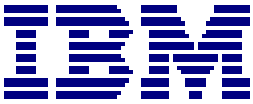

IBM Tivoli Directory Server Version 6.3 Fix Pack 10 Security Target

Version:	**1.12**
Status:	**Released**
Last Update:	**2013-02-25**

Trademarks

IBM and the IBM logo are trademarks or registered trademarks of IBM Corporation in the United States, other countries, or both.

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
1.12	2013-02-25	Scott Chapman, King Ables	Updated from TDS 6.2 to TDS 6.3 FP10.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	IBM Tivoli Directory Server Version 6.3 Fix Pack 10 Security Target
Version:	1.12
Status:	Released
Date:	2013-02-25
Sponsor:	International Business Machines, Corporation
Developer:	International Business Machines, Corporation
Certification Body:	BSI
Certification ID:	BSI-DSZ-CC-0806
Keywords:	Lightweight Directory Access Protocol (LDAP), Access Control List (ACL), Password Policy (PP), Audit Service (AS), IBM Tivoli Directory Server (TDS)

1.2 TOE Identification

The TOE is IBM Tivoli Directory Server Version 6.3 Fix Pack 10 (6.3.0.10-TIV-ITDS).

1.3 TOE Type

The TOE type is a Lightweight Directory Access Protocol (LDAP) server.

1.4 TOE Overview

The IBM Tivoli Directory Server (TDS) is an implementation of Lightweight Directory Access Protocol (LDAP), which is compliant with the Internet Engineering Task Force (IETF) LDAP Version 2 specifications, i.e. [RFC1777] and LDAP Version 3 specifications, i.e. [RFC2251], [RFC2252], [RFC2253], [RFC2254], [RFC2255], [RFC2256]. TDS is a software only product and can be installed and operated on variety of hardware/software platforms.

An LDAP server is a specialized database where the update operations are expected to be less frequent than for a relational database. An LDAP server within an enterprise is often dedicated to the common goal of consolidating and unifying the management of identities. TDS is built for identity management with role support, fine-grained access control, and entry ownership. It provides the foundation for improved security along with rapid development and deployment of Web applications. Using the power of the IBM DB2 Universal Database as a backend data store, the TOE provides high performance, reliability, and stability in an enterprise or e-business. As the central repository for data within an enterprise, it is a powerful, secure, and standards compliant enterprise directory for corporate intranets.

1.4.1 Required non-TOE software

The TOE requires an operating system. The operating system is part of the Operational Environment. The following operating systems may be used with the TOE in the evaluated configuration:

- Microsoft Windows Server 2008 Enterprise Edition (32-bit)
- Microsoft Windows Server 2008 R2 Enterprise Edition (AMD64/EM64T 64-bit)
- IBM AIX 7.1

- Sun Solaris 10 (SPARC)
- Red Hat Advanced Server 6 (AMD64/EM64T 64-bit)
- SuSE Linux Enterprise Server 11 (AMD64/EM64T 64-bit)

The TOE requires the use of a relational database as a backend data store. The relational database is part of the Operational Environment. The following relational database(s) may be used with the TOE in the evaluated configuration:

- IBM DB2 Universal Database

The TOE requires the use of the IBM Global Security Kit (GSKit) library for cryptographic-related functions. GSKit is part of the Operational Environment. IBM TDS v6.3 Fix Pack 10 requires the use of GSKit version 8.0.14.14.

1.4.2 Intended method of use

The TOE is intended to be used in a distributed, non-hostile environment with a well-managed user community. The TOE uses the network security protocols Transport Layer Security (TLS) ([RFC2246] and [RFC2830]) and Secure Sockets Layer ([RFC6101]) to protect network data between clients and the TOE from disclosure and modification when communicating. These network security protocols are provided by the Operational Environment, not by the TOE.

1.4.3 Major security features

The major security features of the TOE are:

- **Auditing** - Generation, review, and storage of audit events.
- **Access control** - Access Control Lists (ACLs) for TOE objects.
- **Identification and authentication (I&A)** - The I&A of users when accessing non-public data.
- **Security management** - Role-based management of the TOE's security features.

1.5 TOE Description

The TOE is an implementation of the Lightweight Directory Access Protocol (LDAP) and meets the requirements of LDAP Version 3 and LDAP Version 2 as defined in section 1.4. The TOE consists of the following major software components:

- LDAP Server
- Administration Server

The LDAP Server provides the general LDAP interface that LDAP Clients use to access data within the directory. The Administration Server provides a more restrictive LDAP interface than the LDAP Server and is used for administrative clients to manage the LDAP Server, such as for starting and stopping the LDAP Server. The combination of the two components is oftentimes referred to as a directory server in this document.

The following sections provide more detail on both the LDAP Server and the Administration Server.

1.5.1 LDAP Server

The LDAP Server, which is the core component of the two, may be viewed as 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 IBM DB2 database.

The LDAP Server supports the standard LDAP operations:

- Bind (connect) to the directory.
- Unbind (disconnect) from the directory.
- 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 LDAP Server may allow unauthenticated users to perform any operation on any entries or attributes that are not blocked by any ACL (i.e., public data). 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.

1.5.1.1 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 directory 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 directory 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) directory server. When information is replicated, more than one directory server stores the same directory entry. In a distributed directory, some information may be partitioned, and some information may be replicated.

1.5.1.2 LDAP Clients and directory servers

Directories are usually accessed using the client-server model of communication. The LDAP Client and LDAP Server processes might or might not be on the same machine. A directory server is capable of serving many LDAP 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 directory server is shown in the picture below.

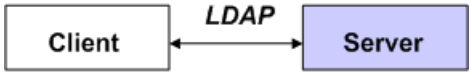

Figure 1: Configuration showing a client and a single directory server

An API defines the programming interface a particular programming language uses to access a service. The format and contents of the messages exchanged between a LDAP client and directory server must adhere to an agreed upon protocol. LDAP defines a message protocol used by LDAP 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).

1.5.2 Administration Server

The Administration Server is used to manage the LDAP Server. Like the LDAP Server, the Administration Server is a standalone daemon process. Administrative users use the Administration Server to perform functions such as to start and stop the LDAP Server.

The Administration Server supports a subset of the LDAP operations. Specifically, it supports the following LDAP operations:

- Bind
- Unbind
- Search
- Extended operations

Administrative users communicate with the Administration Server using this subset of LDAP operations, but over different network ports than the LDAP Server.

The Administration Server identifies and authenticates administrative users using the bind operation. Only the following security roles can bind to the Administration Server:

- Primary Directory Administrator
- Administrative Group Members

Users with these security roles are defined and maintained in the configuration file which is shared with the LDAP Server. The Administration Server does not have access to the LDAP Server's database.

The Administrative Server also includes the following security functions:

- Enforces the same administrative password policy as the LDAP Server
- Generates audit records for its supported LDAP operations
- Supports audit log review
- Enforces the same access control policy as the LDAP Server

1.5.3 Security features

1.5.3.1 Auditing

The TOE generates audit records for all supported LDAP operations and extended operations except for the LDAP abandon operation. The Administration Server and LDAP Server store their audit records in separate audit logs. The TOE also provides the capability for authorized administrators to review the audit logs through the use of LDAP extended operations. The TOE only allows authorized administrators to clear (delete all audit records in) the audit logs.

