CA Directory r8.1 0608 (build 942)

for the Sun Solaris platform

Security Target V2.6

April 29, 2007

Suite 100 West♦7927 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

Table and Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification:	CA Directory r8.1 0608 (build 942) for the Sun Solaris platform
ST Title:	CA Directory r8.1 0608 (build 942) for the Sun Solaris platform
ST Version:	Version 2.6
ST Date:	April 29, 2007
Assurance Level:	EAL3
Strength of Function:	SOF medium
Registration:	<To be filled in upon registration>
Keywords:	Directory, LDAP, X.500, Identification, Authentication, Access Control, Replication, Security Target, and Security Management

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for the CA Directory r8.1 0608 (build 942) for the Sun Solaris platform. The CA Directory is a Lightweight Directory Access Protocol (LDAP) and X.500 standards based directory service that can be configured and applied to meet individual organizational, geographic, information management, and security requirements. The CA Directory offers a configurable, customizable framework for systems integrators and administrators.

1.3 Common Criteria Conformance

The TOE is Part 2 extended and Part 3 conformant (EAL3), and meets the requirements of Evaluation Assurance Level (EAL) 3 from the Common Criteria Version 2.2. The TOE does not claim conformance to any PP.

The ST considered the CC International Interpretations for Version 2.2 and found none are applicable to this ST. The NIAP interpretations were not considered.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, describes the conformance claims of this ST to any PP(s).

Section 8, Rationale presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Sections 9 and 10, provide acronym definitions and references.

2 TOE DESCRIPTION

2.1 Product Type

The CA Directory is a directory software application, and as such it provides a system to store and manage electronic information. The CA Directory can operate in a standalone mode or, as typical for directories, provide directory services to other applications, operating as part of larger systems. CA Directory can also operate in a large distributed directory system and itself be deployed as a large distributed directory, supporting distributed directory functionality such as replication and chaining, involving distributed authentication mechanisms.

A common example of a directory, or distributed directory, system application is a Public Key Infrastructure (PKI) system where the directory provides the means to distribute certificates and CRLs. To interoperate as part of larger systems and to facilitate access to its information the CA Directory supports standard directory and network interface protocols LDAP, X.500 (DAP, DSP and DISP) and SSL, SNMP, CMIP.

The CA Directory product includes several components. The center of the product is the DXserver component. This central component is supported by tools, clients and web service components. The following lists these components that comprise the product: a directory server (DXserver) and its configuration files, a database for data storage (Ingres), an administrative interface (DXconsole), a process that handles the SSL and TLS link encryption (SSLD), components to facilitate operations for a distributed implementation (DXadmind and DXmanager), graphical Directory Browsers (JXplorer, JXweb), UDDI development tools (UDDI server and UDDI client), utilities for importing and exporting data (DXtools), and webservices development tools (DSML Server, SAML server, and SPML server). Sample test LDAP and DAP clients (LDUA and DUA) are also included with the product, but do not provide security functionality for the TOE or its environment.

These CA Directory components are organized into two installation groups. These groups can be installed on the same computer or on different computers with the exception that SSLD must be installed on the same server as the DXserver. All the components in a group must be installed for that group. The Installation process for the TOE installs only the DXserver, Ingres, DXconsole, SSLD, DXtools, and DXadmind, and then the evaluated configuration set up disables DXadmind.

The CA Directory operating environment requires physical security measures to protect access to the Directory Group components commensurate with the value of the information it is managing. Its users access the directory information and services using network, typically internetwork, connections.

2.2 Scope of the Evaluation

The scope of the evaluation includes the CA Directory server (DXserver), its supporting database (Ingres), and the administrative interface (DXconsole). The DXserver and DXconsole implement the directory security services to its users through DAP, LDAP, DSP, and DISP interfaces. These are the only interfaces visible to non-administrative users. DAP and LDAP are used for human users or directory-enabled applications to access the directory repository information. DSP and DISP are

used when the directory works with other standard directory servers (DSAs) as part of a directory system, and are used for distributed authentication and replication, respectively. These other DSAs, external to the TOE, are referred to in this ST as 'Trusted Peer DSAs'.

The Ingres database, when installed in its evaluated configuration provides only operational support to the DXserver. It only provides an interface to the DXserver on the protected platform. There are no external interfaces to the Ingres database. The SSLD process is outside the scope of the evaluation and is considered part of the evaluation IT environment. It provides the cryptographic operations for the certificate-based authentication functions and for data confidentiality and integrity for the trusted channel for remote users.

The CA Directory has two other components that are part of its installation package and are automatically installed in the installation process, DXtools and DXadmind. DXadmind is disabled in the evaluated configuration. These are not required for operations and are not used to provide the functionality specified in the ST. DXtools is a set of utilities used for importing, exporting, and synchronizing data with internal or external data systems. DXadmind is used to support the CA Directory implemented as a distributed directory, i.e., multiple DSAs for a DIB, this is not the evaluated configuration.

The evaluated CA Directory can operate in different environments supporting directory-enabled applications and user interfaces that implement the standard directory interfaces. The evaluation examines a single DXserver as it could operate in a standalone mode or as part of a larger directory system interoperating with other Trusted Peer DSAs. Table 2-1 specifies the evaluated configuration. It defines another instance of the DXserver as the Trusted Peer DSA for evaluating the functions that require a directory system, e.g., distributed authentication and replication. The TOE can also operate as a single directory application for its users, a central repository for an organization, or as part of a larger system, e.g., PKI system.

2.2.1 Physical Scope of the evaluation

The scope of the CA Directory evaluation includes the following components and interfaces. The other components that comprise the CA Directory product are not included in the evaluation and do not contribute to meeting the evaluation requirements except the SSLD process. As specified below in the evaluated configuration, only the 'Directory Group' components (DXserver, DXconsole, DXadmind, and DXtools) are installed for the evaluation, and they are all installed on a single physically protected server.

1. DXserver – the directory server software component:
    - Interface to untrusted users (referred to as relying parties) and remote trusted superusers and administrators using LDAP and DAP;
    - Interface to other DSAs (remoted trusted DSAs) using DSP for distributed authentication and DISP for replication;
    - Interface to local administrative console using local telnet.
2. Ingres r3 database - for data storage, provides operational functionality but no security functionality for the security functions specified in this ST.
3. DXconsole – the administrative interface component

- Local console to DXserver through a local telnet connection.
- Command line interface to the repository data using the DXserver DAP interface, and to configuration parameters in the DXserver operational memory.

4. DXserver Configuration and Log files – text files on the platform that co-reside with the DXserver

The following environment IT components are required for the CA Directory to operate and meet the evaluation requirements:

1. The CA Directory SSLD process provides SSL authentication and cryptographic services for the directory certificate-based authentication and partial protected data transmission;
2. Operating Platform (operating system and hardware) to;
   - support and protect the TOE and its files;
   - provide reliable time; and
   - an identification and authentication mechanism to ensure only a superuser has access to the server platform to access the TSF configuration and log files;
3. A text editor for modifying configuration files on the platform;
4. An application to read or process the audit log text files on the platform;
5. A remote trusted peer DSA to provide:
   - authentication services for the distributed authentication mechanisms, ‘peer DSA password check’ and ‘conveyed originator’;
   - remote side for trusted channel; and
   - replication services to update superuser specified portions of the data maintained in the directory repository.
6. A remote directory-enabled interface (DUA) and platform to provide its side for a trusted channel and an I&A function to ensure only authorized access to certificates used for SASL authentication;
7. Network communication software on the platform;
8. Network connection.
9. Java Runtime Environment 1.4.2 (provided on the CA Directory installation CD)

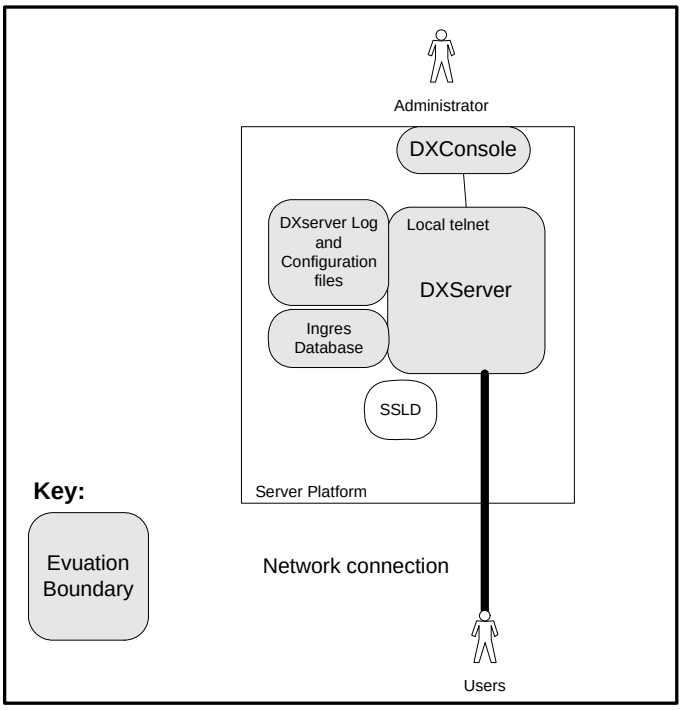

Figure 2-1 – TOE Physical Boundary

2.3 Logical Boundary

The TOE provides the following evaluated security services:

1. Audit Generation and Selection – The TOE generates audit records for selected security events. The records are stored in the log text files on the DXserver platform. An application in the TOE environment is required to read the audit records.
2. Access Control over Repository Data (the information the directory stores and manages for users) – the TOE uses the X.501 access control scheme to control access to its repository data for users accessing the directory using DAP and LDAP. These users are the relying parties and administrative users using a directory-enabled interface. DAP and LDAP are the only interfaces for these users.
3. Identification and Authentication – The DAP and LDAP interface requires its users to identify and authenticate themselves to establish a DAP or LDAP session, or if there is no identification or authentication provided be considered 'anonymous' users. The above access control function controls the information anonymous users have access to. The TOE provides DAP and LDAP users several authentication mechanisms: password-based, certificate-based, and distributed authentication for users in a distributed directory environment. The remote trusted peer DSAs that access the TOE using DSP and DISP, are required to authenticate using the certificate-based mechanism to establish the DSP and DISP sessions. The DXserver uses the SSLD process to validate the certificate provided by the client for the SSL connection. This processed certificate is then used by the DXserver to authenticate the user. The DXconsole users are authenticated by the TOE using a password

mechanism. A TOE configuration file specifies which users are allowed access to the local console and then those users are authenticated using the same password mechanism as the DAP users.

4. Administration and Trusted Data Management – the TOE, through the DXconsole, provides the TOE's superusers access to control the security functions and manage the trusted data. While all the security functions and data can be accessed from the DXconsole, some of the trusted data resides in configuration text files on the DXserver and some in the repository. The data in the configuration files requires a Unix superuser to modify the files using a text editor on the operating system for the modifications to be persistent when the DXserver restarts. The data in the repository can be managed through the DUA interface. In addition, administratively specified remote trusted peer DSAs are able to update defined portions of the repository data through replication.

   Note: It's important to note role terminology for this TOE. The TOE has a 'superuser' role which is NOT the Unix superuser. The TOE's superuser role can delegate management responsibilities for a portion of the Directory Information Tree (DIT) to an 'administrator' role. Different environments may use different terminology. It's common for the terms 'administrator' and 'data manager' to be substituted for the TOE's 'superuser' and 'administrator' roles, respectively.

5. Password Management – supporting the password-based authentication mechanism a TOE superuser can specify a policy for passwords that includes authentication failure mechanisms and rules that define acceptable passwords.

6. Partial Protected Data Transmission – the DXserver enforces when the data transmitted to and from remoted trusted peer DSAs over the network must be through a trusted channel, with assured identification of the end points and the data protected from unauthorized disclosure and modification. The TOE must also provide a trusted channel when users initiate communication with the TOE via a trusted channel. The DXserver relies on the SSLD process in its IT environment to perform the SSL protocol with its associated cryptography to process certificates for authenticating the end points of the communication channel and to encrypt the data.

7. Partial TOE Self Protection - working in concert with its platform, the TOE provides protection of its security functions through non-bypassability and domain separation. All user operations are conducted in the context of an associated session. The TOE manages these sessions to prevent one session from compromising another session. The TOE provides only well-defined interfaces to these sessions, and the sessions allocated only after successful authentication, or when a session is requested from the physically protected local console which is under procedural control. The TOE relies on its platform to operate correctly and to prevent unauthorized access to TOE data and stored executables.

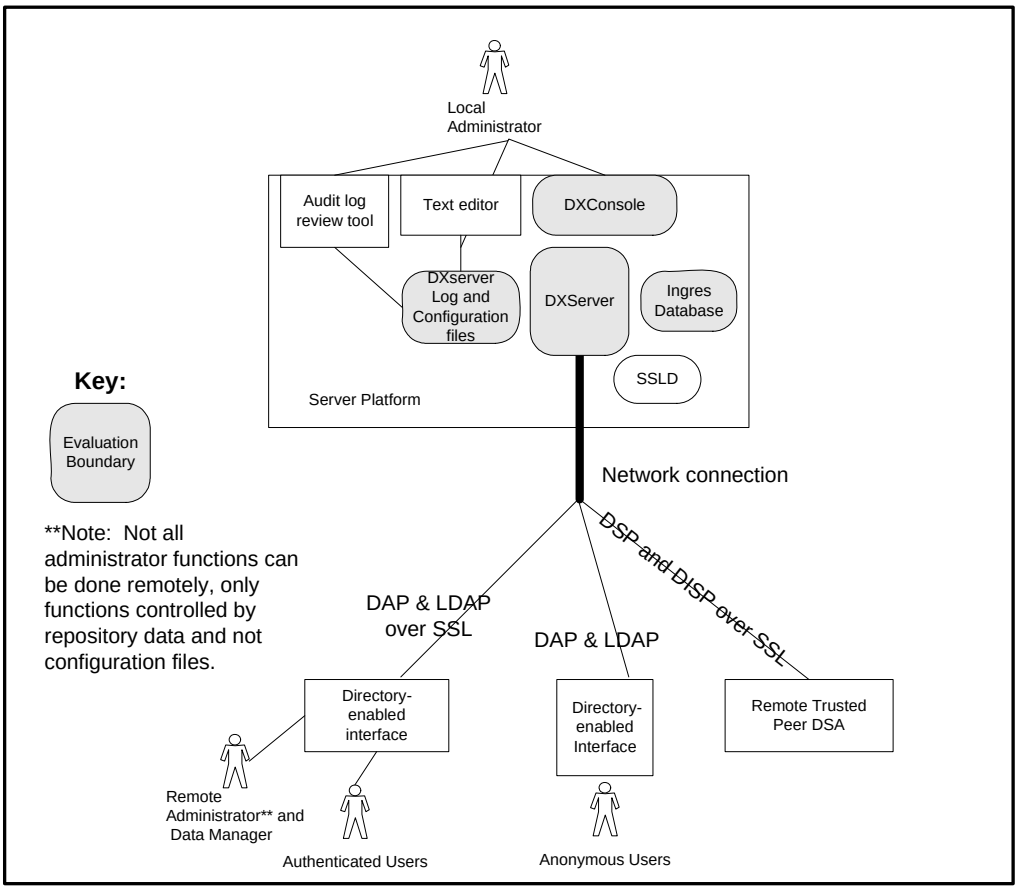

Figure 2-2 – TOE Boundary with Users Direct and Indirect Interfaces

2.4 Evaluated Configuration

The following is the evaluated configuration for the TOE.

