU_GEN.1 provides the ability to track the security related events and actions. FAU_GEN.2 ensures that the individual responsible for generating an audit event is uniquely and unambiguously identified along with the audit data. FAU_SAR.1 and FAU_SAR.2 ensure that authorized users have the capability to review data from the audit records.

8.2.4 Justification of Unresolved Dependencies

No keys are generated, used, or destroyed for FCS_COP.1a and FCS_COP.1b, so FCS_CKM.1 and FCS_CKM.4 are not required and, therefore, are unresolved.

8.2.5 Non-IT Security Requirements Rationale

Table 7 below shows a mapping of the non-IT Security Requirements for the TOE environment to the Security Objectives for the environment.

Table 7: Mapping of non-IT Security Requirements to Security Objectives for the Environment

	OE.MANAGE	OE.ENVMANAGE	OE.PHYSICAL	OE.DATABASE	OE.SOPHISTICATED	OE.BACKUP	OE.COMMUNICATION	OE.ROUTE	OE.TIME	OE.ENCRYPT
ER.ATTACK			X		X					
ER.BACKUP			X			X				
ER.COMMUNICATION							X			
ER.OS-MANAGE		X	X							
ER.MANAGE	X		X							
ER.DATABASE			X	X						
ER.ROUTE								X		

The OE.TIME is addressed by the IT Security Requirement FPT_STM.1 for the TOE environment, as described in the security functional requirements rationale, section 8.2.1.

The OE.ENCRYPT is addressed by the IT Security Requirements FCS_COP.1a and FCS_COP.1b for the TOE environment, as described in the security functional requirements rationale, section 8.2.1.

8.2.6 Appropriateness of Assurance Requirements

The TOE is supposed to thwart attackers of limited resources. The assurance requirements of EAL 4 augmented with ALC_FLR.1 bring enough assurance elements for the TOE, operating within its environment as described in this document. Furthermore, the EAL 4 assurance level augmented with ALC_FLR.1 is technically feasible and achievable based on the requirements on life-cycle support, development documents, secure delivery procedure, and configuration management. It is appropriate to satisfy users' expectations.

8.3 TOE Summary Specification Rationale

The TOE summary specification rationale is intended to show that the TOE security functions and assurance measures are suitable to meet the TOE security (functional and assurance) requirements.

To show that the selection of TOE security functions and assurance measures are suitable to meet TOE security requirements (functional and assurance), it is important to demonstrate the following:

- The specified TOE IT security functions work together so as to satisfy the TOE security functional requirements.
- That the started assurance measures are compliant with the assurance requirements.

8.3.1 TOE Security Functions Rationale

This section is intended to provide a demonstration that the TOE security functions satisfy all TOE SFRs included in the ST. This is accomplished by mapping the TOE security functions onto the TOE SFRs by Table 8, which shows that:

- Each TOE SFR is mapped onto at least one TOE security function, and
- Each TOE security function is mapped onto at least one TOE SFR.

Note that FPT_STM.1, FCS_COP.1a, and FCS_COP.1b are TOE environment security functional requirements and are to be satisfied by the TOE environment.

Table 8: Mapping of Security Functions to Security Functional Requirements

	F.AUDIT	F.ACCESS_CONTROL	F.I&A	F.MANAGEMENT	F.REF_MEDIATION
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1				X	
FAU_SAR.2				X	
FAU_STG.1				X	
FDP_ACC.2		X			
FDP_ACF.1		X			
FIA_AFL.1a			X		
FIA_AFL.1b			X		
FIA_ATD.1			X		
FIA_SOS.1a			X		
FIA_SOS.1b			X		
FIA_UAU.1			X		
FIA_UID.1			X		
FMT_MOF.1a				X	
FMT_MOF.1b				X	
FMT_MSA.1				X	
FMT_MSA.2				X	
FMT_MSA.3				X	
FMT_MTD.1				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_RVM.1					X

Table 8 shows that all the TOE security functional requirements are addressed by the TOE security functions. Below is described how the IT security functions of the TOE are suitable to meet the TOE security functional requirements.