1.5.3.2 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 database backend. 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, 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 Administrative Group Members. These administrators will be granted proxied authorization rights by default, without explicitly being a member of a proxied authorization group.

Two LDAP controls implement proxied authorization:

- 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 Administrative Group Members may use this control to assume an LDAP User or Global Administrative Group Members 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.

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 and SHA-2 algorithms 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 is used in the encryption of the LDAP entry in order to thwart simple dictionary attacks. The

unencrypted value is not stored by the directory 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 Administrative Group Members with the Schema Administrator administrative role (administrative roles are described in section 7.1.4) can specify which LDAP entries are to be encrypted. (The SHA-1 and SHA-2 algorithms and the random number generation for the salt values are provided by the Operational Environment.)

1.5.3.3 Identification and authentication (I&A)

Users are required to identify and authenticate themselves to the TOE prior to accessing information within the TOE, except when the TOE publishes selected entries as public data. The TOE uses the bind operation to identify and authenticate a user. The bind operation requires the user to supply a Distinguished Name (DN) and password which the TOE uses to verify the validity of the user. The DN and password are part of the user's account data.

The TOE supports the following password policies:

- Administrative password policy
- Global password policy

These password policies allow an authorized administrator to control the password complexity rules of all user passwords. The global password policy also controls the expiry of the passwords associated with the policy. The user's security role determines which policy is enforced by the TOE on the user. These password policies and their security attributes are described in section 7.1.3.

The TOE tracks the number of failed login attempts on a per user basis. The user security attributes used to track failed login attempts are described in section 7.1.3 and are part of the user's account data.

The TOE supports the following authentication methods:

- LDAP Server:
  - Simple Bind
  - Simple Authentication and Security Layer (SASL) using the DIGEST-MD5 SASL authentication mechanism provided by GSKit (GSKit is in the operational environment)
- Administration Server:
  - Simple Bind

The SASL method ([RFC2222]) provides a plug-in facility which allows different authentication mechanisms to be used.

If the TOE is configured to support public data, then users can connect as an anonymous or unauthenticated user to the LDAP Server in order to access the public data.

1.5.3.4 Security management

1.5.3.4.1 Security roles

The TOE supports the following security roles:

- Primary Directory Administrator
- Administrative Group Members

- Global Administrative Group Members
- Master Server DN
- LDAP User

Descriptions of each security role are located in section 7.1.4.1.1.

A user account for the TOE operates as one, and only one of these roles. Only by having different accounts can a user act in different security roles, except for the case where administrators can use the Proxy Authorization feature to act as an LDAP User.

In addition, Administrative Group Members have an administrative roles attribute which further sub-divides the Administrative Group Members capabilities; thus, there's a distinction between security roles and administrative roles in this document. Accounts with the Administrative Group Members security role may have one or more of the following administrative roles assigned to them:

- Audit Administrator
- Directory Data Administrator
- No Administrator
- Password Administrator
- Replication Administrator
- Schema Administrator
- Server Configuration Group Member
- Server Start/Stop Administrator

Descriptions of each administrative role are located in section 7.1.4.1.2.

Note: *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.*

1.5.3.4.2 Audit management

The TOE allows authorized administrators to manage the audit configuration data. The audit configuration data and the authorized administrators are specified in section 7.1.4.2.

1.5.3.4.3 Access control management

The TOE allows administrators and non-administrators to perform access control management on directory objects owned by a user or allowed by the user's security role. This includes modifying the ACL and Encryption Information of a directory object as well as the security configuration data in the schema file. In some cases, the access control of certain security configuration-related directory objects, such as the audit configuration data, is hard coded in the TOE and cannot be changed, but in general users can control who can access their directory objects through the use of access control lists (ACLs). (Some system directory objects do not allow modification by any user.) For more information, see section 7.1.4.3.

1.5.3.4.4 I&A management

The TOE allows authorized administrators to perform the following I&A management functions:

- Authentication mechanism selection
- Manage the administrative roles assigned to a user's account
- Password management
- Password policy management

1.5.4 Security policy data

1.5.4.1 Subjects and objects

The following subject and object definitions are used in the TOE security policies:

Subjects:

- **Users** - Users include both administrative and non-administrative users that connect to the TOE using an LDAP client

Objects:

- **Entries** - Directory entries

1.5.4.2 TSF data and security attributes

The following TOE Security Functionality (TSF) data and security attributes are maintained by the TOE:

- Audit records
- Directory entry security attributes:
  - Entry Owner Information (EOI)
  - Access Control Information (ACI)
  - Encryption Information
- Schema file security configuration data
- User account data:
  - Administrative roles
  - Distinguished Name (DN)
  - Failed login attempts data
  - Password
  - Password changed time
  - Security role

1.5.4.3 User data

The following user data are maintained by the TOE:

- User data contained in a directory entry created by the user.

1.5.5 Physical boundary

TDS is a software-only product with guidance documentation. There is also a secure configuration guide that must be downloaded and used for the installation and management of the TOE. The TOE is delivered over the Internet in the form of multiple eAssembly packages, one eAssembly package per operating system type. The eAssembly packages (with their eAssembly Part Numbers in braces) included in the evaluated configuration are:

- IBM Tivoli Directory Server v6.3 for AIX {CRC8DML}
- IBM Tivoli Directory Server v6.3 for Linux x86-64 (64 bit) {CRC8HML}
- IBM Tivoli Directory Server v6.3 for Solaris SPARC {CRC8IML}
- IBM Tivoli Directory Server v6.3 for Windows (32-bit) {CRC8JML}
- IBM Tivoli Directory Server v6.3 for Windows (64-bit) {CRC8NML}

In addition, the following fix pack must be downloaded and installed:

- IBM Tivoli Directory Server v6.3 Fix Pack 10

The Operational Environment 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 and the Adobe Acrobat Reader to access the supplied online documentation.

1.5.6 Logical boundary

The TOE is illustrated in Figure 2, showing the basic client/server based TDS architecture. The rectangle represented by the dashed lines indicates the TOE boundary, i.e. the standalone LDAP Server with the Administration Server. Those, out of the scope of evaluation, are listed as below:

- The underlying hardware and operating system of the TOE
- The database, which serves as the backend data store of the directory
- The LDAP Client
- The TLS/SSL module (IBM Global Security Kit (GSKit)), which provides:
    - Protected communication between an LDAP Client and TOE
    - Protected communication among replication servers
    - Encryption/hash and random number generation support for salted SHA-1 and salted SHA-2 encryption of LDAP entries
    - Encryption/hash generation support for MD5 for the DIGEST-MD5 SASL authentication mechanism.
    - Authentication using X.509v3 public-key certificates.