Table 2-1 – Evaluated Configuration

	TOE Components Version	Support IT Environment
'Directory Group' components (DXserver, DXconsole, Ingres Database, DXadmind and DXtools). Product obtained from: ETRDIR99000-8.1-0608.zip (Solaris ISO).	DXserver 8.1.942 DXconsole 8.1.942 Ingres r3.0.3 211	Solaris 9 on Sun Sparc DXtools r8.1.942 (not used) DXadmind 8.1.942 (disabled)

Text editor and application to read audit log text files		Provided by Solaris
Perl for log file comparison		Perl V5.6.1
Cryptographic support		SSLD 8.1.942
Network communication software for the platform.		Provided by Solaris
Trusted Peer DSA on Remote		DXserver 8.1.942
Remote Directory-enabled LDAP interface		LDUA 8.1.942
Remote Directory-enabled DAP interface		DUA 8.1.942
Java Runtime Environment		JRE 1.4.2_09
Configuration requirements:	Please see Admin Guide for complete and specific list of configuration requirements, the following characterizes them. Remote console disabled DXadmind disabled Sample DSAs disabled Password policy set based on Admin Guidance. Ignore password expiration not allowed. Ignore suspension due to authentication failure not allowed. Dynamic and Static access controls enabled. Audit enabled. Superusers given access to local console Anonymous user access allowed SSL authentication required for remote trusted peer access No DXCache No multiwrite replication. Distributed directory operations set as specified in the Admin Guidance, including: ▪ No routing to prevent forwarding requests to another DSA regardless of access control constraints; ▪ Trusted-conveyed-originator authentication enabled; ▪ No downgrading allowed across a DSP link;	

The SSLD 8.1.942, LDUA 8.1.942, and DUA 8.1.942 components identified in the above list are delivered with CA Directory that were used in the environment. These IT components were part of the evaluated configuration and are recommended to be used. Any potential replacements for these components, in particular the LDUA 8.1.942, and DUA 8.1.942 clients, were not evaluated and should be evaluated before use.

3 TOE Security Environment

This section identifies secure usage assumptions and threats. There are no organizational security policies to be considered for the TOE.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 - Assumptions

No.	Assumption	Description of Assumption
1.	A.DIRECTORY_SYSTEM_SECURITY_ POLICY_ENFORCEMENT	It is assumed before enabling replication and/or distributed I&A mechanisms, a superuser must ensure that the appropriate level of trust has been established and that the I&A and/or access control security policies are understood and enforced.
2.	A.INTEROP	The TSF and the user DUAs, remote trusted peers, and IT environment are configured for proper interoperation.
3.	A.NO_EVIL	Trusted users are non-hostile, appropriately trained and follow all guidance.
4.	A.NO_GENERAL_PURPOSE	The superuser ensures there are no untrusted users, no untrusted software, and no general–purpose computing or storage repository capability (e.g., compilers, editors, or user applications) available on the TOE.
5.	A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE, and as a part of the TOE the access to the local console will have appropriate physical security and procedures to ensure and monitor exclusive superuser access.
6.	A.REMOTE_ADMIN_DUA_ENVIRONMENT	The end user will manage and protect the Administrative DUA in a manner that is commensurate with the value of the IT assets protected by the TOE.
7.	A.USERS	It is assumed that users will protect their authentication data.

3.2 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is proficient with access to specialized equipment and public information.

The TOE must counter the following threats to security:

Table 3-2 - Threats to Security

No.	Threat	Description of Threat
1.	T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
2.	T.TSF_COMPROMISE	A user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
3.	T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according the TOE security policy.
4.	T.UNIDENTIFIED_ACTIONS	The superuser may not have the ability to notice potential security violations, thus limiting their ability to identify and take action against a possible security breach.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 - Security Objectives for the TOE

No.	Objective	Objective Description
1.	O.AUDIT	The TOE will detect and create records of superuser-defined security events.
2.	O.MANAGE	The TOE will provide all the functions and facilities necessary to support administrative users in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
3.	O.MEDIATE	The TOE must protect user data in accordance with its security policy.
4.	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
5.	O.PARTIAL_SELF_ PROTECTION	The TSF will maintain a domain or its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
6.	O.PARTIAL_TRUSTEDCOMM	The TOE in concert with its IT Environment will provide a trusted channel using SSL between the TOE and its environment.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 - Security Objectives for IT Environment

No.	Objective	Objective Description
1E	OE.AUDIT_ACCESS	The IT environment will protect the audit records and provide a means for a superuser to access and read the audit information.
2E	OE.DISTRIBUTED_AUTHENTICATION	The IT environment will provide authentication mechanism to support 'conveyed originator' distributed directory authentication, and will provide a password check to support 'peer DSA password check' distributed directory authentication.

No.	Objective	Objective Description
3E	OE.I&A	The IT environment will provide I&A mechanism(s) to control access to an account on the platform to provide access control to the TSF configuration and log files, and to control access to individual user certificates used for SASL authentication.
4E	OE.TIME	The IT Environment will work in concert with the TOE to provide a reliable time stamp for the TOE use.
5E	OE.PARTIAL_SELF_ PROTECTION	The IT Environment will work in concert with the TOE to protect it from unauthorized modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within its scope of control.
6E	OE.PARTIAL_TRUSTEDCOMM	The IT Environment will work in concert with the TOE will provide a trusted channel using SSL between the TOE and its environment.

4.2.2 Security Objectives for the Non-IT Security Environment

The Non-IT security objectives are as follows:

Table 4-3 - Security Objectives for the Non-IT Security Environment

No.	Objective	Objective Description
1N	ON.DIRECTORY_SYSTEM_SECURITY_POLICY_ ENFORCEMENT	The Environment procedures will ensure that before enabling replication and/or distributed I&A mechanisms, a superuser must ensure that the appropriate level of trust has been established and that the I&A and/or access control security policies are understood and enforced.
2N	ON.INTEROP	The environment procedures will ensure that the TSF and the user DUAs, remote trusted peers, and IT environment are configured for proper interoperation.
3N	ON.NO_EVIL	The environment procedures will ensure trusted users are non-hostile, appropriately trained and follow all guidance.

No.	Objective	Objective Description
4N	ON.NO_GENERAL_PURPOSE	The environment procedures will ensure that there are no untrusted users, no untrusted software, and no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
5N	ON.PHYSICAL	The environment procedures will ensure that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE, and as a part of the TOE the access to the local console will have appropriate physical security and procedures to ensure and monitor exclusive superuser access.
6N	ON.REMOTE_ADMIN_DUA_ ENVIRONMENT	The environment procedures will ensure the end user will manage and protect the Administrative DUA in a manner that is commensurate with the value of the IT assets protected by the TOE.
7N	ON.USERS	The environmental procedures will ensure that the users will protect their authentication data.

5 Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, assurance components from Part 3 of the CC and explicit functional components derived from the CC components.

The notation, formatting, and conventions used in this security target (ST) are consistent with the Common Criteria. The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Section 1.4 above and in Common Criteria, Part 1, Section 4.4.1.3.2.

This ST indicates which text is affected by each of these operations in the following manner:

- Assignments and selections specified by the ST author are in ***[italicized bold text]***.
- Refinements are specified by the ST author by **Refinement:** placed at the beginning of the refined text and are in ***italicized bold and underlined text***.
- Iterations used to indicate varying operations are specified by the ST author by another number placed at the end of the component ID such as FMT_MTD.1-1 and FMT_MTD.1-2.
- Explicitly stated requirement, if applicable, is noted with a "_EXP" added to the component ID.
- Application notes are included with some requirements and provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text*.

5.1 TOE Security Functional Requirements

The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC and explicit components, summarized in the Table 5-1 below.

Table 5-1 - TOE Security Functional Components

No.	Functional Component ID	Functional Component
1.	FAU_GEN.1	Audit data generation
2.	FAU_SEL.1	Selective audit
3.	FDP_ACC.1	Subset access control
4.	FDP_ACF.1	Security attribute based access control
5.	FIA_AFL.1	Authentication failure handling
6.	FIA_ATD.1	User attribute definition
7.	FIA_SOS.1	Verification of secrets
8.	FIA_UAU.1	Timing of authentication
9.	FIA_UAU.5-1	Multiple authentication mechanisms (TOE)

No.	Functional Component ID	Functional Component
10.	FIA_UID.1	Timing of identification
11.	FMT_MSA.1-1	Management of security attributes (TOE)
12.	FMT_MTD.1-1	Management of TSF data (TOE)
13.	FMT_SMF.1	Specification of management functions
14.	FMT_SMR.1	Security roles
15.	FPT_RVM_EXP_TSF.1	Partial Non-bypassability of the TSP by the TOE
16.	FPT_SEP_EXP_TSF.1	Partial TSF domain separation by the TOE
17.	FTP_ITC_EXP_TOE.1	Partial Inter-TSF trusted channel by the TOE

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

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

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the ***[not specified]*** level of audit, and
- c) ***[the auditable events listed in the table below].***

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

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***[information specified in column four of the table below]***.

Table 5-2 – Auditable Events

No.	Requirement	Auditable Events	Additional Audit Record Contents
1.	FAU_GEN.1	None	N/A
2.	FAU_SEL.1	Modifications (close log, set log, and set trace) to the audit configuration in operating memory that occur while the audit collection functions are operating	None
3.	FDP_ACC.1	None	N/A

No.	Requirement	Auditable Events	Additional Audit Record Contents
4.	FDP_ACF.1	Operations that invoke object security attributes.	The identity of the user that caused the event.
5.	FIA_AFL.1	None	N/A
6.	FIA_ATD.1	None	N/A
7.	FIA_SOS.1	None	N/A
8.	FIA_UAU.1	Unsuccessful use of the password based authentication mechanism.	The identity of the user that caused the event.
9.	FIA_UAU.5-1	The final decision on authentication	The identity of the user that caused the event. Must exclude all password information in the audit record.
10.	FIA_UID.1	Unsuccessful use of the password based identification mechanism.	The identity of the user that caused the event.
11.	FMT_MSA.1-1	1. Modifications of the dynamic access control rules, stored in the repository. 2. Modifications of the static access control rules in the operating memory, by the local console.	1. The identity of the user that caused the event. 2. None
12.	FMT_MTD.1-1	1. Operations on the TSF data located in the repository. 2. Operations performed on the operating memory from the console.	1. The identity of the user that caused the event. 2. None
13.	FMT_SMF.1	None	N/A
14.	FMT_SMR.1	None	N/A
15.	FPT_RVM_EXP_TSF.1	None	N/A
16.	FPT_SEP_EXP_TSF.1	None	N/A
17.	FTP_ITC_EXP_TOE.1	The DSP Bind (authentication process with trusted Peer DSA) success.	The identity of the user that caused the event.

Application Note: The TOE defines the startup and shutdown of the audit function as the same as the startup and shutdown of the dxserver.

FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [event type, except alarm events

b) *"no additional attributes"].*

Application Note: The TOE defines event types by the log file used to capture the audit data. The types of events, as defined in Section 6, are: 'alarm events', 'authentication errors', 'failed

operations', 'search activity', 'summary of daily activity', 'diagnostic tracing', and 'all add, delete, modify, and rename operations'.

5.1.2 Class FDP: User Data Protection

Application Note: For evaluation – the specification of the access control policy is based on the Directory PP cited in the reference section.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the ***[CADirectory Access Control SFP]*** on ***[***

- ***Subjects: LDAP and DAP sessions;***
- ***Objects: the repository information, both information entries and information attribute types; and***
- ***Operations: all operations between the subjects and objects specified above.]***

Application Note: the LDAP and DAP sessions are created through the Directory LDAP and DAP Bind process. These sessions created from LDAP and DAP Binds provides access for all users except the superusers using the local console port, and trusted Peer DSAs. The superusers accessing the Directory using DAP or LDAP are subject to this access control policy.

Trusted Peer DSAs also access and update the repository data. They access the directory using DISP Bind for replication functions, and DISP Binds for distributed authentication mechanisms and other trusted operations. The control over these operations is specified in FMT_MTD.1-1.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***[CA Directory Access Control SFP]*** to objects based on the following:

[Subject security attributes:

- ***Distinguished Name,***
- ***User Groups,***
- ***User Roles,***
- ***Authentication level,***

Application Note: Authentication level refers to how the subject authenticated to the directory: anonymously, with a password, or with a certificate.

It's CC convention that the requested operation is an implicit subject attribute.

Object security attributes:

- ***Access control rule(s) each specifying the following:***
  - ***objects for which the access control rule applies***
  - ***subjects for which the access control rule applies***
  - ***priority of the access control rule***

- ***permissions: Superuser, Administrator, Registered User, Public,***
- ***optional permissions: read, add, remove, rename, all.***
- ***authentication level required]***

Application Note: 'Permissions' translates to both X.501 permissions and to X.501 precedence in the access control decision function specified at the end of FDP_ACF.1.2. The 'optional permissions' are direct X.501 permissions, these are used to provide a mechanism for changing the precedence specified by the 'permissions'. Please see Section 6 for information on this translation.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[***

A. The access control rules must include rules where:

1. ***the subject requestor (i.e., distinguished name, user group, role) is in the access control rule subject set;***
2. ***the protected object of the operation is in the access control rule object set;***
3. ***the subject requestor is authenticated at the required level;***

- ***The set of all 'associated access control rules' include static and dynamic access control rules***

B. The access control decision must apply the following rules to the 'associated access control rules':

- ***only access control rules with the highest priority are considered;***
- ***grant access only if all access control decision access control rules grant access, i.e., if there are no access control rules, or at least one of them denies access, then access is denied.]***

Application Note: The policy implements the 1993 X.501 Simplified Access Control requirements. Please see Section 6 for more information.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***[no additional rules].***

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the ***[rules that anonymous users are denied all access except read access].***

5.1.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***[a superuser configurable positive integer from 1 to 2^{31} (~ 2 billion)]*** unsuccessful authentication attempts occur related to ***[unsuccessful simple password bind, and local console password authentication (FIA_UAU.5.1 a and b) attempts since the last successful authentication for the indicated user identity].***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall ***[disable the account for the superuser-specified period of time, e.g., 2 hours.]***

Application Note: The value 2^{31} is not a practical value. The superuser is required to use a value that supports the security policy as specified in the Administrator Guide Supplement, e.g., the evaluated configuration specified 3 retries allowed. The default value is 0 which means the function is disabled. The TOE mechanism that implements this requirement relies on its operating system's definition of integer resulting in this impractical high range of values.

FIA_ATD.1 User attribute definition

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

- ***a) Distinguished Name - the unique identifier***
- ***b) role;***
- ***c) group;***
- ***d) authentication password credential.]***

Application Note: User certificates (another form of user authentication credential) are not listed here because they are not stored in the directory the user binds to. A user supplies their certificate on a bind. The TOE then checks to see if it trusts the root certificate of the user's certificate.

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***[the following superuser-specified rules:***

- ***within the specified range for length;***
- ***includes the minimum number of specified types of characters;***
- ***doesn't exceed the specified limit of repetition of a character(s);***
- ***not specified number of previously used passwords;***
- ***doesn't include the user's own name;***
- ***is valid for specified number of days and considering the specified number of grace period logins allowed; and***
- ***is valid for specified number of days not in use.]***

Application Note: The rule 'valid for a minimum number of days' exists to prevent people from changing their password many times to fill up the password history.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow ***[Anonymous user Read access to public repository information in accordance with the CA Directory Access Control SFP]***

on behalf of the users 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.

FIA_UAU.5-1 Multiple authentication mechanisms (TOE)

FIA_UAU.5-1.1 The TSF shall provide ***[***

a) Simple authentication (password-based in Bind operation),

b) Password (console)

c) SSL authentication (certificate-based in Bind operation),

d) Distributed authentication via 'Peer DSA Password Check',

e) Distributed authentication via 'conveyed originator'.]

to support user authentication.

Application Note: SASL is an entity authentication protocol that uses certificates and associated asymmetric cryptographic algorithms negotiated in session.