FAU_GEN.1	The requirement for generation of audit events is satisfied by the security functions F.AUDIT, which will generate audit records for the specified events to an audit file. The audit record format and events are described as part of F.AUDIT. The audit record containing the timestamp is produced by F.AUDIT. (A reliable time-stamp is provided by the environment as expressed by the IT requirement for the TOE environment FPT_STM.1)
FAU_GEN.2	The requirement is satisfied by the association of user identities (F.I&A) with audit events (F.AUDIT).
FAU_SAR.1	The ability to read all audit records is provided by the security function F.MANAGEMENT, allowing the Primary Directory Administrator and Local Administrative Group Members to view the audit file.
FAU_SAR.2	The requirement is satisfied by the function F.MANAGEMENT, which is restricted only to the Primary Directory Administrator and Local Administrative Group Members, preventing any other users to read the audit file.
FAU_STG.1	The requirement is satisfied by the function F.MANAGEMENT, which is restricted only to Primary Directory Administrators and Local Administrative Group Members with the Audit Administrator administrative role, preventing any other user to erase the audit file.
FDP_ACC.2	The requirement for complete access control is satisfied by the function F.ACCESS_CONTROL. All objects (directory entries and attributes) are subject to access control of F.ACCESS_CONTROL.
FDP_ACF.1	The requirement is satisfied by the F.ACCESS_CONTROL, which enforces the directory access control SFP based on the entry owner information, the Access Control Information, and the Encryption Information. (The encryption functions associated with the Encryption Information are expressed by the IT environment requirements FCS_COP.1a and FCS_COP.1b.)
FIA_AFL.1a FIA_AFL.1b	The requirement for authentication failure is satisfied by F.I&A which will prevent any further authentication attempts of the same user after a specific number of consecutively failed authentication attempts. For the LDAP Users the number of failed attempts is three for a secure configuration, but the Primary Directory Administrator and Local Administrative Group Members can specify any number. For the administrators, only the Primary Directory Administrator can specify the value applicable to all administrators.
FIA_ATD.1	The requirement for user attributes is being fulfilled by F.I&A. The user attribute information is used and maintained by the F.I&A.
FIA_SOS.1a FIA_SOS.1b	The requirement for the verification of secrets is fulfilled by the user ID / password mechanisms being part of the security function F.I&A. The password policy constraints for a secure configuration are given. The Primary Directory Administrator and Local Administrative Group Members have the ability to specify different values for the LDAP Users. The

password policy for the administrators can only be specified by the Primary Directory Administrator. F.MANAGEMENT.2 contains the "maximum number of consecutively repeated characters" attribute in its description for both password policies, but neither FIA_SOS.1a nor FIA_SOS.1b contains this function. This is because the attribute values defined for this attribute in F.MANAGEMENT.2 disable this check; thus, the attribute has no attributable effect on either SFR.

FIA_UAU.1	The requirement is being met by F.I&A, which will only assign the user an identity (Distinguished Name) as part of a successful identification and authentication. Without a successful authentication the user will be regarded as unauthenticated and will only be given access to public information.
FIA_UID.1	The requirement is being met by F.I&A. Since the identification and authentication is performed as one operation, see the description above of how FIA_UAU.1 is being met by F.I&A.
FMT_MOF.1a	The requirement is being fulfilled by F.MANAGEMENT, allowing the Primary Directory Administrator and Local Administrative Group Members to modify the behaviour of the identification and authentication function, by specifying the password policy.
FMT_MOF.1b	The requirement is being fulfilled by F.MANAGEMENT, allowing the Primary Directory Administrator and Local Administrative Group Members with the Audit Administrator administrative role to disable, enable and modify the behaviour of the audit function.
FMT_MSA.1	The requirement is being fulfilled by F.MANAGEMENT, allowing the Primary Directory Administrator and certain Local Administrative Group Members to modify, delete, and read the security attributes and to disable, enable and modify the behaviour of the audit function.
FMT_MSA.2	The requirement is being fulfilled by F.MANAGEMENT where only secure values are used by the TOE to configure and use the encryption module.
FMT_MSA.3	The requirement for restrictive default values are being fulfilled by the security function F.MANAGEMENT by assigning restrictive values by installation and configuration made by the Primary Directory Administrator and Local Administrative Group Members.
FMT_MTD.1	The requirement for management of TSF data is being satisfied by the security function F.MANAGEMENT.
FMT_SMF.1	The requirement for the TSF to provide management functions is being satisfied by the security function F.MANAGEMENT.
FMT_SMR.1	The requirement for roles maintained by the TOE, the LDAP User, Local Administrative Group Members, and the Primary Directory Administrator is satisfied by the security function F.MANAGEMENT.
FPT_RVM.1	The requirement for non-bypassability of the TSP is satisfied by the security function F.REF_MEDIATION, ensuring that the access control functions are being invoked before access is given granted.

The table above shows how the security functions work together to satisfy the security functional requirements.

The requirements FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, and FAU_SAR.2 define the requirements for the audit system by specifying the audit events, in relation to the other security functional requirements. The association of each audit event with user identities is consistent with the use of the identification and authentication function (FIA_UID.1 and

FIA_UAU.1), so that FAU_GEN.2 has a basis for associating the events to user identities causing that event. In order to record the time and date of the events, FAU_GEN.1 requires a reliable time-stamp, which is provided by FPT_STM.1 (provided by the IT environment). The requirements FAU_SAR.1 provides the Primary Directory Administrator and the Local Administrative Group Members with the capability to read all the audit information generated by the audit function. FAU_SAR.2 is preventing all other users from accessing the audit records. FAU_STG.1 is preventing the deletion of audit records, which is provided by FAU_GEN.1 by any other user than the Primary Directory Administrator and Local Administrative Group Members with the Audit Administrator administrative role.