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

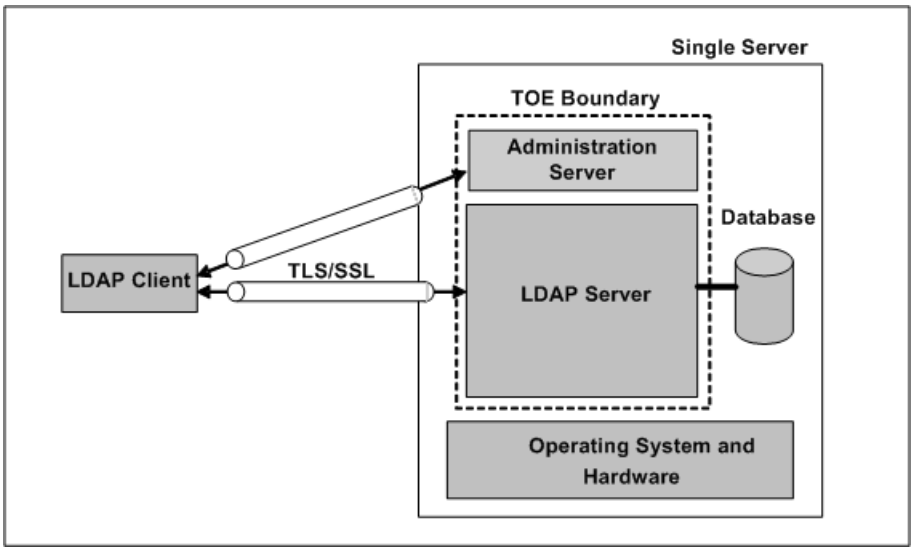

Figure 2: TOE architecture and TOE boundary

Figure 2 provides a high-level overview of the components showing that the LDAP Server and Administration Server are inside the TOE boundary and the remaining components are outside the TOE boundary. It shows that the Administration Server, LDAP Server, Database, and Operating System reside on a Single Server. It also shows that the LDAP Clients exist on systems other than the system containing the TOE.

The figure shows that the LDAP Clients can communicate to both the LDAP Server and the Administration Server through TLS/SSL connections. It also shows that the LDAP 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 or to the Administration Server, using the LDAP protocol but using different port numbers. The LDAP Server provides the LDAP functionality to all of the security roles:

- Primary Directory Administrator
- Administrative Group Members
- Global Administrative Group Members
- Master Server DN
- LDAP User

while the Administration Server is only used by the following security roles:

- Primary Directory Administrator
- Administrative Group Members

(administrative roles are described in section 7.1.4.1.2) for the primary purpose of starting, stopping and querying the status of the TOE. Figure 2 shows the simplest configuration of the TOE as a single 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. This is a one-way information path, the peer does not send updates to the master. The environment must only contact the master, not the peer, to submit updates. The normal operation is shown in Figure 3.

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 Server, LDAP 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. This interaction between the servers is technically the same as the interaction between an LDAP client and server.

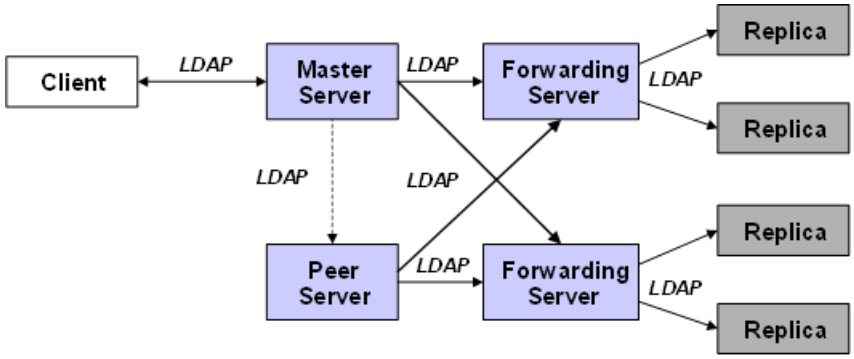

Figure 3: Configuration using multiple servers

The TOE contains the following security features which are described in more detail in section 1.5.3:

- Auditing
- Access control
- Identification and authentication
- Security management

The hardware, operating system, and database that the TOE uses are part of the Operational Environment. The TOE assumes a secured communication link between itself and the LDAP Client.

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

1.5.7 Evaluated configuration

The following features are not supported in the evaluated configuration:

- 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 directory servers, but also a flat tree may be distributed over multiple directory servers. An LDAP request from an LDAP Client is coming in to an directory server, the directory server will then reply to the request either with the result or with a referral to the directory servers that may be able to provide the result. This means that

the client will have to issue the request to the directory server referred to. How this is performed is based on the entry affected by the request and referrals defining the partitioning of the Directory Information Tree (DIT). Distributed directory is not part of the evaluated configuration.

- 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 Administrative Group Members with the Server Configuration Group Member administrative role can enable/disable this feature. This feature must be disabled in the evaluated configuration.
- 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 Administrative Group Members with the Server Configuration Group Member administrative role can enable/disable this feature. This feature must be disabled in the evaluated configuration.
- 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.
- 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.
- PTA - Pass-through authentication (PTA) is not part of the evaluated configuration.
- High availability - The high availability feature of TDS is not part of the evaluated configuration.
- Dynamic tracing - A dynamic tracing facility is provided, which can be activated and deactivated by the Primary Directory Administrator and Administrative Group Members using extended operations. The dynamic tracing facility must not be activated as part of the evaluated configuration of the TOE.

The following features are supported in the evaluated configuration with some restrictions:

- Audit - Version 3, the default audit log format, is the only version supported by the TOE. Versions 1 and 2 are old and are provided only for backward compatibility with applications that parse audit log records.
- Replication - Replication makes additional read-only copies of the directory available, improving performance and reliability of the directory service. See the replication restrictions in the next list. 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 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. Additionally, replication of user security attributes is not allowed in the evaluated configuration.
- 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.

1.5.8 Operational Environment

The Operational Environment is defined in section 1.4.1.

Restrictions on the Operational Environment include:

- AIX WPAR - On AIX systems, workload partitions (WPAR) such as System WPAR and Application WPAR must not be configured.
- Solaris Zones - On Solaris SPARC systems, zones such as Small zone (also known as Sparse Root zone) and Big zone (also known as Whole Root zone) must not be configured.

2 CC Conformance Claim

This Security Target is CC Part 2 conformant and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL4, augmented by ALC_FLR.1.

This Security Target does not claim conformance to any Protection Profile.

Common Criteria [CC] version 3.1 revision 3 is the basis for this conformance claim.

3 Security Problem Definition

3.1 Threat Environment

The threats are categorized as those addressed by the TOE and those addressed by the Operational 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 protects against straightforward or intentional breach of TOE security by attackers possessing an Enhanced-Basic attack potential as defined by the [CEM].

3.1.1 Threats countered 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.ENTRY

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

3.1.2 Threats countered by the Operational Environment

TE.BYPASS

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

3.2 Assumptions

3.2.1 Intended usage of the TOE

A.ADMIN

The TOE Administrators (i.e. the Primary Directory Administrator, the 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.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.ENCRYPT

It is assumed that the Operational Environment provides one-way encryption and random number generation functions for the TOE through the use of GSKit.

A.PHYSICAL

The TOE is operated in a physically secure 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 Operational Environment is as for the TOE (master server).

A.TIME

It is assumed that a reliable time function is provided by the Operational Environment to support the generation of audit records.

A.TOEENV

The Operational Environment administrators are trustworthy to perform discretionary actions in accordance with security policies, assuring that the Operational Environment is competently installed and administered.

3.3 Organizational Security Policies

P.ACCOUNT

The users of the TOE shall be held accountable for their security-relevant actions within the TOE.