Application Note: Distributed authentication is used when the TOE works as part of a distributed directory system where the credential information required to make an authentication decision is in a different directory server than the one that holds the information the user wants to access. A user can authenticate to the TOE with their password credentials stored on a Trusted Peer DSA using 'Peer DSA Password Check'.

FIA_UAU.5-1.2 The TSF shall authenticate any user's claimed identity according to the ***[following rules:***

a) Password authentication for superuser access to local console;

b) Simple authentication is performed when name and password credentials are presented during the Bind request;

c) SASL authentication is performed when:

- ***LDAP clients use SASL/EXTERNAL as their Directory Bind request, and***
- ***X.500 DAP clients use the Bind External Procedure as their Directory Bind request;***
- ***Remote Trusted Peer in the DSP and DISP Bind request, using X.500 Bind External Procedure ;***

Application Note: a remote trusted peer authenticates to perform replication (DISP) and for distributed authentication (DSP).

d) Distributed authentication via 'Peer DSA Password Check' is performed when a user makes a Bind request to the TOE and the TOE does not have the user's entry, their entry including their DN and password is on a trusted peer DSA.

e) ***Distributed authentication via 'conveyed originator is performed when the TOE receives a user request from a chained operation from a trusted peer DSA.]***

Application Note: A Directory Bind is the name of the operation users, via their DUA using the DAP or LDAP protocol, use to establish a connection to the DSA, i.e., the TOE. The Bind operation is the process where the user presents their credentials for authentication. Note, a DSA Bind also exists and is used among trusted peer DSAs for DSP and DISP operations.

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow ***[Anonymous user Read access to public repository information in accordance with the CA Directory Access Control SFP]***

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing

any other TSF-mediated actions on behalf of that user.

Application Note: Anonymous users do not need to provide an identifier during the bind operation, the TOE assigns the identifier 'anonymous' to these users.

5.1.4 Class FMT: Security Management

FMT_MSA.1-1 Management of security attributes (TOE)

FMT_MSA.1-1.1 The TSF shall enforce the ***[CA Directory Access Control SFP]*** to restrict the ability to ***[see table below]*** the security attributes ***[see table below]*** to ***[see table below].***

Table 5-3 – Management of security attributes in the TOE

Operations	Security Attributes	Roles
query, modify, and delete	***Dynamic access control rule, which reside in the repository***	• ***Superuser via DUA* interface** • ***Superuser via local console DAP.*** • ***Administrator superuser-specified privileges to access the data***
query, modify, and delete	***Static access control rules that reside in TOE memory***	• ***Superuser via the local console***
query	***X.501 representation of the combined dynamic and static access control rules***	• ***Superuser via the local console***

Application Note: The access control policy combines two sets of access controls, dynamic and active. The dynamic access controls are maintained in the directory repository and are accessible to the superuser by both the local console and a DUA. The static access controls are defined and stored in configuration files, and are copied into the TOE memory during startup. This memory copy is used during operation. Please see Section 6 for more information.

It's important to note that changes made to TSF data residing in the TOE memory, from the local console, are not saved after the DSA is shutdown. Therefore changes made to the static access control rules from the local console are not saved after the DSA is shutdown. Users must edit the configuration file from the operating system for these changes to remain after the DSA has been reinitialized or stopped and started, FMT_MSA.1-2, Management of security attributes (IT Environment).

FMT_MTD.1-1 Management of TSF data (TOE)

FMT_MTD.1.1-1 The TSF shall restrict the ability to ***[see table below]*** the ***[see table below]*** to ***[see table below]***.

Table 5-4 – Management of TSF data in the TOE

Operations	TSF data	Roles
Repository Data		
query, modify, delete	• ***(FMT_MTD.1-1) Managing the group of roles that can interact with the security attributes and TSF data.*** • ***(FIA_UID.1) DN for users of the repository.***	• ***Superuser via DUA interface*** • ***Superuser via local console DAP*** • ***Administrator superuser-specified privileges to access the data***
Replicate (successful, failure)	• ***(FMT_MTD.1-1) Managing the group of roles that can interact with the security attributes and TSF data.*** • ***(FIA_UID.1) DN for users of the repository.***	• ***Superuser-specified Trusted Peer DSA***
modify	• ***(FIA_UAU.1) Passwords***	• ***Superuser via DUA interface*** • ***Superuser via local console DAP*** • ***Administrator superuser-specified privileges to access the data*** • ***Registered user for own password when specified by a superuser***

Operations	TSF data	Roles
Configuration File Data in TOE Memory		
Query, modify	• ***(FAU_SEL.1) the TSF data that determines which events are being audited.*** • ***(FIA_AFL.1) management for the threshold for unsuccessful authentication attempts and action to be taken in the event of an authentication failure.*** • ***(FIA_SOS.1) metrics used to verify secrets***	• ***Superuser at the local console***

Application Note: Similar to FMT_MSA.1-1 above, changes made to TSF data residing in the TOE memory, (loaded into the memory from the configuration file at startup are not saved after the DSA is shutdown. Users must edit the configuration file from the operating system for changes to remain after the DSA has been reinitialized or stopped and started, see FMT_MTD.1-2, Management of security attributes (IT Environment). Also, there is some TSF data that can only be updated in the configuration from the IT environment, it's not maintained during operation in the TOE memory, see FMT_MTD.1-2.

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***[as specified in FMT_MTD.1-1 and FMT_MSA.1-1].***

FMT_SMR.1 Security roles

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

- ***Superuser***
- ***Administrator,***
- ***Registered User***
- ***Trusted Peer DSA*****].**

Application Note: The superuser role delegates to the administrator role administrative responsibilities for a portion of the Directory Information Tree (DIT). Usually these responsibilities are limited to managing the data in the DIT, rather than the structure of the DIT.

Note: Different environments may user different terminology. It's also common for the terms 'administrator' and 'data manager' to be used for the TOE's 'superuser' and 'administrator' roles, respectively.

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

5.1.5 Class FPT: Protection of the TSF

FPT_RVM_EXP_TSF.1 Partial Non-bypassability of the TSP by the TOE

FPT_RVM_EXP_TSF.1.1 The TSF, when invoked by the underlying platform, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP_EXP_TSF.1 Partial TSF domain separation by the TOE

FPT_SEP_EXP_TSF.1.1 The TSF, when invoked by the underlying host platform, shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_EXP_TSF.1.2 The TSF, when invoked by the underlying host platform, shall enforce separation between the security domains of subjects in the TSC.

Application Note: The TOE subjects are the user sessions.

5.1.6 Class FTP: Trusted path/channels

FTP_ITC_EXP_TOE.1 Partial Inter-TSF trusted channel by the TOE

FTP_ITC_EXP_TOE.1.1: The TSF shall provide assured identification of the end points of a trusted communication channel and relies on the IT environment to provide protection of the channel data from modification or disclosure.

FTP_ITC_EXP_TOE.1.2 The TSF shall permit the TSF or the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC_EXP_TOE.1.3 The TSF shall implement a trusted channel for:

- all communication between itself and a trusted peer DSA,
- all communication between itself and user DUAs when the user initiates the communication via a trusted channel

5.2 Security Functional Requirements for the IT Environment

The IT environment includes trusted external IT entities (e.g., peer trusted directories, time synchronization server) and any IT entities that are used by Directory Administrative users to remotely administer the TOE. These requirements consist of functional components from Part 2 of the CC. CA Directory requires that the operating system platform provide reliable time stamps and domain separation. All cryptographic functions are part of the environment, not part of the TOE.

Table 5-5 - Environment Functional Components

No.	Functional Component ID	Functional Component
1.	FAU_SAR.1	Audit Review
2.	FIA_UAU.2	User authentication before any action
3.	FIA_UAU.5-2	Multiple authentication mechanisms (IT environment)

4.	FIA_UID.2	User identification before any action
5.	FMT_MSA.1-2	Management of security attributes (IT environment)
6.	FMT_MTD.1-2	Management of TSF data (IT environment)
7.	FPT_RVM_EXP_PFM.1	Partial Non-bypassability of the TSP by the platform
8.	FPT_SEP_EXP_PFM.1	Partial TSF domain separation by the platform
9.	FPT_STM.1	Reliable time stamps
10.	FTP_ITC_EXP_ENV.1	Partial Inter-TSF trusted channel by the IT environment

5.2.1 Class FAU: Security Audit

FAU_SAR.1 Audit review

FAU_SAR.1.1 **Refinement:** The ***IT Environment*** shall provide ***[superusers]*** with the capability to read ***[all audit information]*** from the audit records.

FAU_SAR.1.2 **Refinement:** The ***IT Environment*** shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: these trusted users are typically trusted IT entities that facilitate the management of audit data for systems.

5.2.2 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 **Refinement:** The ***IT environment*** shall require each user to be successfully authenticated before allowing any ***platform***-mediated actions ***to the TSF, and remote DUA users access to their certificates when authenticating to the TSF using SASL*** on behalf of that user.

FIA_UAU.5-2 Multiple authentication mechanisms (IT Environment)

FIA_UAU.5-2.1 **Refinement:** The ***remote trusted peer DSA*** shall provide ***[***

- ***Distributed authentication via 'Peer DSA Password Check',***
- ***Distributed authentication via 'conveyed originator']***

to support user authentication.

FIA_UAU.5-2.2 **Refinement:** The ***remote trusted peer DSA*** shall authenticate any user's claimed identity according to the ***[***

- ***SASL***

- ***Distributed authentication via 'Peer DSA Password Check' is performed when a user makes a Bind request to the TOE and the TOE does not have the user's entry, their entry including their DN and password is on a trusted peer DSA.***
- ***Distributed authentication via 'conveyed originator is performed when the TOE receives a user request from a chained operation from a trusted peer DSA.]***

FIA_UID.2 User identification before any action

FIA_UID.2.1 **Refinement:** The ***IT Environment*** shall require each user to identify itself before allowing any *platform*-mediated actions ***to the TSF, and remote DUA users access to their certificates when authenticating to the TSF using SASL*** on behalf of that user.

5.2.3 Class FMT: Security Management

FMT_MSA.1-2 Management of security attributes (IT Environment)

FMT_MSA.1-2.1 **Refinement:** The ***IT Environment*** shall enforce the ***[CA Directory Access Control SFP]*** to restrict the ability to ***[query, modify, and delete]*** the security attributes ***[static access control rules]*** to ***[(Directory) Superuser]***.

Application Note: Superuseres are also able to make these changes via the TOE (FMT_MSA.1-1) however these changes are not saved after the DSA is shutdown. Users must edit the configuration file from the operating system for changes to remain after the DSA has been reinitialized or stopped and started.

FMT_MTD.1-2 Management of TSF data (IT Environment)-

FMT_MTD.1-2.1 **Refinement:** The ***IT Environment*** shall restrict the ability to ***[see table below]*** the ***[see table below]*** to ***[see table below].***

Table 5-6 – Management of TSF data in the environment

Operations	TSF data	Roles
query	***Log files***	***(Directory) superuser***
Query, modify	• (FDP_ACC/ACF) static access control rules • (FAU_SEL.1) the TSF data that determines which events are being audited. (FIA_AFL.1) management for the threshold for unsuccessful authentication attempts and action to be taken in the event of an authentication failure. • (FIA_UAU.1 and FIA_UID.1) allowing unidentified and unauthenticated (i.e., anonymous) users, and DN for trusted peers (authenticating with DSP and DISPBind) • (FIA_UAU.5): specifying the authentication mechanism parameters • (FIA_SOS.1) metrics used to verify secrets. • (FMT_MTD.1-1 and FMT_SMR.1) specifying the replication agreements that define the trusted peer DSAs that can updated specified portions of the repository data • (FTP_ITC_EXP.1) The configuration data that requires a trusted channel be used for communication with a trusted peer DSA and to enable it to respond to requests for a trusted channel from IT environment entities as specified in the requirement.	***(Directory) superuser***

Application Note: The (Directory) Superuser role is the same as the TOE superuser role, defined in FMT_SMR.1. '(Directory)' preceeding superuser' is to distinguish this is the role defined in the TOE vs. the platform UNIX Superuser.

Most of these operations are able to be made via the TOE (FMT_MTD.1-1) however the changes made through the local console are not saved after the DSA is shutdown. Users must edit the configuration file from the operating system for changes to remain after the DSA has been reinitialized or stopped and started. The TSF data associated with the following security requirements can only be updated via the configuration file as stated here in FMT_MTD.1-2 (and not via the local console): FIA_UAU.1, FIA_UID.1, FIA_UAU.5, FMT_MTD.1-1, FMT_SMR.1, and FTP_ITC_EXP.1.

5.2.4 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP_PFM.1 Partial Non-bypassability of the TSP by the platform

FPT_RVM_EXP_PFM.1.1 The security functions of the host platform shall ensure that the host platform security policy enforcement functions are invoked and succeed before each function within the scope of control of the host platform is allowed to proceed.

FPT_SEP_EXP_PFM.1 Partial TSF domain separation by the platform

FPT_SEP_EXP_PFM.1 The security functions of the host platform shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host platform.

FPT_SEP_EXP_PFM.2 The security functions of the host platform shall enforce separation between the security domains of subjects in the scope of control of the host platform.

Application Note: The subjects for the host platform are the subjects in execution.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 **Refinement:** The IT Environment shall be able to provide reliable time stamps for its own use.

5.2.5 Class FTP: Trusted path/channels

FTP_ITC_EXP_ENV.1 Partial Inter-TSF trusted channel by the IT environment

FTP_ITC_EXP_ENV.1.1: The IT Environment shall provide assured identification of the end points of a trusted communication channel and provide protection of the channel data from modification or disclosure using SSL.

FTP_ITC_EXP_ENV.1.2 The IT Environment shall initiate or permit the TSF to initiate communication via the trusted channel.

FTP_ITC_EXP_ENV.1.3 The IT Environment shall implement a trusted channel for:

- all communication between the TOE and a trusted peer DSA,
- all communication it initiates for users with the TOE when transmitting authentication and other trusted data.

5.3 Strength of Function

The overall strength of function requirement is SOF-medium. The strength of function requirement applies to the password mechanisms required in FIA_UAU.5-1, password authentication for superuser access to local console, and simple authentication in the Bind request. These are constrained by FIA_AFL.1 and FIA_SOS.1. The SOF claim for FIA_UAU.5-1.1 is SOF-medium. The strength of the password mechanism when constrained by the “secrets” mechanism is consistent with the objectives of authenticating users (O.TOE_ACCESS). Strength of Function shall be demonstrated for the password-based authentication mechanisms to be SOF-medium, as defined in Part 1 of the CC. Specifically, the local authentication mechanism must demonstrate adequate protection against attackers possessing a moderate attack potential.

5.4 TOE Security Assurance Requirements

The TOE assurance requirements for this ST are EAL3. All assurance requirements are summarized in the table below.

Table 5-7 - Assurance Requirements: EAL3

Assurance Class	Item	Assurance Components	
Configuration management	1	ACM_CAP.3	Authorisation controls
	2	ACM_SCP.1	TOE CM coverage
Delivery and operation	3	ADO_DEL.1	Delivery procedures
	4	ADO_IGS.1	Installation, generation, and start-up procedures
Development	5	ADV_FSP.1	Informal functional specification
	6	ADV_HLD.2	Security enforcing high-level design
	7	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	8	AGD_ADM.1	Administrator guidance
	9	AGD_USR.1	User guidance
Life cycle support	10	ALC_DVS.1	Identification of security measures
Tests	11	ATE_COV.2	Analysis of coverage
	12	ATE_DPT.1	Testing: high-level design
	13	ATE_FUN.1	Functional testing
	14	ATE_IND.2	Independent testing - sample
Vulnerability assessment	15	AVA_MSU.1	Examination of guidance
	16	AVA_SOF.1	Strength of TOE security function evaluation
	17	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

The following describes the IT Security Functions of the CA Directory TOE, and provides a mapping to the SFRs. The following table includes the IT environment SFRs that are required to support the IT Security Function for the TOE, note: there are additional IT requirements specified in the ST to help mitigate the Threats but are not required for supporting a TOE function, e.g., FAU_SAR.1 is included in the ST however it's not required to support the TOE Security Function 'Audit Generation and Selection'.