The requirements for access control is defined by the discretionary access control policy in FDP_ACC.2, providing complete access control based on the Entry Owner information and the Access Control Information and according to the evaluation order defined in FDP_ACF.1.

The requirements for identification and authentication are addressed by FIA_AFL.1a, FIA_AFL.1b, FIA_ATD.1, FIA_SOS.1a, FIA_SOS.1b, FIA_UAU.1 and FIA_UID.1. The timing of identification and authentication is specified by FIA_UID.1 and FIA_UAU.1. Authentication failures are handled by FIA_AFL.1a and FIA_AFL.1b, by detecting and suspending users or prohibit further login after a certain number of failed consecutive login attempts. The attributes, including passwords, associated with individual users are specified in FIA_ATD.1. Restrictions on the passwords used for user authentication is specified by FIA_SOS.1a and FIA_SOS.1b, preventing the user and administrator to select weak or easy to guess passwords.

The management functions are specified by FMT_SMF.1, specifying management functions for password management, password policy management, user management, access control management and audit management. The roles identified by the TOE are specified in FMT_SMR.1.

The management of the authentication function is described in FMT_MOF.1a and the management of passwords, password policy, entry owner information and access control information and audit options is covered by FMT_MOF.1b. These management functions are also restricted to specific identified, authenticated and authorized users. For the discretionary access control, restricted attributes are specified by FMT_MSA.3. Also for discretionary access control, the use of only secure values for Encryption Information is specified by FMT_MSA.2. The management of TSF data is authorized users as specified in FMT_MTD.1. Note that management of the replication behavior is controlled by F.ACCESS_CONTROL. This relationship is done by a dependency between FMT and FDP, instead as over FMT to F_ACCESS_CONTROL.

FPT_RVM.1 defines that the TSP enforcement functions are invoked and succeed before any other function is allowed to proceed, preventing bypassability of the TSP.

The ability of the TOE security functions to fulfill the security functional requirements is demonstrated by the internal consistency of the security functional requirements, shown in section 8.2.3, and by the demonstration that each of these security requirements are being satisfied with one or more TOE security functions in combination as explained above.

8.3.2 Minimum Strength of Function Level rationale

The TOE mechanisms will resist technical attacks by unauthorized users. The TOE mechanisms will also resist user errors, system errors, or non-malicious actions by authorized users. Resistance to sophisticated types of attacks, when such resistance is required, is provided by the TOE operational environment. The environment also assumes that those individuals who have authorized physical access to the TOE are trusted to not behave maliciously.

Consequently, a level of strength of function medium (**SOF-medium**) which indicates that a function provides adequate protection against straightforward or intentional breach of TOE

security by attackers possessing a moderate attack potential is consistent with the security objectives of the TOE. This claim applies to identification and authentication as specified in FIA_SOS.1a and FIA_SOS.1b, using the described settings, and satisfied by F.I&A.

8.4 Assurance measures rationale

This section is to show that the identified assurance measures are appropriate to meet the assurance requirements by providing mapping between the identified assurance measures and the assurance requirements, as shown in Table 9.

In this case, the specification of assurance measures is done by reference to the appropriate document (e.g., Configuration Management Plan, System Architecture, User Guide, etc.). Rationale is provided to show that the referenced document (assurance measure) meets the requirements of the associated assurance requirement.

Table 9: Mapping of Assurance Measures to Assurance Requirements

	ACM_AUT.1	ACM_CAP.4	ACM_SCP.2	ADO_DEL.2	ADO_IGS.1	ADV_FSP.2	ADV.HLD.2	ADV_IMP.1	ADV_LLD.1	ADV_RCR.1	AGD_SPM.1	AGD_ADM.1	AGD_USR.1	ALC_DVS.1	ALC_FLR.1	ALC_LCD.1	ALC_TAT.1	ATE_COV.2	ATE_DPT.1	ATE_FUN.1	ATE_IND.2	AVA_MSU.1	AVA_SOF.1	AVA_VLA.1
M.AUT	X																							
M.CAP		X																						
M.SCP			X																					
M.DEL				X																				
M.IGS					X																			
M.FSP						X																		
M.HLD							X																	
M.IMP								X																
M.LLD									X															
M.RCR										X														
M.SPM											X													
M.ADM												X												
M.USR													X											
M.DVS														X										
M.FLR															X									
M.LCD																X								
M.TAT																	X							
M.COV																		X	X					
M.FUN																				X				
M.IND																					X			
M.SOF																							X	
M.VLA																						X	X	X