P.ENCRYPT

Sensitive data may be stored one-way encrypted to prevent direct observation. Administrators determine which entries will be encrypted.

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.

4 Security Objectives

4.1 Objectives for the TOE

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 the TOE.

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, 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.

4.2 Objectives for the Operational Environment

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.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.ENCRYPT

The Operational Environment must provide functions for support of one-way encryption of sensitive data and random number generation to the TOE.

OE.ENVMANAGE

Those responsible for the Operational Environment must ensure that the underlying operating system and hardware are configured and managed in a secure way.

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.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.ROUTE

The Operational Environment must ensure that in a replicated environment all the update requests are made to the master server only. It must also ensure that all replicas are under the same administration and have the same protection as is required for the TOE (master server).

OE.TIME

The Operational Environment must provide a reliable time source.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.ACCOUNT	P.ACCOUNT
O.AUTHENTICATE	T.ACCESS T.ENTRY P.ACCOUNT
O.AUTHORIZE	T.ACCESS P.ENCRYPT P.PUBLIC

Table 1: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.COMMUNICATION	A.COMM T.ACCESS
OE.DATABASE	A.ADMIN A.TOEENV T.ACCESS TE.BYPASS
OE.ENCRYPT	A.ENCRYPT

Objective	Assumptions / Threats / OSPs
OE.ENVMANAGE	A.ADMIN A.TOEENV TE.BYPASS
OE.MANAGE	A.ADMIN A.COOP A.TOEENV
OE.PHYSICAL	A.PHYSICAL TE.BYPASS
OE.ROUTE	A.ROUTE
OE.TIME	A.TIME

Table 2: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T.ACCESS	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. 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 Operational Environment and are addressed by the objectives OE.DATABASE and OE.COMMUNICATION.
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.

Threat	Rationale for security objectives
TE.BYPASS	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.

Table 3: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	Rationale for security objectives
A.ADMIN	OE.MANAGE, OE.ENVMANAGE and OE.DATABASE require that TOE and the Operational Environment are managed and administered in a secure manner. Assuming that the administrators should be trusted to perform discretionary actions in accordance with security policies.
A.COMM	OE.COMMUNICATION requires that communication links between the TOE and LDAP clients on external systems are protected against unauthorized modification and disclosure of communication data.
A.COOP	OE.MANAGE requires that the TOE is managed in a secure manner 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.ENCRYPT	OE.ENCRYPT requires that the Operational Environment provides one or more encryption algorithms and random number generation functions through the use of GSKit.
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.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 the same protection as required by the TOE (master server).
A.TIME	OE.TIME requires that the Operational Environment provides a reliable time function.

Assumption	Rationale for security objectives
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 Operational Environment are competently installed and administered.

Table 4: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy, that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented:

OSP	Rationale for security objectives
P.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.
P.ENCRYPT	O.AUTHORIZE requires that the TOE provides the ability to encrypt sensitive data in order to prevent direct observance of that data.
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.

Table 5: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

This Security Target does not extend the security components provided by the Common Criteria.

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the Security functional requirements for the TOE, and the operations performed on the components according to CC part 2: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association		CC Part 2	No	No	No	No
	FAU_SAR.1 Audit review		CC Part 2	No	No	Yes	No
	FAU_SAR.2 Restricted audit review		CC Part 2	No	Yes	No	No
	FAU_STG.1 Protected audit trail storage		CC Part 2	No	No	No	Yes
FDP - User data protection	FDP_ACC.2 Complete access control		CC Part 2	No	No	Yes	No
	FDP_ACF.1 Security attribute based access control		CC Part 2	No	Yes	Yes	No
FIA - Identification and authentication	FIA_AFL.1-admin Authentication failure handling	FIA_AFL.1	CC Part 2	Yes	No	Yes	Yes
	FIA_AFL.1-user Authentication failure handling	FIA_AFL.1	CC Part 2	Yes	No	Yes	Yes
	FIA_ATD.1 User attribute definition		CC Part 2	No	No	Yes	No
	FIA_SOS.1-admin Verification of secrets	FIA_SOS.1	CC Part 2	Yes	Yes	Yes	No
	FIA_SOS.1-user Verification of secrets	FIA_SOS.1	CC Part 2	Yes	Yes	Yes	No
	FIA_UAU.1 Timing of authentication		CC Part 2	No	No	Yes	No
	FIA_UID.1 Timing of identification		CC Part 2	No	No	Yes	No
FMT - Security management	FMT_MOF.1-audit Management of security functions behaviour	FMT_MOF.1	CC Part 2	Yes	Yes	Yes	Yes
	FMT_MOF.1-auth Management of security functions behaviour	FMT_MOF.1	CC Part 2	Yes	Yes	Yes	Yes
	FMT_MSA.1 Management of security attributes		CC Part 2	No	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FMT_MSA.2 Secure security attributes		CC Part 2	No	No	Yes	No
	FMT_MSA.3 Static attribute initialisation		CC Part 2	No	No	Yes	Yes
	FMT_MTD.1 Management of TSF data		CC Part 2	No	No	Yes	Yes
	FMT_SMF.1 Specification of Management Functions		CC Part 2	No	No	Yes	No
	FMT_SMR.1 Security roles		CC Part 2	No	Yes	Yes	No

Table 6: Security functional requirements for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

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) **The following events:**

- **LDAP Server:**
  - **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)**
  - **Compare (LDAP v2 and v3)**
  - **Event notification (LDAP v3)**
  - **Extended operations (LDAP v3)**
- **Administration Server:**
  - **Bind (LDAP v2 and v3)**
  - **Unbind (LDAP v2 and v3)**
  - **Search (LDAP v2 and v3)**
  - **Extended operations (LDAP v3).**

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 (if applicable), 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 PP/ST, **none**.

Application Note: *The subject identity for 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.*

6.1.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, 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.*

6.1.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **the following security roles**

- **Primary Directory Administrator**
- **Administrative Group Members with the Audit Administrator administrative role**
- **Administrative Group Members with the Server Configuration Group Member administrative role**

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.

6.1.1.4 Restricted audit review (FAU_SAR.2)

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~~ *for the following security roles:*

- *Primary Directory Administrator*
- *Administrative Group Members with the Audit Administrator administrative role*
- *Administrative Group Members with the Server Configuration Group Member administrative role.*

6.1.1.5 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

6.1.2 User data protection (FDP)

6.1.2.1 Complete access control (FDP_ACC.2)

SFP_ACL		
Type	**Short name**	**Definition**
Subjects	S_User	All users that can access the TOE including authenticated and unauthenticated/anonymous users.
Objects	O_Entry	All directory entries maintained in the database backend.
Operations	Add	Add
	Compare	Compare
	Delete	Delete
	Read	Read
	Search	Search
	Write	Write
Subject Security Attributes	AS_DN	Distinguished Name (DN) of the subject.
Object Security Attributes	AO_EOI	Entry Owner Information (EOI): ● entryOwner: defines the entry owner. ● ownerPropagate: indicates whether to propagate the ownership of the entry to all descendant entries.
	AO_ACI	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.
	AO_Encrypt	Encryption Information: ● ENCRYPT: defines the encryption type if the value is encrypted. Supported encryption types are: ○ salted SHA-1

SFP_ACL		
Type	**Short name**	**Definition**
		○ salted SHA-224 ○ salted SHA-256 ○ salted SHA-384 ○ salted SHA-512
Rules	R_Step1	By comparing the subject's DN with the effective entryOwner attribute values. The entry owner has full access to the target entry.
	R_Step2	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: 1. 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. 2. 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.
	R_Step3	If no ACI information is found for the target object (either explicitly or through inheritance), then default access is given.
	R_Owners	The following security roles are always owners (entryOwner) of all directory objects: ● Primary Directory Administrator ● Administrative Group Members with the Directory Data Administrator administrative role ● Global Administrative Group Members
	R_Public	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.*
	R_Encrypted	If an object is one-way encrypted by the TOE, an operation on the object will not return the unencrypted value of the object.