Table 6-1 – IT Security Functions and Requirements

No.	IT Security Function	Security Functional Requirements and the IT Environment Requirements
1.	Audit Generation and Selection	FAU_GEN.1
		FAU_SEL.1
		(IT Environment) FPT_STM.1, FAU_SAR.1
2.	Access Control over Repository Data	FDP_ACC.1
		FDP_ACF.1
		(IT Environment) FPT_STM.1
3.	Identification and Authentication	FIA_ATD.1
		FIA_UAU.1
		FIA_UAU.5-1
		FIA_UID.1
		(IT Environment) FIA_UAU.5-2
		(IT Environment) FIA_UAU.2
		(IT Environment) FIA_UID.2
4.	Password Management	FIA_AFL.1
		FIA_SOS.1
5.	Administration and Trusted Data Management	FMT_MSA.1-1
		FMT_MTD.1-1
		FMT_SMF.1
		FMT_SMR.1
		(IT Environment) FMT_MSA.1-2
		(IT Environment) FMT_MTD.1-2
6.	Partial Protected Data Transmission	FTP_ITC_EXP_TOE.1
		(IT Environment) FTP_ITC_EXP_ENV.1

No.	IT Security Function	Security Functional Requirements and the IT Environment Requirements
7.	Partial TOE Self Protection	FPT_RVM_EXP_TSF.1
		FPT_SEP_EXP_TSF.1
		(IT Environment) FPT_RVM_EXP_PFM.1
		(IT Environment) FPT_SEP_EXP_PFM.1

6.1.1 Audit Generation and Selection

The TOE generates audit records in its log files, stored on the operating system supporting the DXserver for auditable events of the security functions as specified in Section 5, FAU_GEN.1. The audit mechanism is always active while the DXserver is running, therefore starting and stopping the audit function is done when the DXserver is started and stopped. This action is recorded in the alarm.log; the alarm log cannot be closed (i.e., the logging turned off).

The superuser selects the auditable events to include and exclude by opening and closing the associated log file. The types of audit events are organized by the event type of the log file. The following is the list of the log files that are used to meet the requirements and their associated event types:

- Alarm_log – alarm events
- Alert_log – authentication errors
- Diag_log – failed operations
- Query_log – search activity
- Summary_log – summary of daily activity
- Trace-log - diagnostic tracing
- Update_log – all add, delete, modify, and rename operations
- Connect_log – all connects and disconnects by identity and authentication level

The following table identifies where the audit record is generated and the associated event type that forms the basis for including or excluding the auditable event for FAU_SEL.1. The superuser can specify which log files are open and closed through the TOE configuration file using a text editor in the IT environment, as specified in FMT_MTD.1-2. The superuser can also modify which log files are open and closed by modifying the operating memory through the local console command line interface. These modifications are active immediately but are not persistent when the DXserver is restarted. Physical protection and procedural measures ensure only the superuser has physical access to the console (A.PHYSICAL). The audit logs are stored as text files and are viewed from the IT environment operating system as specified in FAU_SAR.1 in the IT environment.

The identity of the user that caused the event is included in the audit records except for updates to the operating memory from the local console. The summary log show association numbers, and the

binds recorded in these logs show the user name if it's not anonymous access. The identity of the remote trusted peer for the DSP bind is included in the trace-log.

Table 6-2 – Audit Log and Event Information

Auditable Events from Secton 5, FAU_GEN.1	Audit Record Contents	Audit log file	FAU_SEL.1 Event Type
o (FAU_SEL.1) Modifications to the audit configuration that occur while the audit collection functions are operating	Standard contents: o Date and time of the event o Type of event o Subject identity, and the outcome (success or failure)	o Trace-log Note: This is not affected by trace levels, this is recorded even if the trace level is set to 'none'	o Trace Log must be open. Event type: diagnostic tracing.
o (FDP_ACF.1) Requests to perform a security relevant operation on object security attributes.	o Standard contents (see above) o The identity of the user that caused the event.	o Query_log o Diag_log also records failures with detail on the reason for failure.	o Query_log - Operations requested o Diag_log - Operations refused.
(FIA_UAU.1) Use of the authentication mechanism	o Standard contents o The identity of the user that caused the event.	o Alert_log - console authentication Network interface authentication errors o Summary_log – DXserver authentication o Connect_log – connects and disconnects by identity	o Console Authentication activity and Network interface authentication errors (alert_log) o Network interface authentication activity - Summary_log - Summary of daily activity o Successful authentication or anonymous connections and disconnects.

Auditable Events from Secton 5, FAU_GEN.1	Audit Record Contents	Audit log file	FAU_SEL.1 Event Type
(FIA_UAU.5-1) The final decision on authentication	o Standard contents o The identify of the user that caused the event. o Must exclude all password information in the audit record.	o Alert_log records unsuccessful binds o Summary_log o Connect_log – connects and disconnects by identity and authentication level	Event types: o Authentication errors (alert_log) o Summary_log - Summary of daily activity o Successful authentication or anonymous connections and disconnects.
(FIA_UID.1) Unsuccessful use of the identification mechanism.	o Standard contents o The identify of the user that caused the event.	o Alert_log - console authentication Network interface authentication errors o Summary_log – DXserver authentication	o Console Authentication activity and Network interface authentication errors (alert_log) o Network interface authentication activity - Summary_log - Summary of daily activity
(FMT_MSA.1) 1. Modifications of the dynamic access control rules, stored in the repository. 2. Modifications of the static access control rules in the operating memory, by the local console	1. dynamic access control rules o Standard contents o The identify of the user that caused the event. 2. static rules: o Standard contents	1. dynamic access control rules o Update_log o Diag_log - Failures are recorded in more detail o Summary-log 2. static rules: None o Trace_log	1. dynamic o Update_log: add, delete, modify, and rename operations. o Diag_Log: rejected operations. o Summary-log - Summary of daily activity 2. static: o trace_log – diagnostic tracing.
(FMT_MTD.1-1) 1. Operations on the TSF data located in the repository. 2. Operations performed from the console on the the operating memory.	1. repository o Standard contents o The identity of the user that caused the event. 2. console o Standard contents	1. repository o Query_log o Diag_log also records failures with detail on the reason for failure. o Summary-log 2. console o Trace_log	1. repository o Query_log - Operations requested o Diag_log - Operations refused. o Summary-log - Summary of daily activity 2. console o trace_log – diagnostic tracing.

Auditable Events from Secton 5, FAU_GEN.1	Audit Record Contents	Audit log file	FAU_SEL.1 Event Type
o The DSP Bind (authentication process with trusted Peer DSA) success or failure.	o The identify of the user that caused the event.	Trace_log DSP binds are only recorded in the trace log (when x500 tracing is enabled).	DSP binds are only recorded in the trace_log which covers general events and is often used for diagnostic purposes.

6.1.2 Access Control over Repository Data

The TOE implements the X.501 simplified access control scheme over users accessing the TOE through the LDAP and DAP Directory interface, with the Bind operating being the initial process that establishes these sessions. It controls access to the repository DIB, i.e., the repository information entries, and repository information attribute types. The access control decision is based on the subject and object security attributes specified in FDP_ACF.1.1 and the rules specified in FDP_ACF.1.2.

The TOE uses access two sets of access control rules to define the access control policy: 1) 'static' access control rules and 2) 'dynamic access control rules'. The static access control rules are stored as text files in the DXserver configuration files, and the dynamic access control rules are stored in an attribute in the repository DIB. These rules are structured to provide administrative users a simplified version of the complex X.501 access control definitions. When making the access control decision the TOE maps the rules onto the X.501 prescriptive access control information items (ACIs) used in the X.501 decision function. The following provides more information on the attributes defined in FDP_ACF.1.1 and how they map to X.501.

6.1.2.1 Subject Security Attributes

- Distinguished Name (DN) – the unique identifier for the user. The DN is the attribute that is used for the definitive point in the access control decision (see Access Control Decision subsection below). The User Group or User Role attributes, below, in the access control rules, are to apply the same rule to many Distinguished names.
- User Groups - Groups provide a short-hand mechanism for specifying rules for a set of users. They are defined in the static access control configuration file along with the access control rules that use them. A group definition consists of a group name and a number of Distinguished Names of the members of the group. The static access control rules can refer to user group in the access control rule subject set.
- User Roles - users are defined as being a member of a role in the DIT. Role entries are created within the DIT of the directory, in a specified role subtree. The base of the role subtree is defined in a configuration file. A role entry contains the DN of the users who have that role. When a user authenticates to the directory the role subtree is searched for the users DN and the role entries that are returned are then used in access control decisions for that connection. Both dynamic and static rules can refer to roles as the subject requestor in the access control rule subject set.

- Authentication level – users authenticate, i.e., bind to the directory using either simple or ssl-auth authentication. The TOE maintains the method of the bind for the current session to be compared with access control rules during the access control decision, see Access Control Decision subsection below.
- Requested Operation Day and time – the TOE reads the time/date from the platform clock with the operation request, and then uses this timestamp during the access control decision to determine which access control rules apply, see Access Control Decision below.

6.1.2.2 Object Security Attributes:

The access control rule(s) are specified in FDP_ACF.1.1. As described above these rules include the static rules, defined in the configuration file, and the dynamic rules defined as attributes in the repository DIB. These rules are mapped to the X.501 access control information ACI elements, the following provides more information on this mapping.

- **objects for which the access control rule applies** – the distinguished name in the repository DIB used in the ACI rule object set.
- **subjects for which the access control rule applies** – the distinguished name of the subject requestor used in the rule subject set.
- **priority of the access control rule** – this maps to X.501 precedence. The priority is determined from the permissions; the following lists the permissions from highest priority to lowest priority, i.e., an access control rule with permission set to Superuser has the highest priority and an access control rule with permission set to Public user has the lowest priority:
    1) Superuser – highest priority
    2) Administrative user
    3) Protected item
    4) Registered user
    5) Public user – lowest priority.
- **permissions:** *Superuser, Administrator, Registered User, Public* defines whether access is allowed or denied for the requested operation. The following table provides a mapping for the TOE access control permissions to the X.501 permissions and then the tables below lists the X.501 permissions required for each Directory operation.

Table 6-3 – Mapping TOE access control permission to X.501 permissions

TOE access control permission	X.501 permission
Superuser	Browse, Export, Import, Modify, Rename, ReturnDN, Compare, FilterMatch, Add, DiscloseOnError, Read, Remove
Administrator	Browse, Export, Import, Modify, Rename, ReturnDN, Compare, FilterMatch, Add, DiscloseOnError, Read, Remove

TOE access control permission	X.501 permission
Registered User	Browse, Compare, FilterMatch, DiscloseOnError, and Read
Public	Browse, Compare, FilterMatch, DiscloseOnError, and Read

Table 6-4 – TOE Operations Permissions

Directory Operation	Permissions Required for 'Entry' Protected Item	Permissions Required for Attribute Type
Compare	Read	Compare for attribute type
Read	Read ReturnDN (only if an alias name is not available)	Read for each attribute type returned
List	Browse and ReturnDN for each subordinate	None
Search	Browse for each entry in scope of Search ReturnDN for each entry (only if an alias name is not available)	FilterMatch for each attribute type and value used to evaluate the filter Read for each attribute type returned
AddEntry	Add	Add for each attribute type
RemoveEntry	Remove	None
ModifyEntry	Modify	Add for all attribute types added Remove for all attribute types removed
ModifyDN	Rename if operation only modifies RDN else Export at old name and Import at new name	None

- **optional permissions**: *read, add, remove, modify, rename, all* provide a mechanism for changing the access control rule precedence. Optional permissions replace the implicit permissions, so if a rule specifies an admin-user with optional permissions = read, the subject has only read permissions, rather than all permission, however it will still have a higher precendence than 'registered user' (the permission with only read access). The following table provides a mapping of the optional permissions to the X.501 permissions.

Table 6-5 – TOE Optional Permission to X.501 Permissions

TOE optional permission	X.501 permission

TOE optional permission	X.501 permission
Read	Browse, Compare, discloseOnError, export, FilterMatch, Read, returnDN
Add	Browse, Compare, discloseOnError, export, FilterMatch, Read, returnDN, add, import
Remove	Browse, Compare, discloseOnError, export, FilterMatch, Read, returnDN, remove
Modify	Browse, Compare, discloseOnError, export, FilterMatch, Read, returnDN, modify
Rename	Browse, Compare, discloseOnError, export, FilterMatch, Read, returnDN, rename, import
All	Browse, Compare, discloseOnError, export, FilterMatch, Read, returnDN, add, remove, modify, rename, import

- **authentication level required** - Defines the authentication level at which the user must bind: ***simple***(Default) and ***ssl-auth.*** If no auth level is specified then the user can bind using simple or ssl-auth. If an auth-level is the user must bind using the specified authentication level, or be considered an anonymous user.

- **Validity period** defines the days of the week on which the rule is valid and the time range during those days. The default is any time.

6.1.2.3 The Access Control Decision

As defined in FDP_ACF.1.2, the access control decision made by first gathering all the relevant access control rules as specified in requirements specified in the element include two steps to the access control decision function. The first step gathers the access control rules from both the static access control configuration file, and by traversing the repository for relevant access control entries as specified in FDP_ACF.1.2 A. The TOE implements a single administrative domain, therefore the process only needs to traverse the repository once and the algorithm remains straightforward.

The second step is referred to as the Access Control Decision Function in X.501 and results in the access control decision to the user's LDAP and DAP requests to the repository. This function implements the requirements specified in FDP_ACF.1.2 B and C, and Figure 6.1 below represents the inputs and outputs to this process[1].

[1] Chadwick, D.W., 'Understanding X.500 – The Directory, Copyright 1994, http://sec.cs.kent.ac.uk/x500book/

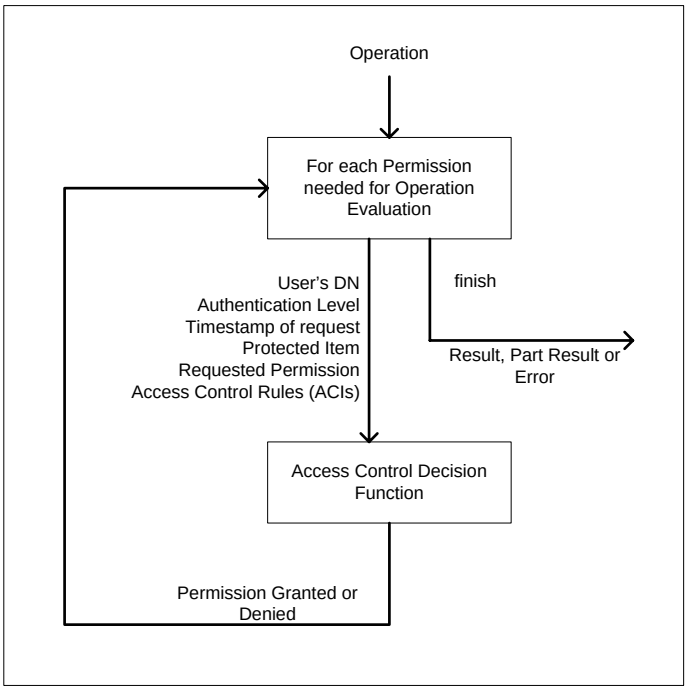

Figure 6.1 X.501 Access Control Decision

6.1.2.4 Anonymous Users Access

The requirement to deny anonymous users all access except read access is explicitly stated to clarify the mechanism to enforce this requirement, a common requirement for directory applications. For this TOE the mechanism is to specify 'public user' rules and DN = anonymous rules.

6.1.3 Identification and Authentication

The TOE requires and provides mechanisms for users to identify and authenticate themselves to the TOE before they can access the TOE data except for anonymous user Read access to public repository information in accordance with the CA Directory Access Control SFP.

Allowing anonymous users access to repository data is a necessary capability for many directory applications, e.g., as a component in a PKI system a directory may be required to make certificates available to relying parties of many external, and unforeseeable systems. The mechanism to allow anonymous users is the LDAP and DAP Bind process when no credentials are provided or only simple credentials are provided without a password (for instance, just a name). The DXserver accepts this Bind request and internally identifies these users as anonymous, resulting in effectively no identification or authentication required to access the 'public' data. An anonymous bind is accepted only when the minimum authentication level is 'none'.

The TOE provides the following authentication mechanisms, with the same rules applying to all users:

- Simple authentication (i.e., password-based): the user's Directory Bind request presents a distinguished name and password, the TOE verifies:

    1. the name corresponds to a real entry in the repository;
    2. that entry has a password attribute; and
    3. the supplied password matches it.

- Password authentication: similar to simple authentication, users authenticate to the local console with an identifier and password, the same ones as used for simple authentication. Through a configuration parameter in a TSF configuration file, the TSF enforces that only authorized superusers can authenticate to the local console. The following summarizes this mechanism:

    1. the TSF verifies the distinguished name is defined in the TSF configuration file as a DXconsole user;
    2. the name corresponds to a real entry in the repository;
    3. that entry has a password attribute; and
    4. the supplied password matches it.

- SASL authentication:

    1. an SSL connection is established between the user's DUA and the TOE, see 'Trusted Data Transmission security function below.
    2. the user presents a SSL bind request using their certificate, i.e., their personal certificate. For LDAP this is known as SASL/EXTERNAL, in X.500 it's known as 'Bind External Procedure. This tells the DXServer to use the certificate from the SSL connection (the link layer) for the authentication. An I&A mechanism in the IT environment ensures authorized access to the certificate on the DUA used in SASL.
    3. the DXServer verifies the entry named by the subject DN contained in the certificate exists an entry in the repository for the LDAP and DAP users, and verifies the DN name in its knowledge configuration file for remote trusted peers accessing through DSP and DISP requests .

- Distributed authentication via 'Peer DSA Password Check': A user can bind to the TOE when their entry (i.e., credentials) is held on a trusted peer DSA. During simple authentication, the TOE can forward the password check to the trusted peer DSA provided a trusted channel can be established between the TOE and the trusted peer DSA, and the correct trust-lags are set in the TOE configuration. The forwards the password check to the trusted peer DSA using the compare DAP/LDAP operation, if the result is 'compare confirm' the user is authenticated by the TOE, the bind is successful and the session is established.
- Distributed authentication via 'conveyed originator'. A user can bind to a trusted peer DSA and then have the trusted peer DSA convey the user's authentication to the TOE establishing a session for the authenticated user using the following process:

    1. A user binds to a trusted peer DSA. The bind request includes the user's DN, and the user's credentials.
    2. The trusted peer DSA authenticates the user.
    3. The user makes another request which the trusted peer DSA cannot fulfill.

4. The trusted peer DSA passes the request to the TOE. The request includes the user's DN and authentication.
5. The TOE, using its knowledge configuration file, verifies the trusted peer DSA is trusted to perform conveyed authentication. If accepted the user is considered authenticated by the TOE and uses the received DN to determine what access controls apply. The user, the subject of the conveyed authentication, is considered to be the same level of authentication as the trusted peer DSA, SSL, unless allow-downgrading or allow-upgrading is set.

(FIA_ATD.1) To support the above authentication mechanisms the TOE maintains the following user attributes: Distinguished Name, role, group and authentication password credential. For users accessing the TOE using DAP and LDAP the distinguished name is maintained in the repository as an entry in the DIB. For trusted remote peer DSAs the DN is maintained in the knowledge file. The password is maintained in the repository as an attribute of the DN and is hashed to obscure the entry. User certificates for SSL authentication are not stored in the directory the user binds to. A user supplies their certificate on a bind. The TOE then checks to see if it trusts the root certificate of the user's certificate. Passwords are maintained in the repository. The role attribute is also maintained in the repository, and the group attribute is maintained in the static access control configuration file.

6.1.4 Password Management

The TOE includes a password management function to support the simple (password-based), and local console password authentication mechanisms described above. The policy management function includes mechanisms to ensure the strength of the password (FIA_SOS.1) and an authentication failure mechanism (FIA_AFL.1) to help prevent unauthorized access using a brute force attack. Both mechanisms are implemented through the password policy that includes the following rules and parameters for password management. The password policy rules fall into two categories; password management and password constraints. The password management deals with the rules that apply to changing passwords and account management while the password constraints specify the password formatting rules.

Table 6-6 – Password Policy Rules

Rule	Description
Management Rules	
Required	
set password-policy	Enable password management
set password-retries	The number of consecutive failed logon attempts before a password is locked
set password-max-suspension	The number of seconds after which a locked password reactivates
set password-allow-ignore-expired	Setting this option enables a bypass of the expiration check of the password for entries that include the attribute dxPwdIgnoreExpire
set password-allow-ignore-suspend	Setting this option enables a bypass of the password-max-suspension time delay for entries that include the attribute dxPwdIgnoreSuspend
set password-age	The number of days for which a password will remain valid

Rule	Description
Recommended	
set password-history	Number of previous passwords to be checked against new passwords.
set password-last-use	The number of days a password remains valid if it is not used. If the value is exceeded then the password expires.
Others	
set password-min-age	Sets the number of days since a password was changed until it can be changed again (lockout period). Note: this exists to prevent people from changing their password many times to fill up the password history.
set password-allow-locking	Allows a users account to be locked. It only affects entries that include the attribute dxPwdLocked
password-enforce-quality-on-reset	ensure that when passwords are reset (modified under a different DN) that new passwords adhere to the password quality policy.
set password-force-change	Forces users to change their passwords after their passwords have been reset
set password-grace-logins	The maximum number of times a user can log in with their password after it has expired. The TOE records a timestamp of each grace authentication after a password has expired.
Constraint Rules	
Required	
set password-min-length	Sets the minimum length of a password.
set password-numeric	Sets the minimum number of numeric characters a password must contain.
set password-non-alpha-num	The minimum number of non-alphanumeric characters in the password
set password-uppercase	The minimum number of uppercase characters in the password
set password-lowercase	The minimum number of lowercase characters in the password
Recommended	
set password-alpha	The minimum number of alphabetic characters in the password
set password-max-repetition	The maximum number of single characters that can be repeated in a password
set password-username-substring	Determines whether the password can contain the users RDN value. If set to true the password cannot contain the value of the users last RDN
Others	
set password-max-length	The maximum length of a password
set password-non-alpha	Sets the minimum number of non-alphanumeric characters a password must contain.
set password-alpha-num	The minimum number of alphanumeric characters in the password
set password-min-length-repeated-substring	Sets the minimum length of substrings that will be checked. Only affects entries that include the attribute maxSubstrRep
set password-substring-attrs = attr1, attr2, ..;	Specifies attributes that cannot have its values contained in a password

6.1.5 Administration and Trusted Data Management

As specified in FMT_SMR.1 the TOE maintains the following roles: Superuser, Administrator, Registered User, and Trusted Peer DSA. The Administrative users that access the TOE through the DUA interface are implicitly defined through permissions granted to these users and the associated trusted data for the Administrative functions. Similarly, data manager and registered user roles are specified implicitly by the permissions granted to these users over specified trusted data. The Data Manager is a mechanism to delegate administrative privileges to users over a portion of the repository. The Trusted Peer DSA role and its users are specified through the TOE configuration knowledge file.

Administration and Trusted Data Management functions provide a means for superusers, Administrators, and Trusted Peer DSAs to manage the data necessary for secure operations of the TOE. This data resides in either the repository, in configuration files on the operating system of the TOE server, or in the operating memory of the TOE after being read from the configuration files.

Trusted Data in the Repository:

The trusted data that resides in the repository is accessed through the TOE standard directory interfaces defined by the DAP, LDAP, and DISP protocols. The superusers and administrators are able to access the repository data over a network connection using DAP or LDAP from a DUA interface in the IT environment. The local console includes a DAP DUA interface providing the same access as over a network connection. The remoted trusted peer DSAs access the repository data through the replication process over the DISP interface. The TOE configuration knowledge file specifies the DSAs and the portions of the repository for which they have replication agreements. These agreements provide the mechanism for controlling this access.

The DUA interface for the network access is specified as being in the environment to allow a variety of DUA interfaces for the evaluated configuration. The security functions specified for the TOE do not rely on the DUA to contribute to the security functions, all security functionality for managing the trusted data in the repository is provided by the TOE, except for the support required by the environment to maintain the integrity and when necessary the confidentiality of the transmitted data, see 'Partial Protected Data Transmission' security function below. The TOE uses the same access control mechanism as described above in the access control section, to meet the data management requirements for DAP and LDAP access to the trusted data maintained in the directory repository.

Trusted Data in TOE Memory from the Configuration Files:

The trusted data required to manage the static access control lists, Audit functions, Identification and Authentication mechanisms, Password Policy, Remote Trusted Peers and protected data transmission are managed using configuration files, as specified in FMT_MSA.1-2 and FMT_MTD.1-2. Some of this data is maintained in the operational memory of the TOE in a manner that's accessible to superusers via the local console interface. As specified in FMT_MTD.1-1 the TSF data in the memory that's accessible via the local console are: static access control rules, audit functions, and password policy.

The local console interface is the same interface for superusers as the one that accesses repository data via DAP, but it uses a separate interface to the DXserver to access its memory. These updates

take effect immediately, however the updates are lost when the DSA restarts. Note, Password Policy refers to the rules for failed authentication attempts and strength of secret requirements, this does not manage individual passwords, these are maintained in the repository.

Control of Security Attributes:

As specified in FMT_MSA.1-1, the administrative users are responsible for configuring the security attributes for the Directory SFP that controls this repository data access. The controls for the Directory access control mechanism exist in two places: the dynamic access control rules in the repository, and the static access control rules in the configuration files. Dynamic rules can be changed during run-time. The static rules are activated when the DXserver starts-up. As described above in the access control section the dynamic access control rules are access control lists for repository entries. The access control to these is the same mechanism as the Directory SFP where the superuser is responsible for defining the access and delegating control for portions of the repository as required. superuser via the local console are able to modify the static access control rules that exist in the configuration files and the dynamic access controls in the repository. However, the static access control modifications via the local console are lost when the DSA restarts. To modify the static access control rules so they are persistent when the DSA restarts a superuser must modify the files through the operating system (FMT_MSA.1-2). The superuser may view the combined active access control rules in its X.501 representation using the local console.

6.1.6 Partial Protected Data Transmission

The TOE DXserver includes mechanisms to enforce when the data transmitted to and from remote trusted peer DSAs, over the network, must be protected from unauthorized disclosure and modification. The DX server relies on the SSLD process in its IT environment to perform the SSL protocol with its associated encryption to process certificates for authenticating the end points of the communication channel and to encrypt the data.

The TOE is able to require DSP and DISP communication with a trusted peer DSA to be over a trusted channel using SSL through its configuration file, as specified above in management. For these protocols, SSL is implemented with mutual authentication, i.e. each end of the communication channel is authenticated to the other, using public key cryptography.

Users authenticating must initiate the bind request over an SSL trusted channel. The DXserver handles all its directory services (DAP, LDAP, DSP, and DISP protocols) through a single port in SSL-encrypted and unencrypted forms. When the DXserver determines that SSL encryption or decryption is required it passes the packets to the SSLD process to handle the operation. When a user attempts to create an authenticated bind without SSL, the DXserver will disallow the bind and return an error. Establishing the SSL trusted channel for the bind establishes the trusted channel for the user's entire session and serves to protected any trusted data transmitted during the session.

6.1.7 Partial TOE Self Protection

The TOE ensures that security protection enforcement functions are invoked and succeed before each function within its scope of control is allowed to proceed. The TOE's domain is the DXserver. All user operations are conducted in the context of an associated session. These sessions are allocated only after successful authentication, except for the local console which is under procedural

control. User operations are checked for conformance to the granted level of access, and rejected if not conformant. The sessions are destroyed when the corresponding user sessions end. The sessions are controlled by the access protocol, DAP, LDAP, DISP, and DISP. The trusted channel above in 'Partial Protected Data Transmission' ensures the integrity of the data controlling the sessions.

Since the TSF is software it relies on the IT environment OS and underlying hardware to ensure that the Operating System DAC Security Policy enforcement functions are invoked and succeed before each function within the Operating System's Scope of Control is allowed to proceed, and to support non-bypassability. To support non-bypassability, the system data files stored on the operating system are binary executables, this prevents any user from modifying the files, only the TSF generates the files during installation. Further protection is provided by the underlying assumption that the TOE is maintained in a physically secure environment with no untrusted users or software.

6.2 SOF Claims

The simple Bind and superuser console access password authentication mechanism used in 'Identification and Authentication' (Section 6.1.3) is realized by probabilistic or permutational mechanisms. Note: 'Password Management' (Section 6.1.4) provides functionality to ensure the passwords are difficult-to-guess and meet the SOF claim of medium.

6.3 Assurance Measures

The CA Directory satisfies the assurance requirements for Evaluation Assurance Level (EAL) 3.

The following items are provided as evaluation evidence to satisfy the EAL3 assurance requirements:

Table 6-7 – Assurance Requirements Evaluation Evidence

No.	Security Assurance Requirement	Description	How Satisfied
1	ACM_CAP.3	CM Documentation	CA eTrust Mooroolbark Lab CVS_CM_Plan-V1.doc CA eTrust Mooroolbark Lab CVS HTML .zip Scanned image of product.pdf
2	ACM_SCP.1	TOE CM coverage	Configuration Item List: eTrustDir-r8 1 0608 (build 942)-fileList.xls Directory listing of new cd.bmp Directory listing of new cd part2.bmp CA-Directory_ListOfDocuments.doc

No.	Security Assurance Requirement	Description	How Satisfied
3	ADO_DEL.1	Delivery Procedures	Distribution_Centers_Procedures_Manual-NorthAmerica-2004Mar01.doc DNload instructions for r8.1 0608 (build 942).doc Product_Submission_Form_(WI)-2003Dec18.doc Product_Submission_Form_Process_Flow.doc Preservation_of_Product_Procedure.doc
4	ADO_IGS.1	Installation, generation, and start-up procedures	CA eTrust Directory Guidance CC Supplement v1.0.doc eTrust™ Directory r8.1 Getting Started eTrust™ Directory r8.1 Release Summary eTrust™ Directory r8.1 Administrator Guide eTrust™ Directory r8.1 Reference Guide
5	ADV_FSP.1	Functional Specification	eTrust™ Directory r8.1 Administrator Guide eTrust™ Directory r8.1 Reference Guide eTrust Directory_ADVsupplementV1.0.doc
6	ADV_HLD.2	High-Level Design	eTrust Directory_ADVsupplementV1.0.doc
7	ADV_RCR.1	Representation Correspondence	eTrust Directory_ADVsupplementV1.0.doc
8	AGD_ADM.1	Administrator Guidance	CA eTrust Directory Guidance CC Supplement v1.0.doc eTrust™ Directory r8.1 Getting Started eTrust™ Directory r8.1 Release Summary eTrust™ Directory r8.1 Administrator Guide eTrust™ Directory r8.1 Reference Guide
9	AGD_USR.1	User Guidance	eTrust™ Directory r8.1 User Guide
10	ALC_DVS.1	Identification of security measures	CA Development Security Procedures Manual Evaluation Team Plan for a Site Visit for CA EAL3 Evaluation of eTrust OCSPro, eTrust Access Control and eTrust Directory, Version 1.1, February 22, 2005 Data Center Server Room Policies and Procedures.doc Guest_Registration_for_Employees.pdf Guest_Registration_for_Receptionists.pdf Guest_Registration_for_Security.pdf Password Policy - Effective 12152005.htm Wireless_Networking_Policy-2003Mar31.pdf eAC 8.0 LifeCycleDev.jpg

No.	Security Assurance Requirement	Description	How Satisfied
11	ATE_COV.2	Test Coverage Analysis	CA eTrust Directory Test Coverage Analysis v2.0.doc
12	ATE_DPT.1	Testing: high-level design	CA eTrust Directory Test Coverage Analysis v2.0.doc
13	ATE_FUN.1	Test Documentation	DeveloperTestPlan-V2-9.doc Tests Scripts Logs/Results from execution AuditLogVerification spreadsheet.
14	ATE_IND.2	TOE for Testing	TOE for Testing CA eTrust Directory r8.1 0608 (build 942) Test Plan and Report V1.0.
15	AVA_MSU.1	Misuse Analysis	eTrust™ Directory r8.1 Administrator Guide eTrust™ Directory r8.1 Reference CA eTrust Directory Guidance CC Supplement v1.0.doc eTrust Directory_ADVsupplementV1.0.doc ATE documentation
16	AVA_SOF.1	SOF Analysis	CADirectorySOFAnalysisv1.0.doc
17	AVA_VLA.1	Vulnerability Analysis	etrust Directory Vulnerability Analysis v1.0.doc eDirectory Vulnerability scan results (20061129).html Secunia - Vulnerability Report - eTrust Directory 8.x.htm

7 PP Claims

The CA Directory Security Target was not written to comply with any Protection Profile.