Table 7: Access control SFP SFP_ACL

FDP_ACC.2.1 The TSF shall enforce the **SFP_ACL** on **all subjects and objects as defined in SFP_ACL** 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 controlled by the TSF and any object controlled by the TSF 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.*

6.1.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the **SFP_ACL** to objects based on the following: **all subjects and objects together with their respective security attributes as defined in SFP_ACL**.

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

1. **R_Step1**
2. **R_Step2**
3. **R_Step3.**

Application Note: *For proxied authorization, the user assumes the proxied identity and the ACL restrictions for the proxied identity.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules *as defined in SFP_ACL*:

- **R_Owners**
- **R_Public.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules *as defined in SFP_ACL*:

- **R_Encrypted.**

6.1.3 Identification and authentication (FIA)

6.1.3.1 Authentication failure handling (FIA_AFL.1-admin)

FIA_AFL.1.1 The TSF shall detect when **3** unsuccessful authentication attempts occur related to **consecutive unsuccessful authentication attempts by the same Administrator (i.e., the Primary Directory Administrator, Administrative Group Members, Master Server DN)**.

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 TOE is running; noting that after a successful local login (only possible for the Primary Directory Administrator) or a restart of the LDAP Server, the Administrator's account is restored to normal access**.

Application Note:

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

6.1.3.2 Authentication failure handling (FIA_AFL.1-user)

FIA_AFL.1.1 The TSF shall detect when **3** unsuccessful authentication attempts occur related to **consecutive unsuccessful authentication attempts of the same End User (i.e., Global Administrative Group Members, LDAP 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 the Primary Directory Administrator or Administrative Group Members with the Password Administrator administrative role resets that End User's password**.

6.1.3.3 User attribute definition (FIA_ATD.1)

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

- **Administrative roles**
- **Distinguished Name (DN)**
- **Failed login attempts data:**
  - **pwdAccountLockedTime - the time that the user's account was locked**
  - **pwdFailureTime - the times of the consecutive authentication failures**
  - **pwdReset - a flag to indicate whether or not the user password has been reset and, therefore, must be changed by the user on next authentication**
- **Password**
- **pwdChangedTime - the last time the user's password was changed**
- **Security role - one of the roles defined in FMT_SMR.1.**

6.1.3.4 Verification of secrets (FIA_SOS.1-admin)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets *for the security roles*

- *Primary Directory Administrator*
- *Administrative Group Members*
- *Master Server DN*

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.**

6.1.3.5 Verification of secrets (FIA_SOS.1-user)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets *for the security roles*

- *Global Administrative Group Members*
- *LDAP User*

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.**

6.1.3.6 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow **limited operations as assigned by authorized administrators (i.e., the Primary Directory Administrator and the Administrative Group Members with the Server Configuration Group Member administrative role) 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.

6.1.3.7 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow **limited operations as assigned by authorized administrators (i.e., the Primary Directory Administrator and the Administrative Group Members with the Server Configuration Group Member administrative role) 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.

6.1.4 Security management (FMT)

6.1.4.1 Management of security functions behaviour (FMT_MOF.1-audit)

Security feature	Operations	Security function	Authorized security roles
Audit management	enable, disable	Auditing	• Primary Directory Administrator • Administrative Group Members with the Audit Administrator administrative role
	modify the behaviour of	Audit logging (by specifying an audit log file name and the audit version -- version	

Security feature	Operations	Security function	Authorized security roles
		3 must be used in the evaluated configuration)	
	modify the behaviour of	Event auditing (by selecting the event types and event outcome types to be audited)	

Table 8: Management of auditing security function behavior

FMT_MOF.1.1 The TSF shall restrict the ability to **disable, enable, modify the behavior of** *(as specified in Table 8)* the functions **in Table 8** to **the security roles in Table 8**.

6.1.4.2 Management of security functions behaviour (FMT_MOF.1-auth)

Security feature	Operations	Security function	Authorized security roles
I&A management	modify the behaviour of	LDAP Server authentication mechanism (by selecting either Simple Bind or SASL)	• Primary Directory Administrator • Administrative Group Members with the Directory Data Administrator administrative role • Global Administrative Group Members • Master Server DN
	modify the behaviour of	Administrative password policy function	• Primary Directory Administrator
	modify the behaviour of	Global password policy function	• Primary Directory Administrator • Administrative Group Members with the Directory Data Administrator administrative role • Global Administrative Group Members • Master Server DN

Table 9: Management of authentication security function behavior

FMT_MOF.1.1 The TSF shall restrict the ability to **modify the behavior of** *(as specified in Table 9)* the functions **in Table 9** to **the security roles in Table 9**.

6.1.4.3 Management of security attributes (FMT_MSA.1)

Security attributes	Operations	Authorized users and/or security roles
Entry Owner Information	read, modify, delete	• Primary Directory Administrator • Administrative Group Members with the Directory Data Administrator administrative role • Global Administrative Group Members • LDAP User (entry owner)
Access Control Information	read, modify, delete	• Primary Directory Administrator • Administrative Group Members with the Directory Data Administrator administrative role • Global Administrative Group Members • LDAP User (entry owner)
Encryption Information	read, modify	• Primary Directory Administrator • Administrative Group Members with the with Schema Administrator administrative role

Table 10: SFP_ACL security attribute management

FMT_MSA.1.1 The TSF shall enforce the **SFP_ACL** to restrict the ability to **perform the operations in Table 10 on** the security attributes **in Table 10** to **the authorized users and/or security roles in Table 10**.

6.1.4.4 Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for **the Encryption Information security attribute as defined in SFP_ACL**.

6.1.4.5 Static attribute initialisation (FMT_MSA.3)

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

FMT_MSA.3.2 The TSF shall allow the **following security roles**

- **Primary Directory Administrator**
- **Administrative Group Members**
- **Global Administrative Group Members**
- **Master Server DN**
- **authorized LDAP User**

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 an account with the Administrative Group Members security role to perform these actions depends on the administrative roles assigned to the account.*

6.1.4.6 Management of TSF data (FMT_MTD.1)

TSF data	Operations	Authorized user or security roles
Administrative roles	modify	• Primary Directory Administrator
Password of an account that has the LDAP User security role	modify	• Primary Directory Administrator • Administrative Group Members with the Directory Data Administrator administrative role • Administrative Group Members with the Password Administrator administrative role • Global Administrative Group Members • Self (account owner)
Schema file security configuration data	modify	• Primary Directory Administrator • Administrative Group Members with the Schema Administrator administrative role

Table 11: TSF data management

FMT_MTD.1.1 The TSF shall restrict the ability to **perform the operations in Table 11 on** the **TSF data in Table 11** to **the security roles in Table 11**.