8 RATIONALE

8.1 Security Objectives Rationale

8.1.1 Threats Countered by the Objectives

Table 8-1 shows that all the identified threats to security are countered by Security Objectives for the TOE and environment. Rationale is provided for each threat below the table. There are no Organizational Policies defined for this ST.

Table 8-1 – All Threats to Security Countered

Policy/Threat/Assumption	TOE Objective	Rationale
T.UNIDENTIFIED_ACTIONS: The superuser may not have the ability to notice potential security violations, thus their ability to identify and take action against a possible security breach.	O.AUDIT: The TOE will detect and create records of superuser-defined security events.	O.AUDIT mitigates this threat by providing an audit mechanism to record security-related events. Additionally, a superuser can select which security events to include or exclude in the record, providing more control regarding the information that needs to read or processed.
	OE.AUDIT_ACCESS The IT environment will protect the audit records and provide a means for a superuser to access and read the audit information.	OE.AUDIT_ACCESS mitigates this threat by: • Protecting the audit records the TOE generates ensuring their integrity and they are only viewable by superusers; and • Providing a means for the users to view the audit information in a form that's readable useful towards identifying possible security breaches and having information to appropriately respond to the potential breach.
	OE.TIME: The IT Environment will work in concert with the TOE to provide a reliable time stamp for the TOE use.	OE.TIME ensures the platform on which the TOE operates provides a reliable timestamp for the audit records.
T.TSF_COMPROMISE: A user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).	O.PARTIAL_SELF_PROTECTION: The TSF will maintain a domain or its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.	O.PARTIAL_SELF_PROTECTION contributes to countering this threat by ensuring that the TSF can protect itself and its resources within its scope of control from external interference, tampering, or unauthorized disclosure through its own interfaces. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to resources under its control.
	O.MANAGE: The TOE will provide all the functions and facilities necessary to support the administrative users in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	O.MANAGE mitigates this attack by dictating who is able to view and modify TSF data, as well as the behavior of TSF functions.

Policy/Threat/Assumption	TOE Objective	Rationale
	O.PARTIAL_TRUSTEDCOMM: The TOE in concert with its IT Environment will provide a trusted channel using SSL between the TOE and its environment.	O.PARTIAL_TRUSTEDCOMM contributes to countering this threat by working in concert with its IT environment OE.PARTIAL_TRUSTEDCOMM to ensure authentication data and TSF data is not compromised in transit between the TOE and its remote users. The TOE enforces that a trusted channel is used for all communication with trusted peer DSAs, and it ensures all communication between itself and user DUAs is protected when the communication is initiated via a trusted channel.
	OE.PARTIAL_SELF_PROTECTION: The IT Environment will work in concert with the TOE to protect it from unauthorized modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within its scope of control.	OE.PARTIAL_SELF_PROTECTION works in concert with and compliments O.PARTIAL_SELF_PROTECTION by ensuring the IT environment provides the operating system and hardware platform aspects of protection. It also compliments O.MANAGE by providing access control and protection for TSF configuration files that reside on the operating system and require superusers to modify them through the operating interface to make changes that are persistent when the DSA restarts.
	OE.PARTIAL_TRUSTEDCOMM: The IT Environment will work in concert with the TOE will provide a trusted channel using SSL between the TOE and its environment.	OE.PARTIAL_TRUSTEDCOMM, please see O.PARTIAL_TRUSTEDCOMM.
T.UNAUTHORIZED_ACCESS: A user may gain access to user data for which they are not authorized according the TOE security policy.	O.MEDIATE: The TOE must protect user data in accordance with its security policy.	O.MEDIATE ensures that all access to user data is subject to mediation. The mediation mechanism is only available to authorized users and uses their identity to ensure control and appropriate access over the data.
	OE.TIME: The IT Environment will work in concert with the TOE to provide a reliable time stamp for the TOE use.	OE.TIME mitigates this threat by providing time to the TOE for its security policy that considers time and day of the week for its access control decisions.

Policy/Threat/Assumption	TOE Objective	Rationale
T.MASQUERADE: A user may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.TOE_ACCESS: The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objectives helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, unauthorized access is further prevented by providing an authentication failure mechanism that disables users' access for a superuser specified time.
	OE.DISTRIBUTED_AUTHENTICATION: The IT environment will provide authentication services to support 'conveyed originator' distributed directory authentication, and will provide a password check to support 'peer DSA password check' distributed directory authentication.	OE.DISTRIBUTED_AUTHENTICATION mitigates this threat by providing elements of the TOE distributed authentication mechanisms that must be provided by a remote trusted peer DSA when the TOE is operating as part of a larger directory system. Note: A.DIRECTORY_SYSTEM_SECURITY_POLICY_ENFORCEMENT ensures the remote trusted peer DSAs mechanisms are appropriate to mitigate this threat in the TOE's environment.
	OE.I&A: The IT environment will provide I&A mechanism(s) to control access to an account on the platform to provide access control to the TSF configuration and log files, and to control access to individual user certificates used for SASL authentication.	OE.I&A mitigates this threat by providing an identification and authentication mechanism to superusers accessing the TOE's platform, required to modify the TSF configuration and log files. Also an identification and authentication is required by the DUA to have to ensure only authorized access to the certificates used for the SASL authentication.

8.1.2 Assumptions Addressed

The table below shows that each identified assumption is countered by at least one security objective for non-IT environment objective. (Objectives for the IT environment correspond to requirements).

Table 8-2 - All Assumptions Addressed

Assumption	Objective	Rationale
A.DIRECTORY_SYSTEM_SECURITY_POLICY_ENFORCEMENT: It is assumed before enabling replication and/or distributed I&A mechanisms, a superuser must ensure that the appropriate level of trust has been established and that the I&A and/or access control security policies are understood and enforced.	ON.DIRECTORY_SYSTEM_SECURITY_POLICY_ENFORCEMENT: The Environment procedures will ensure that before enabling replication and/or distributed I&A mechanisms, a superuser must ensure that the appropriate level of trust has been established and that the I&A and/or access control security policies are understood and enforced.	A restatement of the assumption and therefore is suitable for covering the assumption.
A.INTEROP: The TSF and the user DUAs, remote trusted peers, and IT environment are configured for proper interoperation.	ON.INTEROP: The Environment procedures will ensure that the TSF and the user DUAs, remote trusted peers, and IT environment are configured for proper interoperation.	A restatement of the assumption and therefore is suitable for covering the assumption.
A.NO_EVIL: Trusted users are non-hostile, appropriately trained and follow all guidance.	ON.NO_EVIL: The Environment procedures will ensure trusted users are non-hostile, appropriately trained and follow all guidance.	A restatement of the assumption and therefore is suitable for covering the assumption.
A.NO_GENERAL_PURPOSE: The superuser ensures there are no untrusted users, no untrusted software, and no general–purpose computing or storage repository capability (e.g., compilers, editors, or user applications) available on the TOE.	ON.NO_GENERAL_PURPOSE: The environment procedures will ensure that there are no untrusted users, no untrusted software, and no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.	A restatement of the assumption and therefore is suitable for covering the assumption.
A.PHYSICAL: It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE, and as a part of the TOE the access to the local console will have appropriate physical security and procedures to ensure and monitor exclusive superuser access.	ON.PHYSICAL: The environment procedures will ensure that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE, and as a part of the TOE the access to the local console will have appropriate physical security and procedures to ensure and monitor exclusive superuser access.	A restatement of the assumption and therefore is suitable for covering the assumption.

Assumption	Objective	Rationale
A.REMOTE_ADMIN_DUA_ ENVIRONMENT: The end user will manage and protect the Administrative DUA in a manner that is commensurate with the value of the IT assets protected by the TOE.	ON.REMOTE_ADMIN_DUA_ENVIRONMENT: The environment procedures will ensure the accreditation process will ensure that the procuring organization will manage and protect the Administrative DUA in a manner that is commensurate with the value of the IT assets protected by the TOE.	A restatement of the assumption and therefore is suitable for covering the assumption.
A.USER: It is assumed that the users will protect their authentication data.	ON.USER: Environment procedures will ensure that the users will protect their authentication data.	A restatement of the assumption and therefore is suitable for covering the assumption.

8.1.3 All Objectives covered

The table below shows all the objective for the TOE and environment and their mapping to the Threats and Assumptions.

Table 8-3 Reverse Mapping of Security Objectives to Threats/Assumptions

No.	Objective	Assumption/Threat
1.	O.AUDIT	T.UNIDENTIFIED_ACTIONS
2.	O.MANAGE	T.TSF_COMPROMISE
3.	O.MEDIATE	T.UNAUTHORIZED_ACCESS
4.	O.TOE_ACCESS	T.MASQUERADE
5.	O.PARTIAL_SELF_PROTECTION	T.TSF_COMPROMISE
6.	O.PARTIAL_TRUSTEDCOMM	T.TSF_COMPROMISE
1E.	OE.AUDIT_ACCESS	T.UNIDENTIFIED_ACTIONS
2E	OE.DISTRIBUTED_AUTHENTICATION	T.MASQUERADE
3E	OE.I&A	T.MASQUERADE
4E.	OE.TIME	T.UNIDENTIFIED_ACTIONS
		T.UNAUTHORIZED_ACCESS
5E.	OE.PARTIAL_SELF_PROTECTION	T.TSF_COMPROMISE
6E.	OE.PARTIAL_TRUSTEDCOMM	T.TSF_COMPROMISE
1N.	ON.DIRECTORY_SYSTEM_ SECURITY_POLICY_ENFORCEMENT	A.DIRECTORY_SYSTEM SECURITY_POLICY_ENFORCEMENT
2N.	ON.INTEROP	A.INTEROP
3N.	ON.NO_EVIL	A.NO_EVIL
4N.	ON.NO_GENERAL_PURPOSE	A.NO_GENERAL_PURPOSE
5N.	ON.PHYSICAL	A.PHYSICAL
6N.	ON.REMOTE_ADMIN_DUA_ENVIRONMENT	A.REMOTE_ADMIN_DUA_ENVIRONMENT

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements for the TOE

The table below shows that all of the security objectives for the TOE are satisfied by at least one security functional requirement (SFR).

Table 8-4 - All Objectives for the TOE Met by Functional Requirements for the TOE

Item	Objective ID	SFR ID/Title	Rationale
1	O.AUDIT	FAU_GEN.1 Audit data generation	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that a superuser has the ability to audit security relevant events that take place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event, including the identity of the user who caused the auditable event for many of the events.
		FAU_SEL.1 Selective Audit	FAU_SEL.1 allows the superuser to configure which auditable events will be recorded in the audit trail. This provides the superuser with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the audit mechanism.
2	O.MANAGE	FMT_MSA.1-1 Management of security attributes (TOE)	FMT_MSA.1-1 requires that the TSF restricts the ability to manage security attributes with respect to the user data access control policy (FDP_ACC.1) to the administrative users. This requirement covers all attributes, however it requires the iteration for the IT environment (FMT_MSA.1-2) for more complete management control where the changes to the static access attributes are persistent when the DSA restarts.
		FMT_MTD.1-1 Management of TSF data (TOE)	FMT_MTD.1-1 requires that the ability to manipulate TOE data, including configuration data, is restricted to superusers and superuser-authorized users. This requirement covers all TSF data, however it requires the iteration for the IT environment (FMT_MTD.1-2) for more complete management control where the changes to the data in the configuration files are persistent when the DSA restarts.

Item	Objective ID	SFR ID/Title	Rationale
		FMT_SMF.1 Specification of management functions	FMT_SMF.1 defines the ability to perform the functions in FMT_MSA.1-1 and FMT_MTD.1-1.
		FMT_SMR.1 Security roles	FMT_SMR.1 defines the specific security roles for the administration, management, and use of the system.
3	O.MEDIATE	FDP_ACC.1 Subset access control	The FDP_ACC.1 and FDP_ACF.1 requirements were chosen to define the policies, the subjects, objects, and operations for how and when mediation of access to the user data takes place. FDP_ACC.1 specifies that the subjects under control of the policy are to be defined, and that all operations from DAP and LDAP sessions that involve access to the repository data are controlled by the policy.
		FDP_ACF.1 Security attribute based access control	FDP_ACF.1 details the manner in which the user data are to be protected. The basics called for by the requirement is to match a set of attributes associated with a subject to a set of “access control items” associated with the object they wish to access; all applicable ACIs need to grant access in order for the subject to perform the operation on the object. The details of how the ACIs are collected and the specific operations supported are specified in FDP_ACF.1.2 , and with the attributes define the security policy to be enforced. Setting the attributes (implementing the security policy) is an administrative function.

Item	Objective ID	SFR ID/Title	Rationale
4	O. PARTIAL_SELF_PROTECTION	FPT_RVM_EXP.1-1 Partial Non-bypassability of the TSP by the TOE	FPT_RVM_EXP_TSF.1 ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies. Without this non-bypassability requirement, the TSF could not be relied upon to completely enforce the security policies, since interfaces may otherwise exist that would provide a user with access to TOE resources regardless of the defined policies. This includes controlling the accessibility to interfaces, as well as what access control is provided within the interfaces. The explicitly specified version is used to distinguish the aspects of FPT_RVM provided by the TOE vs. the aspects provided by the IT environment.
		FPT_SEP_EXP_TSF.1 Partial TSF domain separation by the TOE	FTP_SEP_EXP_TSF.1 ensures the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version is used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment.
5	O. TOE_ACCESS	FIA_AFL.1 Authentication failure handling	FIA_AFL.1 requires the TOE to disable the account for the superuser-specified period of time, e.g., 2 hours when an superuser-specified number of failed password authentication attempts occur. This protection helps prevent brute force attacks for unauthorized access.
		FIA_ATD.1 User attribute definition	FIA_ATD.1 defines the attributes of users, including userid that is used by the TOE to determine a user's identity and the association between userid and role(s) and groups, and the user's authentication data for password access. These attributes provide control over individual users access. This requirement also allows a human user to have more than one user identity assigned, so that a single human user could assume all the roles necessary to manage the TOE.

Item	Objective ID	SFR ID/Title	Rationale
		FIA_SOS.1 Verification of secrets	FIA_SOS.1 provides a mechanism to ensure passwords meet requirements to support an organization's security policy and the strength of function for the password authentication mechanism.
		FIA_UAU.1 Timing of authentication	FIA_UAU.1 requires users to be authenticated before accessing the TOE as a mechanism to control the logical access to the TOE. An exception to this is access for anonymous users who are allowed access to portions of the repository data as specified by O.MEDIATE. This is necessary to support some systems, e.g., PKI's require directories to disseminate certificate and CRLs to the public or unregistered users.
		FIA_UAU.5-1 Multiple authentication mechanisms (TOE)	FIA_UAU.5-1 requires the TOE to support multiple authentication mechanisms. This allows superusers to specify the appropriate mechanism for their environment and provides the multiple mechanism typically required for a Directory to authenticate remote trusted peers and for distributed authentication mechanisms for distributed directory systems.
		FIA_UID.1 Timing of identification	FIA_UID.1 is similar to FIA_UAU.1 and provides the identification portion of the I&A mechanism.
6	O.PARTIAL_TRUSTEDCOMM	FTP_ITC_EXP_TOE.1 Partial Inter-TSF trusted channel by the TOE	FTP_ITC_EXP_TOE.1 requires the TOE to work in concert with the IT environment to provide a trusted channel using SSL for the specified operations: all communication between itself and a trusted peer DSA, and all communication initiated by users via trusted channel. As specified in OE.PARTIAL_TRUSTEDCOMM all users must initiate communication with the TOE when transmitting authentication and other trusted data. The TOE is responsible enforcing the requirement to use a trusted channel for all communication with trusted peer DSAs It relies on the SSLD process in its IT environment to implement SSL, providing the cryptographic support to process certificates for authentication and to encrypt the data to protect if from unauthorized disclosure or modification.

8.2.2 All TOE Security Functional Requirements covered

The table below shows all the Security Functional Requirements for the TOE their mapping to the TOE Objectives.

.

Table 8-5 Reverse Mapping of TOE SFRs to TOE Security Objectives

No.	Functional Component ID	TOE Security Objective
1.	FAU_GEN.1	O.AUDIT
2.	FAU_SEL.1	O.AUDIT
3.	FDP_ACC.1	O.MEDIATE
4.	FDP_ACF.1	O.MEDIATE
5.	FIA_AFL.1	O. TOE_ACCESS
6.	FIA_ATD.1	O. TOE_ACCESS
7.	FIA_SOS.1	O. TOE_ACCESS
8.	FIA_UAU.1	O. TOE_ACCESS
9.	FIA_UAU.5-1	O. TOE_ACCESS
10.	FIA_UID.1	O. TOE_ACCESS
11.	FMT_MSA.1-1	O.MANAGE
12.	FMT_MTD.1-1	O.MANAGE
13.	FMT_SMF.1	O.MANAGE
14.	FMT_SMR.1	O.MANAGE
15.	FPT_RVM_EXP_TSF.1	O. PARTIAL_SELF_PROTECTION
16.	FPT_SEP_EXP_TSF.1	O. PARTIAL_SELF_PROTECTION
17.	FTP_ITC_EXP_TOE.1	O.PARTIAL_TRUSTEDCOMM

8.2.3 Dependencies

Table 8-6 below shows the dependencies between the functional requirements. All CC defined dependencies are satisfied except one where an explanation is provided for why the dependency is not necessary.

Table 8-6 TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	IT Environment
2	FAU_SEL.1	Selective audit	FAU_GEN.1	1
			FMT_MTD.1	12

Item	SFR ID	SFR Title	Dependencies	Item Reference
3	FDP_ACC.1	Subset access control	FDP_ACF.1	4
4	FDP_ACF.1	Security attribute based access control	FDP_ACC.1	3
			FMT_MSA.3	N/A – This dependency is not applicable for this TOE since restrictive default values for the SFP is already required in FDP_ACF.1, and the ST does not allow the default to be changed. This rationale is consistent with the Directory PP.
5	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	8
6	FIA_ATD.1	User attribute definition	None	None
7	FIA_SOS.1	Verification of secrets	None	None
8	FIA_UAU.1	Timing of authentication	FIA_UID.1	10
9	FIA_UAU.5-1	Multiple authentication mechanisms	None	None
10	FIA_UID.1	Timing of identification	None	None
11	FMT_MSA.1-1	Management of security attributes (TOE)	FDP_ACC.1	3
			FMT_SMF.1	13
			FMT_SMR.1	14
12	FMT_MTD.1-1	Management of TSF data (TOE)	FMT_SMF.1	13
			FMT_SMR.1	14
13	FMT_SMF.1	Specification of management functions	None	None
14	FMT_SMR.1	Security roles	FIA_UID.1	10
15	FPT_RVM_EXP_TSF.1	Partial Non-bypassability of the TSP by the TOE	None	None
16	FPT_SEP_EXP_TSF.1	Partial TSF domain separation by the TOE	None	None
17	FTP_ITC_EXP_TOE.1	Partial Inter-TSF trusted channel by the TOE	None	None
1E.	FAU_SAR.1	Audit Review	FAU_GEN.1	1
2E	FIA_UAU.2	User authentication before any action	FIA_UID.1	4E(H)

Item	SFR ID	SFR Title	Dependencies	Item Reference
3E	FIA_UAU.5-2	Multiple authentication mechanisms (IT environment)	None	
4E	FIA_UID.2	User identification before any action	None	
5E.	FMT_MSA.1-2	Management of security attributes (IT environment)	FDP_ACC.1	3
			FMT_SMF.1	N/A – this dependency is not applicable for the environment for this TOE since all the management functions required by the IT environment are implicit in the FMT_MSA.1-2 requirement.
			FMT_SMR.1	N/A – this dependency is not applicable as a requirement for the IT environment of this TOE since the IT environment does not maintain the roles, e.g., a role may be implicit by access, or may be controlled through procedural controls.
6E.	FMT_MTD.1-2	Management of TSF data (IT environment)	FMT_SMF.1	N/A – this dependency is not applicable for the environment for this TOE since all the management functions required by the IT environment are implicit in the FMT_MTD.1-2 requirement.
			FMT_SMR.1	N/A – this dependency is not applicable as a requirement for the IT environment of this TOE since the IT environment does not maintain the roles, e.g., a role may be implicit by access, or may be controlled through procedural controls.
7E.	FPT_RVM_EXP_PFM.1	Partial Non-bypassability of the TSP by the platform	None	None
8E.	FPT_SEP_EXP_PFM.1	Partial TSF domain separation by the platform	None	None
9E.	FPT_STM.1	Reliable time stamps	None	None
10E.	FTP_ITC_EXP_ENV.1	Partial Inter-TSF trusted channel by the IT environment	None	None

8.2.4 Rationale for Dependencies not Satisfied

As stated in the table above: for FMT_MSA.1 regarding its dependency on FMT_MSA.3, this dependency is not applicable for this TOE since restrictive default values for the SFP is already required in FDP_ACF.1, and the ST does not allow the default to be changed. The dependencies for FMT_SMF.1 in the IT Environment requirements are not specified for the IT environment because their function is implicit in their FMT requirements. These are consistent with the Directory PP. The FMT_SMR.1 dependencies in the IT Environment requirements are not specified for the IT Environment since it's not necessary for the roles to be maintained in the environment by IT mechanisms, they can be controlled through procedural controls.

8.2.5 Strength of Function Rationale

Part 1 of the CC defines "strength of function" in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-medium is the strength of function level chosen for this ST. SOF-medium states, "A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential."

The rationale for choosing SOF-medium was to be consistent with the assurance requirements included in this ST; namely the environment is one where the potential attacker is proficient with access to specialized equipment and public information, consistent with a Common Criteria Level of Evaluation of EAL3. Specifically, AVA_VLA.1 requires that the TOE be resistant to an attacker with a low to moderate attack potential, this is consistent with SOF-medium. Consequently, the metrics (password) chosen for inclusion in this ST for this TOE were determined to be acceptable for SOF-medium.

The one security function based on probabilistic methods is identified in Section 6.1.3, Identification and Authentication and applies to FIA_UAU.5-1. This is constrained by the Password Management function identified in Section 6.1.4 and applies to FIA_AFL.1 and FIA_SOS.1. The specific "strength" required of the methods used provide difficult-to-guess passwords.

8.2.6 Evaluation Assurance Level Rationale

Evaluation Assurance Level (EAL) 3 was chosen because it provides appropriate assurance measures for the expected application of the product. EAL3 was selected because the TOE requires a moderate level of independently assured security and requires a thorough investigation of the TOE and its development without substantial re-engineering.

8.2.7 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, FAU_GEN.1, Audit data generation, details auditable events generated by the TSF and consistent with the security functions claimed by the TOE, and FAU_SEL.1 specifies selectable events that are consistent with the audit records being generated. The IT environment provides

protection of these audit records in FMT_MTD.1-2 and a facility to read or process the records in FAU_SAR.1, and reliable time stamps required in FPT_STM.1. Since most directory implementations are a part of a larger system, providing a means to process the records outside of the TOE is reasonable.

FIA_ATD.1, User attribute definition, specifies the security attributes belonging to individual users. FIA_SOS.1, Verification of secrets, supports strong authenticators with FIA_AFL.1 providing for the disabling of a user account after a specified number of invalid login attempts have been made.

Together FDP_ACC.1 and FDP_ACF.1 provide User Data Protection by defining the Directory Access Control Policy. They specify that the TSF controls user access to controlled resources based upon rules and security attributes. These requirements are supported by FIA_ATD.1 which specifies the user attributes needed to enforce the policy, this also specifies attributes required to identify and authenticate users in FIA_UAU.1, FIA_UAU.5, FIA_UID.1.

The TOE partial self-protection requirements, FPT_RVM_EXP_TSF.1 and FPT_SEP_EXP_TSF.1 apply to the entire TOE, and the partial protected data transmission requirement, FTP_ITC_EXP_TOE.1 applies to all the data transmitted between the TOE and its users.

FMT_MTD.1-1, FMT_MSA.1-1, FMT_MTD.1-2 and FMT_MSA.1-2 specifies the Management of TSF data and attributes according to assigned roles, as defined in FMT_SMR.1. FMT_SMF.1, Specification of management functions, specifies the security management functions of the TSF.

The following table shows the management specifications are complete and consistent with the requirements:

Table 8-7 Management Specifications Complete

ST Functional Component ID	CC recommendation	Application in ST
FAU_GEN.1	none	N/A
FAU_SEL.1	Maintenance of rights to view/modify the audit events	Only the superuser at console can view/modify, however the TSF restricts the ability to view and modify the events to the superuser at the Console.
FDP_ACC.1	none	N/A
FDP_ACF.1	Managing the attributes used to make explicit access or denial based decisions	See requirement.
FIA_AFL.1	1. Management for the threshold for unsuccessful authentication attempts 2. Management of actions to be taken in the event of an authentication failure.	Console commands

ST Functional Component ID	CC recommendation	Application in ST
FIA_ATD.1	If so indicated in the assignment, the authorized administrator might be able to define additional security attributes for users.	Not applicable, the superuser is not required to be able to define additional security attributes for users.
FIA_SOS.1	The management of the metric used to verify secrets	Console commands
FIA_UAU.1	1. Management of the authentication data by the administrator 2. Management of the authentication data by the associated user, 3. Managing the list of actions that can be taken before the user is authenticated.	1. included - in repository 2. included - in repository 3. Superuser at console by setting the minimum authentication level that allows anonymous users.
FIA_UAU.5-1	1. The management of the authentication mechanisms 2. the management of the rules for authentication	Console for both.
FIA_UID.1	1. the management of the user identities 2. if an authorized administrator can change the actions allowed before identification, the managing of the action lists.	1. included – DN for password and DAP and LDAP in repository Console - DN for DSP and DISP in knowledge file 2. Superuser at console by setting the minimum authentication level that allows anonymous users
FMT_MSA.1-1	Managing the group of roles that can interact with the security attributes	Superuser
FMT_MTD.1-1	Managing the group of roles that can interact with the TSF data	Superuser
FMT_SMF.1	None	N/A
FMT_SMR.1	Managing the group of users that are part of a role.	Superuser
FPT_RVM_EXP_TSF.1	(based on FPT_RVM.1) None	N/A
FPT_SEP_EXP_TSF.1	(based on FPT_SEP.1) None	N/A
FTP_ITC_EXP_TOE.1	(based on FTP_ITC) Configuring the actions that require a trusted channel.	Superuser at the console

8.2.8 Explicitly Stated Requirements Rationale

The table below presents the rationale for each of the explicit requirements found in this ST. All the explicit requirements are closely modeled on existing CC requirements.

Table 8.8 – Rationale for Explicit Requirements

Explicit Requirement	Identifier	Rationale
FPT_RVM_EXP_TSF.1	Partial Non-bypassability of TSP by the TOE	NIAP policy requires software-only TOEs to use explicit requirements to specify the aspects provided by the TOE and those provided by the platform. The current reference for this policy is documents: 'TOE Protection, March 12, 2005', and 'CCEVS Policy on Accepting Security Target, April 8, 2005' The requirement is modeled on FPT_RVM.1 and modified to reflect to cooperative relationship between the TOE and its platform. As with FPT_RVM.1 this explicit requirement has no dependencies.
FPT_SEP_EXP_TSF.1	Partial TSF domain separation by the TOE	NIAP policy requires software-only TOEs to use explicit requirements to specify the aspects provided by the TOE and those provided by the platform. The current reference for this policy is documents: 'TOE Protection, March 12, 2005', and 'CCEVS Policy on Accepting Security Target, April 8, 2005' The requirement is modeled on FPT_SEP.1 and modified to reflect to cooperative relationship between the TOE and its platform. As with FPT_SEP.1 this explicit requirement has no dependencies.

Explicit Requirement	Identifier	Rationale
FTP_ITC_EXP_TOE.1	Partial Inter-TSF trusted channel by the TOE	Since the TOE does not implement all aspects of the trusted channel requirement FTP_ITC.1 and requires mechanisms from the IT environment, the functionality provided by the TOE is explicitly stated and the functionality for the environment is explicitly stated. The ST explicitly states these rather than iterating the requirements based on the NIAP policy that requires software-only TOEs to use explicit requirements to specify the aspects provided by the TOE and those provided by the platform. The current reference for this policy is documents: 'TOE Protection, March 12, 2005', and 'CCEVS Policy on Accepting Security Target, April 8, 2005' The requirement is modeled on FTP_ITC.1 and modified to reflect to cooperative relationship between the TOE and the IT environment. As with FTP_ITC.1 this explicit requirement has no dependencies.
FPT_RVM_EXP_PFM.1	Partial Non-bypassability of the TSP by the platform	NIAP policy requires software-only TOEs to use explicit requirements to specify the aspects provided by the TOE and those provided by the platform. The current reference for this policy is documents: 'TOE Protection, March 12, 2005', and 'CCEVS Policy on Accepting Security Target, April 8, 2005' The requirement is modeled on FPT_RVM.1 and modified to reflect to cooperative relationship between the TOE and its platform. As with FPT_RVM.1 this explicit requirement has no dependencies.

Explicit Requirement	Identifier	Rationale
FPT_SEP_EXP_PFM.1	Partial TSF domain separation by the platform	NIAP policy requires software-only TOEs to use explicit requirements to specify the aspects provided by the TOE and those provided by the platform. The current reference for this policy is documents: 'TOE Protection, March 12, 2005', and 'CCEVS Policy on Accepting Security Target, April 8, 2005' The requirement is modeled on FPT_SEP.1 and modified to reflect to cooperative relationship between the TOE and its platform. As with FPT_SEP.1 this explicit requirement has no dependencies.
FTP_ITC_EXP_ENV.1	Partial Inter-TSF trusted channel by the IT environment	This requirement is the compliment for FTP_ITC_EXP_TOE specified above. Please see above entry for rationale.