6.1.4.7 Specification of Management Functions (FMT_SMF.1)

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

- **Access control management**
- **Audit management**
- **Authentication mechanism management**
- **Password policy management**
- **User management.**

6.1.4.8 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the *security* roles

- **Primary Directory Administrator**
- **Administrative Group Members**
- **Global Administrative Group Members**
- **Master Server DN**
- **LDAP User.**

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

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security Functional Requirements	Objectives
FAU_GEN.1	O.ACCOUNT
FAU_GEN.2	O.ACCOUNT
FAU_SAR.1	O.ACCOUNT
FAU_SAR.2	O.ACCOUNT
FAU_STG.1	O.ACCOUNT
FDP_ACC.2	O.AUTHORIZE
FDP_ACF.1	O.AUTHORIZE
FIA_AFL.1-admin	O.AUTHENTICATE
FIA_AFL.1-user	O.AUTHENTICATE
FIA_ATD.1	O.AUTHORIZE
FIA_SOS.1-admin	O.AUTHENTICATE
FIA_SOS.1-user	O.AUTHENTICATE
FIA_UAU.1	O.AUTHENTICATE
FIA_UID.1	O.ACCOUNT, O.AUTHENTICATE
FMT_MOF.1-audit	O.ACCOUNT
FMT_MOF.1-auth	O.AUTHENTICATE, O.AUTHORIZE
FMT_MSA.1	O.AUTHORIZE
FMT_MSA.2	O.AUTHORIZE
FMT_MSA.3	O.AUTHORIZE
FMT_MTD.1	O.AUTHORIZE
FMT_SMF.1	O.ACCOUNT, O.AUTHENTICATE, O.AUTHORIZE

Security Functional Requirements	Objectives
FMT_SMR.1	O.AUTHORIZE

Table 12: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.ACCOUNT	FAU_GEN.1 ensures that audit log of security related activity and events are recorded. FAU_GEN.2 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 Administrative Group Members in accordance to security policy, it doesn't pose threats to the TOE. FAU_SAR.1 provides the Primary Directory Administrator and the Administrative Group Members with the capability to review audit logs. FAU_SAR.2 restricts the read access to the audit log to users of Primary Directory Administrator role and Administrative Group Members. FAU_STG.1 further prevents any other user than the Primary Directory Administrator and Administrative Group Members with the Audit Administrator administrative role from manipulating the audit log and thereby preserves the integrity audit log. FIA_UID.1 provides user identification necessary for accountability. FMT_MOF.1-audit ensures that the behavior of the audit function is managed by the Primary Directory Administrator and 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.AUTHENTICATE	FIA_AFL.1-user for LDAP Users and FIA_AFL.1-admin 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 Administrative Group Members in accordance with security policies, each user is successfully identified before allowing any TSF-mediated actions for that user.

Security objectives	Rationale
	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 Administrative Group Members in accordance to security policies, each user is successfully authenticated before allowing any TSF-mediated actions for that user. FIA_SOS.1-user 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.1-admin ensures that the passwords for administrators are of a certain quality, to prevent easy to guess passwords being used. FMT_MOF.1-auth ensures that the authentication mechanism is managed by the Primary Directory Administrator or 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.1-auth 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 Operational Environment are appropriately set by the TOE to only use secure values. FMT_MSA.3 ensures that TOE access 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 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.

Security objectives	Rationale
	Such security requirements work together to ensure full control and management of user, data, and services, providing authorized user access to resources and functionality.

Table 13: Security objectives for the TOE rationale

6.2.3 Security Requirements Dependency Analysis

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	The TOE does not provide reliable time stamps. Instead, reliable time stamps are provided by the Operational Environment. See OE.TIME.
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	FDP_ACC.2
	FMT_MSA.3	FMT_MSA.3
FIA_AFL.1-admin	FIA_UAU.1	FIA_UAU.1
FIA_AFL.1-user	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	No dependencies.	
FIA_SOS.1-admin	No dependencies.	
FIA_SOS.1-user	No dependencies.	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	No dependencies.	
FMT_MOF.1-audit	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1

Security Functional Requirement	Dependencies	Resolution
FMT_MOF.1-auth	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2
	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies.	
FMT_SMR.1	FIA_UID.1	FIA_UID.1

Table 14: TOE SFR dependency analysis

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 components as specified in [CC] part 3, augmented by ALC_FLR.1.

The following table shows the Security assurance requirements, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3	No	No	No	No
	ADV_FSP.4 Complete functional specification	CC Part 3	No	No	No	No
	ADV_IMP.1 Implementation representation of the TSF	CC Part 3	No	No	No	No
	ADV_TDS.3 Basic modular design	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	CC Part 3	No	No	No	No
	ALC_CMS.4 Problem tracking CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No
	ALC_DVS.1 Identification of security measures	CC Part 3	No	No	No	No
	ALC_FLR.1 Basic flaw remediation	CC Part 3	No	No	No	No
	ALC_LCD.1 Developer defined life-cycle model	CC Part 3	No	No	No	No
	ALC_TAT.1 Well-defined development tools	CC Part 3	No	No	No	No
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_OBJ.2 Security objectives	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.2 Derived security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_COV.2 Analysis of coverage	CC Part 3	No	No	No	No
	ATE_DPT.1 Testing: basic design	CC Part 3	No	No	No	No
	ATE_FUN.1 Functional testing	CC Part 3	No	No	No	No
	ATE_IND.2 Independent testing - sample	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis	CC Part 3	No	No	No	No

Table 15: Security assurance requirements

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen to match an Enhanced-Basic attack potential commensurate with the threat environment that is experienced by typical consumers of the TOE. In addition, the evaluation assurance level has been augmented with ALC_FLR.1 commensurate with the augmented flaw remediation capabilities offered by the developer beyond those required by the evaluation assurance level.

7 TOE Summary Specification

7.1 TOE Security Functionality

The TOE security functions are described in the following subsections.

7.1.1 Auditing

Both the Administration Server and LDAP Server generate audit records, each saving their records in separate audit logs. The audit records are stored as human readable text in the audit logs and can be retrieved for review through the TOE by authorized administrators.

The TOE audits the start-up and shutdown of the audit functions. It also audits the following events:

- LDAP Server:
  - 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)
  - Compare (LDAP v2 and v3)
  - Event notification (LDAP v3)
  - Extended operations (LDAP v3)
- Administration Server:
  - Bind (LDAP v2 and v3)
  - Unbind (LDAP v2 and v3)
  - Search (LDAP v2 and v3)
  - Extended operations (LDAP v3)

Each record contains:

- the date and time represented by a timestamp
- the event type represented by an operation or extended operation
- the subject identity (if applicable) represented by the user's DN, "unauthenticated", or "anonymous"
- the event outcome (success or failure)

The version of the audit function may be selected by an authorized administrator, but version 3 is the default and the only selection allowed in the evaluated configuration. Management of the audit functions is described in section 7.1.4.2.

The TOE prevents unauthorized modification of the audit records by not providing an interface to modify the audit records, except to allow authorized administrators to delete (clear) all audit records from an audit log.

Table 16 maps the audit log functions to security roles.