8.2.9 Security Functional Requirements for the IT Environment

Table below shows that all of the security objectives for the IT environment are satisfied.

Table 8-9 - All Objectives for the IT Environment Met by Functional Requirements

Item	Objective	Requirement for the IT Environment	Rationale
1E	OE.AUDIT_ACCESS	FAU_SAR.1 Audit Review	FAU_SAR.1 requires the IT environment to provide a mechanism to read the audit log files.
		FMT_MTD.1-2 Management of TSF data (IT environment)	FMT_MTD.1-2 requires control to ensure authorized access to the audit log files that reside on the operating system, ensuring the log files are not modified and authorized users have access to read and process them.

Item	Objective	Requirement for the IT Environment	Rationale
2E	OE.DISTRIBUTED_AUTHENTICATION	FIA_UAU.5-2 Multiple authentication mechanisms (IT environment)	FIA_UAU.5-2 requires a remote trusted peer DSA to provide authentication services for the TOE's conveyed originator authentication mechanism, and to provide a password check for the TOE's peer DSA password check mechanism. Both of these TOE distributed authentication mechanism require a remote trusted peer DSA and support the TOE operating in a larger directory system.
3E	OE.I&A	FIA_UAU.2 User authentication before any action and FIA_UID.2 User identification before any action	FIA_UAU.2 and FIA_UID.2 require the operating platform to provide an I&A mechanism to control access to a platform account, required for access to the TOE's configuration and log files. Also, users are required to be identified and authenticated to ensure authorized access to the certificates used for SASL authentication.
4E	OE. PARTIAL_SELF_PROTECTION	FMT_MSA.1-2 Management of security attributes (IT environment)	FMT_MSA.1-2 requires control to ensure superuser access to static access control configuration files through the operating system to make changes that are persistent when the DSA restarts.
		FMT_MTD.1-2 Management of TSF data (IT environment)	FMT_MTD.1-2 requires control to ensure superuser access to configuration files through the operating system to make changes that are persistent when the DSA restarts.
		FPT_RVM_EXP_PFM.1 Partial Non-bypassability of the TSP by the platform	FPT_RVM_EXP_PFM.1 requires the Operating System's security policy enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.

Item	Objective	Requirement for the IT Environment	Rationale
		FPT_SEP_EXP_PFM.1 Partial TSF domain separation by the platform	FPT_SEP_EXP_PFM.1 requires the Operating System to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface. The IT environment must enforce separation between security domains of subjects in the Operating System's Scope of Control.
5E	OE.PARTIAL_TRUSTEDCOMM	FTP_ITC_EXP_ENV.1 Partial Inter-TSF trusted channel by the IT environment	FTP_ITC_EXP_ENV.1 requires the IT environment to work in concert with the TOE to provide a trusted channel using SSL, providing its side of mutual authentication, SSL and a cryptomodule. The end user must initiate communication with the TOE via a trusted channel to protect the authentication data (A.USERS) and any trusted data transmitted by trusted users.
6E	OE.TIME	FPT_STM.1 Reliable time stamps	FPT_STM.1 requires that time stamps be provided by the IT environment.

Note: This table has been provided for completeness to show that all security functional requirements map to at least on TOE Security Objective.

Table 8-10 Reverse Mapping of Environment SFRs to Environment Security Objectives

No.	Functional Component ID	Environment Security Objectives
1.	FAU_SAR.1	OE.AUDIT_ACCESS
2.	FIA_UAU.2	OE.I&A
3.	FIA_UAU.5-2	OE.DISTRIBUTED_AUTHENTICATION
4.	FIA_UID.2	OE.I&A

5.	FMT_MSA.1-2	OE. PARTIAL_SELF_PROTECTION
6.	FMT_MTD.1-2	OE.AUDIT_ACCESS
		OE. PARTIAL_SELF_PROTECTION
7.	FPT_RVM_EXP_PFM.1	OE. PARTIAL_SELF_PROTECTION
8.	FPT_SEP_EXP_PFM.1	OE. PARTIAL_SELF_PROTECTION
9.	FPT_STM.1	OE.TIME
10.	FTP_ITC_EXP_ENV.1	OE.PARTIAL_TRUSTEDCOMM

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions Rationale

Table below shows that the IT security functions in the TOE Summary Specification (TSS) implement all of the TOE Security Functional Requirements.

Table 8-11 - Mapping of the SFRs for the TOE to TOE Summary Specification

Item	SFR ID/Title	Item	TSF ID/Title	Rationale
1	FAU_GEN.1	1	Audit Generation and Selection	The logging mechanism in Audit Generation provides the required audit records.
2	FAU_SEL.1	1	Audit Generation and Selection	The interface available to turn on and off logging functions provides the required selection control.
3	FDP_ACC.1	2	Access Control over Repository Data	The inherent X.501 access control mechanism scope of control meets the requirements.
4	FDP_ACF.1	2	Access Control over Repository Data	The repository access control ACLs and static rules along with the X.501 decision function meets the access control policy requirements.
5	FIA_AFL.1	4	Password Management	The TOE password policy as specified in its configuration file provides the required control.
6	FIA_ATD.1	3	Identification and Authentication	The repository identification entry and role and password entry attributes along with the groups in the static access control rules provide the required level of control over individual user attributes.

Item	SFR ID/Title	Item	TSF ID/Title	Rationale
7	FIA_SOS.1	4	Password Management	Same as FIA_AFL.1
8	FIA_UAU.1	3	Identification and Authentication	The identification and authentication function requires all users to identify and authenticate themselves to the TOE before they can access the TOE data and services. There is one exception, Read access to public repository information for anonymous users.
9	FIA_UAU.5-1	3	Identification and Authentication	The Identification and authentication function through its configuration files and its password and certificate-based mechanism meets the requirements. In addition to support the TOE in a distributed directory environment the distributed authentication mechanisms meet the specified requirements.
10	FIA_UID.1	3	Identification and Authentication	Same as FIA_UAU.1
11	FMT_MSA.1-1	5	Administration and Trusted Data Management	The superuser console access and Administrative repository data access provides the interface for the required management control.
12	FMT_MTD.1-1	5	Administration and Trusted Data Management	Same as FMT_MTD.1-1
13	FMT_SMF.1	5	Administration and Trusted Data Management	The TOE provides the interface for the management functions to manage TSF data and security attributes as specified in FMT_MTD.1-1 and FMT_MSA.1-1, respectively.
14	FMT_SMR.1	5	Administration and Trusted Data Management	The TOE explicit roles specified in the repository and the implicit role from the superuser console provide the required role definitions.
15	FPT_RVM_EXP_TSF.1	7	Partial TOE Self Protection	The well-defined interfaces and TOE boundary meet the requirement.
16	FPT_SEP_EXP_TSF.1	7	Partial TOE Self Protection	The sessions within the scope of control of the TOE meet the requirement

Item	SFR ID/Title	Item	TSF ID/Title	Rationale
17	FTP_ITC_EXP_TOE.1	6	Partial Protected Data Transmission	The DXserver enforcement of the requirement for when a trusted channel is required and its role in authenticating the two end points of the trusted channel, using the SSLD process to provide the SSL protocol and cryptographic support, meet the requirement.
IT Environment SFRs required to support the TOE Security Functions				
FAU_SAR.1		1	Audit Generation and Selection	The ability to view the audit records is provided by the IT environment. The requirement to view the records is a practical aspect of the audit generation and selection function.
FIA_UAU.2		3	Identification and Authentication	The platform requires the superuser to successfully identify and authenticate themselves before allowing access to the TOE local console interface.
FIA_UID.2		3	Identification and Authentication	Same as FIA_UAU.2
FIA_UAU.5-2		3	Identification and Authentication	The trusted remote DSA provides authentication mechanisms for 'conveyed originator' distributed directory authentication, and will provides a password check for 'peer DSA password check' distributed directory authentication.
FPT_STM.1		1	Audit Generation and Selection	The Timestamp from the IT environment provides the timestamp required for the audit records.
		2	Access Control over Repository Data	The time from the IT environment provides the check for the access control rules that specify time and day.
FMT_MSA.1-2		5	Administration and Trusted Data Management	The IT Environment provides an interface to allow authorized access and prevent unauthorized access to the TOE configuration and data files required to be modified so changes can be persistent when the DSA restarts.

Item	SFR ID/Title	Item	TSF ID/Title	Rationale
FMT_MTD.1-2		5	Administration and Trusted Data Management	Same as FMT_MSA.1-2
FTP_ITC_EXP_ENV.1		6	Partial Protected Data Transmission	The SSLD process in the IT environment provides the SSL protocol to support the TOE requirements.
FPT_RVM_EXP_PFM.1		7	Partial TOE Self Protection	Since the TOE is software only, the IT environment operating system and hardware mechanism must support its operation.
FPT_SEP_EXP_PFM.1		7	Partial TOE Self Protection	Same as FPT_RVM_EXP_PFM.1

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements were satisfied. The rationale is provided in Table 8-12 below.

Table 8-12 – Assurance Requirements Evaluation Evidence

No.	Security Assurance Requirement	Description	How Satisfied	Rationale
1	ACM_CAP.3	CM Documentation	CA eTrust Mooroolbark Lab CVS_CM_Plan-V1.doc CA eTrust Mooroolbark Lab CVS HTML .zip Scanned image of product.pdf	Describes the access controls used to control access to configuration items. Describes the roles of individuals authorized to make changes to source code configuration items.
2	ACM_SCP.1	TOE CM coverage	Configuration Item List: eTrustDir-r8 1 0608 (build 942)-fileList.xls Directory listing of new cd.bmp Directory listing of new cd part2.bmp CA-Directory_ListOfDocuments.doc	Lists: o source code files and version numbers o design documents with version numbers o test documents with version numbers o user and administrator documentation with version numbers

No.	Security Assurance Requirement	Description	How Satisfied	Rationale
3	ADO_DEL.1	Delivery Procedures	Distribution_Centers_Procedures_Manual-NorthAmerica-2004Mar01.doc DNload instructions for r8.1 0608 (build 942).doc Product_Submission_Form_(WI)-2003Dec18.doc Product_Submission_Form_Process_Flow.doc Preservation_of_Product_Procedure.doc	Provides a description of all procedures that are necessary to maintain security when distributing TOE software to the user's site. Applicable across all phases of delivery from packaging, storage, distribution.
4	ADO_IGS.1	Installation, generation, and start-up procedures	CA eTrust Directory Guidance CC Supplement v1.0.doc eTrust™ Directory r8.1 Getting Started eTrust™ Directory r8.1 Release Summary eTrust™ Directory r8.1 Administrator Guide eTrust™ Directory r8.1 Reference Guide	Provides detailed instructions on how to configure and install TOE.
5	ADV_FSP.1	Functional Specification	eTrust™ Directory r8.1 Administrator Guide eTrust™ Directory r8.1 Reference Guide eTrust Directory_ADVsupplementV1.0.doc	Provides rationale that TSF is fully represented. Describes the TSF interfaces and TOE functionality.
6	ADV_HLD.2	High-Level Design	eTrust Directory_ADVsupplementV1.0.doc	Describes the TOE subsystems and their associated security functionality.
7	ADV_RCR.1	Representation Correspondence	eTrust Directory_ADVsupplementV1.0.doc	Provides the following two dimensional mappings: o TSS and functional specification; o Functional specification and high-level design.

No.	Security Assurance Requirement	Description	How Satisfied	Rationale
8	AGD_ADM.1	Administrator Guidance	CA eTrust Directory Guidance CC Supplement v1.0.doc eTrust™ Directory r8.1 Getting Started eTrust™ Directory r8.1 Release Summary eTrust™ Directory r8.1 Administrator Guide eTrust™ Directory r8.1 Reference Guide	Describes how to administer the TOE securely.
9	AGD_USR.1	User Guidance	eTrust™ Directory r8.1 User Guide	Describes the secure use of the TOE.
10	ALC_DVS.1	Identification of security measures	CA Development Security Procedures Manual Evaluation Team Plan for a Site Visit for CA EAL3 Evaluation of eTrust OCSPro, eTrust Access Control and eTrust Directory, Version 1.1, February 22, 2005 Data Center Server Room Policies and Procedures.doc Guest_Registration_for_Employees.pdf Guest_Registration_for_Receptionists.pdf Guest_Registration_for_Security.pdf Password Policy - Effective 12152005.htm Wireless_Networking_Policy-2003Mar31.pdf eAC 8.0 LifeCycleDev.jpg	Describes the physical, procedural, personnel, and other security measures necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
11	ATE_COV.2	Test Coverage Analysis	CA eTrust Directory Test Coverage Analysis v2.0.doc	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
12	ATE_DPT.1	Testing: high-level design	CA eTrust Directory Test Coverage Analysis v2.0.doc	Demonstrates that the TSF operates in accordance with its High-Level Design.

No.	Security Assurance Requirement	Description	How Satisfied	Rationale
13	ATE_FUN.1	Test Documentation	DeveloperTestPlan-V2-9.doc Tests Scripts Logs/Results from execution AuditLogVerification spreadsheet.	Test documentation includes test plans and procedures and expected and actual results.
14	ATE_IND.2	TOE for Testing	TOE for Testing CA eTrust Directory r8.1 0608 (build 942) Test Plan and Report V1.0.	The TOE will be provided for testing.
15	AVA_MSU.1	Misuse Analysis	eTrust™ Directory r8.1 Administrator Guide eTrust™ Directory r8.1 Reference CA eTrust Directory Guidance CC Supplement v1.0.doc eTrust Directory_ADVsupplementV1.0.doc ATE documentation	The guidance documentation shall be analyzed and demonstrated to be complete.
16	AVA_SOF.1	SOF Analysis	CADirectorySOFAnalysisv1.0.doc	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
17	AVA_VLA.1	Vulnerability Analysis	etrust Directory Vulnerability Analysis v1.0.doc eDirectory Vulnerability scan results (20061129).html Secunia - Vulnerability Report - eTrust Directory 8.x.htm	Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

9 ACRONYMS

ACI	Access Control Information Items
ADUA	Administrative Directory User Agent
AM	Assurance Maintenance
ANSI	American National Standards Institute
ARL	Authority Revocation List
CA	Certificate Authority
CC	Common Criteria [for IT Security Evaluation]
CIMC	Certificate Issuing and Management Component
CM	Configuration Management
CMA	Certificate Management Authority
CMIP	Common Management Information Protocol
CRL	Certificate Revocation List
DA	Directory Administrator
DAP	X.500 Directory Access Protocol
DES	Data Encryption Standard
DIB	Directory Information Base
DISA	Defense Information Services Agency
DIB	Directory Information Base
DISP	X.500 Directory Information Shadowing Protocol
DIT	Directory Information Tree
DN	Distinguished Name
DoD	Department of Defense
DSA	Directory System Agent
DSP	X.500 Directory System Protocol
DUA	Directory User Agent
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
I&A	Identification and Authentication
ID	Identifier
IP	Internet Protocol
IT	Information Technology
JRE	Java Runtime Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDUA	LDAP Directory User Agent
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Tests
NSA	National Security Agency
PKI	Public Key Infrastructure
PP	Protection Profile

RL	Revocation List
SASL	Simple Authentication and Security Layer
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer Protocol
SSLD	SSL Daemon
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDDI	Universal Description, Discovery, and Integration

10 References

Reference
Chadwick, D.W., 'Understanding X.500 – The Directory, Copyright 1994, http://sec.cs.kent.ac.uk/x500book/
Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-002, Version 2.2, January 2004.
*e*Trust™ Directory r8.1 Administrator Guide
*e*Trust™ Directory r8.1 CM Reference
*e*Trust™ Directory r8.1 User Guide
*e*Trust™ Directory r8.1 Getting Started
U.S. Department of Defense Directory Protection Profile for Medium Robustness Environments, Version 4.0, August 9, 2003