Audit log function	Security role
Clear audit log records	• Primary Directory Administrator • Administrative Group Members with the Audit Administrator administrative role
Read audit log records	• Primary Directory Administrator • Administrative Group Members with the Audit Administrator administrative role • Administrative Group Members with the Server Configuration Group Member administrative role

Table 16: Mapping of audit log functions to security roles

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.*

Note: *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 Operational Environment). In case the Administration Server or the LDAP Server is not able to write to the audit log (e.g., the device is out of space), an error message will be written in the corresponding error log file. The TOE will continue to operate, but the auditing function will no longer add audit records into the audit log.*

This section maps to the following SFR(s):

- 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

7.1.2 Access control

Permission to perform a particular LDAP operation (such as add, delete, modify, modify the DN, search, compare, and extended operations) 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 an unauthenticated user and an 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, Administrative Group Members, and 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, a user that is 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 Administrative Group Members. The Primary Directory Administrator, 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 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 database backend 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 Entry Owner Information (EOI), specifically in the attribute entryOwner. In addition, each entry has a set of associated Access Control Information (ACI) and Encryption Information. When determining access, the EOI, ACI, and Encryption 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 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. 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.

This section and its subsections map to the following SFR(s):

- FDP_ACC.2 - Complete access control
- FDP_ACF.1 - Security attribute based access control

7.1.2.1 Order of evaluation

When determining 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 following security roles are always the owner of all entries in the directory tree:
    - Primary Directory Administrator
    - Administrative Group Members with the Directory Data Administrator administrative role
    - Global Administrative Group Members
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.

7.1.2.2 Preventing direct viewing of selected information

String and binary LDAP entries may be one-way encrypted using salted SHA-1 and salted SHA-2 to prevent direct viewing of the values. The type of encryption algorithm used to one-way encrypt the entry is stored as the Encryption Information part of the entry. The supported salted algorithms are:

- salted SHA-1
- salted SHA-224
- salted SHA-256
- salted SHA-384
- salted SHA-512

The Primary Directory Administrator and 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 one-way 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.

The GSKit library is used to perform the hash functions such as SHA-224. GSKit is part of the Operational Environment.

7.1.2.3 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

7.1.3 Identification and authentication (I&A)

Users are required to identify and authenticate themselves to the TOE prior to accessing information within the TOE, except when the TOE publishes selected entries as public data. The TOE uses the bind operation to identify and authenticate a user. The bind operation requires the user to supply a Distinguished Name (DN) and password which the TOE uses to verify the validity of the user. The DN and password are part of the user's account data.

If the TOE is configured to support public data, then users can connect as an anonymous or unauthenticated user to the LDAP Server in order to access the public data.

The TOE supports the following authentication methods:

- LDAP Server:
  - Simple Bind
  - Simple Authentication and Security Layer (SASL) using the DIGEST-MD5 SASL authentication mechanism provided by GSKit (GSKit is in the operational environment)
- Administration Server:
  - Simple Bind

The TOE supports the following password policies:

- Administrative password policy
- Global password policy

These password policies allow an authorized administrator to control the password complexity of user passwords. The global password policy also allows an authorized administrator to control the expiry of the security roles associated with this policy. The user's security role determines which policy is enforced by the TOE on the user.

The administrative password policy applies to the following security roles:

- Primary Directory Administrator
- Administrative Group Members
- Master Server DN

The administrative password policy enforces the following password complexity constraints:

- Minimum length of passwords (pwdMinLength) – default for secure configuration is 8
- Minimum number of non-alphabetic characters (passwordMinOtherChars) – default for secure configuration is 2
- Minimum number of alphabetic characters (passwordMinAlphaChars) – default for secure configuration is 4
- Maximum number of repeated/identical characters (passwordMaxRepeatedChars) – default for secure configuration is 2

The global password policy applies to the following security roles:

- Global Administrative Group Members
- LDAP User

Note: *The product supports a combination of the following user password policies, but only the global password policy must be enabled in the evaluated configuration:*

- *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 (disabled in the evaluated configuration).*
- *Individual password policy – An optional password policy assigned to a user (disabled in the evaluated configuration).*

The global password policy enforces the following password complexity constraints and expiry constraints:

- Minimum length of passwords (pwdMinLength) – default for secure configuration is 8
- Minimum number of non-alphabetic characters (passwordMinOtherChars) – default for secure configuration is 2
- Minimum number of alphabetic characters (passwordMinAlphaChars) – default for secure configuration is 4
- Maximum number of repeated/identical characters (passwordMaxRepeatedChars) – 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)

The TOE tracks the number of failed login attempts on a per user basis for all security roles. For users associated with the administrative password policy, the TOE will prohibit further login of that user after an administrator configured 3 attempts from any host other than the one on which the TOE is running; noting that after a successful local login (only possible for the Primary Directory Administrator) or a restart of the LDAP Server, the user's account will be restored to normal access.

For users associated with the global password policy, the TOE will prohibit further login of that user after an administrator configured 3 attempts until the Primary Directory Administrator or Administrative Group Members with the Password Administrator administrative role resets the user's password.

The TOE maintains the following security attributes for each user:

- Administrative roles - one or more administrative roles; only valid when the user's security role is Administrative Group Members
- Distinguished Name (DN)
- Failed login attempts data:
  - pwdAccountLockedTime - the time the user's account was locked
  - pwdFailureTime - the time stamps of the consecutive authentication failures
  - pwdReset - a flag to indicate whether or not the user's account was locked
- Password
- pwdChangedTime - the last time the user's password was changed (for user's associated with the global password policy)
- Security role - one role per user

This section maps to the following SFR(s):

- FIA_AFL.1-admin - Authentication failure handling
- FIA_AFL.1-user - Authentication failure handling
- FIA_ATD.1 - User attribute definition
- FIA_SOS.1-admin - Verification of secrets
- FIA_SOS.1-user - Verification of secrets
- FIA_UAU.1 - Timing of authentication
- FIA_UID.1 - Timing of identification
- FMT_MOF.1-auth - Management of security functions behavior

7.1.4 Security management

This section describes the security management capabilities of the TOE. This section is divided into the following subsections:

- Roles
- Audit management
- Access control management
- I&A management

7.1.4.1 Roles

7.1.4.1.1 Security roles

Each user account has one security role assigned to it. The TOE supports the following security roles:

- **Primary Directory Administrator** - This security role 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.

- **Administrative Group Members** - This security role is for users that have been assigned a subset of administrative privileges. Administrative Group Members can have a different set of administrative roles assigned to each of them by the Primary Directory Administrator (administrative roles are described in section 7.1.4.1.2). The 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.
- **Global Administrative Group Members** - This security role is equivalent to the Administrative Group Members security role with the Directory Data Administrator administrative role (see section 7.1.4.1.2 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 Administrative Group Members with the Directory Data Administrator administrative role may act as Global Administrative Group Members using the proxy authorization.
- **Master Server DN** - This 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** - This security role is for 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.

All roles are defined within the TOE. While the LDAP User and the Master Server DN security roles 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 Administrative Group Members, which will have a limited set of the Primary Directory Administrator's administrative rights.

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. 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 an account with the Administrative Group Members security role to perform these actions depends on the administrative roles assigned to the account.)

The Primary Directory Administrator or 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).

Administrative Group Members or Global Administrative Group Members also cannot perform some extended operations.

This section maps to the following SFR(s):

- FMT_SMF.1 - Specification of Management Functions
- FMT_SMR.1 - Security roles

7.1.4.1.2 Administrative roles

Only the 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 an account with the Administrative Group Members security role.

At a minimum, all administrative roles, including No Administrator, have the following capabilities:

- 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 TOE supports the following administrative roles. The name in parentheses is the administrative role short name used by the TOE.

- **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.
- **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.
- **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 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 LDAP Server and the Administration Server.

This section maps to the following SFR(s):

- FMT_MTD.1 - Management of TSF data
- FMT_SMF.1 - Specification of Management Functions
- FMT_SMR.1 - Security roles

7.1.4.2 Audit management

The TOE allows authorized administrators to manage the security behavior of the following audit functions:

- **Auditing** - enable/disable auditing
- **Audit logging**:
  - Specify an audit log file name
  - Specify the audit version: version 3 must be selected in the evaluated configuration
- **Event auditing** - select the event types (e.g., bind, add) and event outcome types (success, failure) to be audited

The following security roles are authorized to modify the security behavior of the audit functions:

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

This section maps to the following SFR(s):

- FMT_MOF.1-audit - Management of security functions behavior
- FMT_SMF.1 - Specification of Management Functions

7.1.4.3 Access control management

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 security roles are the entryOwners for all objects in the directory by default, and this entryOwnership cannot be removed from any object:

- Primary Directory Administrator
- Administrative Group Members with the Directory Data Administrator administrative role
- Global Administrative Group Members

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 following security roles:
    - Primary Directory Administrator
    - Administrative Group Members with the Schema Administrator administrative role

  This means that these users can specify if an entry is encrypted and specify the encryption type. 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 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 constraints 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.

This section maps to the following SFR(s):

- FMT_MSA.1 - Management of security attributes
- FMT_MSA.2 - Secure security attributes
- FMT_MSA.3 - Static attribute initialization
- FMT_SMF.1 - Specification of Management Functions

7.1.4.4 I&A management

The following security roles can modify the LDAP Server authentication mechanism function's behavior (i.e., select Simple Bind or SASL):

- Primary Directory Administrator

- Administrative Group Members with the Directory Data Administrator administrative role
- Global Administrative Group Members
- Master Server DN

The following security role can modify the behavior of the administrative password policy:

- Primary Directory Administrator

The following security roles can modify the behavior of the global password policy:

- Primary Directory Administrator
- Administrative Group Members with the Directory Data Administrator administrative role
- Global Administrative Group Members
- Master Server DN

The following security role can modify a user's administrative roles security attribute:

- Primary Directory Administrator

The following user or security roles can modify the password of a user account that has the LDAP User security role:

- Primary Directory Administrator
- Administrative Group Members with the Directory Data Administrator administrative role
- Administrative Group Members with the Password Administrator administrative role
- Global Administrative Group Members
- Self (account owner)

The following security roles can modify the schema file security configuration data:

- Primary Directory Administrator
- Administrative Group Members with the Schema Administrator administrative role

This section maps to the following SFR(s):

- FMT_MOF.1-auth - Management of security functions behaviour
- FMT_MTD.1 - Management of TSF data
- FMT_SMF.1 - Specification of Management Functions

8 Abbreviations, Terminology and References

8.1 Abbreviations

ACI
Access Control Information

ACL
Access Control List

API
Application Programming Interface

DB2
IBM DB2 Database

DIT
Directory Information Tree

DN
Distinguished Name

EOI
Entry Owner Information

IETF
The Internet Engineering Task Force

GSKit
IBM Global Security Kit

JNDI
Java Naming and Directory Interface

LDAP
Light weight Directory Access Protocol

MD5
Message Digest algorithm 5

RDN
Relative Distinguished Name

SASL
Simple Authentication and Security Layer

SFR
Security Functional Requirement

SHA-1
Secure Hash Algorithm 1

SHA-2
Secure Hash Algorithm 2 family of algorithms

SSL
Secure Sockets Layer

TDS
Tivoli Directory Server

TLS
Transport Layer Security

TOE
Target of Evaluation

TSF
TOE Security Function

UCS
Universal Character Set

UTF-8
UCS Transformation Format — 8-bit

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administration Server
The daemon that allows administrators to control and manage the LDAP Server.

Directory server
Depending on context, either the combination of the Administration Server and LDAP Server as a single instance or any manufacturer's LDAP directory server.

LDAP Client
A program that communicates with a directory server using LDAP.

LDAP Server
The daemon that provides the full LDAP interface to standard LDAP clients.

rootDSE
The root Directory Specific Entries contains directory server maintained attribute values which describe the capabilities of the directory server. The rootDSE can be read by searching the directory with an empty baseDN and a search scope of base level.

8.3 References

CC	**Common Criteria for Information Technology Security Evaluation**	
	Version	3.1R3
	Date	July 2009
	Location	http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf
	Location	http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf
	Location	http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf
CEM	**Common Methodology for Information Technology Security Evaluation**	
	Version	3.1R3
	Date	July 2009
	Location	http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf

PSEARCH **Persistent Search: A Simple LDAP Change Notification Mechanism**
Author(s) M. Smith, G. Good, T. Howes, R. Weltman
Date 2000-11-15
Location http://www.ietf.org/proceedings/51/I-D/draft-ietf-ldapext-psearch-03.txt

RFC1777 **Lightweight Directory Access Protocol**
Author(s) W. Yeong, T. Howes, S. Kille
Date March 1995
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc1777.txt.pdf

RFC2222 **Simple Authentication and Security Layer (SASL)**
Author(s) J. Myers
Date October 1997
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc2222.txt.pdf

RFC2246 **The TLS Protocol Version 1.0**
Author(s) T. Dierks, C. Allen
Date January 1999
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc2246.txt.pdf

RFC2251 **Lightweight Directory Access Protocol (v3)**
Author(s) M. Wahl, T. Howes, S. Kille
Date December 1997
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc2251.txt.pdf

RFC2252 **Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions**
Author(s) M. Wahl, A. Coulbeck, T. Howes, S. Kille
Date December 1997
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc2252.txt.pdf

RFC2253 **Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names**
Author(s) M. Wahl, S. Kille, T. Howes
Date December 1997
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc2253.txt.pdf

RFC2254 **The String Representation of LDAP Search Filters**
Author(s) T. Howes
Date December 1997
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc2254.txt.pdf

RFC2255 **The LDAP URL Format**
Author(s) T. Howes, M. Smith
Date December 1997
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc2255.txt.pdf

RFC2256 **A Summary of the X.500(96) User Schema for use with LDAPv3**
Author(s) M. Wahl
Date December 1997
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc2256.txt.pdf

RFC2830 **Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security**
Author(s) J. Hodges, R. Morgan, M. Wahl
Date May 2000
Location http://www.rfc-editor.org/rfc/pdfrfc/rfc2830.txt.pdf

RFC6101 **The Secure Sockets Layer (SSL) Protocol Version 3.0**
Author(s) Alan O. Freier, Philip Karlton, Paul C. Kocher
Version RFC 6101
Date August 2011
Location http://www.rfc-editor.org/rfc/rfc6101.txt

