National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

CA Directory, r8.1 0608 (build 942)

for the Sun Solaris Platform

Report Number: CCEVS-VR-07-0040
Dated: April 30, 2007
Version: Version 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

Table of Figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the CA Directory r8.1 0608 (build 942) for the Sun Solaris platform only, a product of CA Inc. Islandia, NY.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The CA Directory is a directory software application, which 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.

The Target of Evaluation (TOE) includes the following components and interfaces. As specified below in the evaluated configuration, only the 'Directory Group' components (DXserver, DXconsole, DXadmind, and DXtools) are installed for the evaluation.

1. DXserver – the directory server software component:
   - Interface to untrusted users (referred to as relying parties) and remote trusted administrators and data managers using LDAP and DAP;
   - Interface to other DSAs (remoted trusted DSAs) using DSP for distributed authentication and DISP for replication;
   - Interface to local administrator console using local telnet.
2. Ingres database - for data storage, provides operational functionality but no security functionality for the security functions specified in this ST.
3. DXconsole – the administrator 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. Configuration and Log files – text files on the platform that co-reside with the DXserver

Important Note: The TOE does not equal the entire product. Some components such as DXmanager and DXadmind are 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. Therefore, they were scoped out of the TOE.

The SSLD component works with the CA Directory to provide SSL services that secure remote client-to- server communications, and server-to-server communications (trusted channels.) These SSL services include X.509 certificate-based authentication and encryption operations which provide the trusted channels with data confidentiality and integrity. The SSLD process itself is outside the scope of the evaluation and is considered part of the IT environment. However, the SSLD SSL services that are utilized by the TOE are within the scope of the evaluation. Therefore, the cryptographic algorithms performed within the SSLD component are out of scope and not verified by this evaluation.

Aspects of the following security functions are controlled / provided by the TOE in conjunction with its information technology (IT) environment:

1. Audit Generation and Selection
2. Access Control over Repository Data (the information the directory stores and manages for users)
3. Identification and Authentication
4. Password Management
5. Administration and Trusted Data Management
6. Partial Protected Data Transmission
7. Partial TOE Self Protection

The following are explicitly excluded from the TOE configuration, but are included in its IT environment:

1. The CA Directory SSLD process provides SSL authentication and cryptographic services for the directory certificate-based authentication and protected data transmission
2. Operating Platform (Sun Solaris 9 operating system only and hardware) to support and protect the TOE and its files, reliable timestamps, and identification and authentication 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

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during April 2007. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.2 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL3 from the Common Methodology for Information Technology Security Evaluation, Version 2.2, [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The Policy 10 review, Policy 13 review, and the initial VOR were not conducted as the eDirectory evaluation was started prior to the establishment of these policies.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) for CA Directory is contained within the document Security Target for CA Directory r8.1 0608 (build 942) [ST]. The ST has been shown to be compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of CC.

2. Identification

Target of Evaluation:	CA Directory r8.1 0608 (build 942) for the Sun Solaris platform
Evaluated Software:	CA Directory r8.1 0608 (build 942) for the Sun Solaris platform
Developer:	CA Inc. Islandia, NY.
CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive McLean, VA 22102-3305
Validation Team:	Jim Brosey, Lead Validator Olin Sibert, Senior Validator
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. A description of the principle security policies is as follows:

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.

A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

Class FAU: Audit Generation	
FAU_ GEN.1	Audit data generation
FAU_SEL.1	Selective audit
Class FDP: Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
Class FIA: Identification & Authentication	
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.5-1	Multiple authentication mechanisms
FIA_UID.1	Timing of identification
Class FMT: Security Management	
FMT_MSA.1-1	Management of security attributes (TOE)
FMT_MTD.1-1	Management of TSF data (TOE)
FMT_SMR.1	Security roles
FMT_SMF.1	Specification of Management Functions
Class FPT: Protection of TSF	
FPT_RVM_EXP_TSF.1	Partial Non-bypassability of the TSP by the TOE
FPT_SEP_EXP_TSF.1	Partial TSF domain separation by the TOE
Class FTP: Trusted Path/Channels	

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

IT Environment Security Functional Requirements

Class FAU: Audit Generation	
FAU_SAR.1	Audit review
Cass IFA: Identification and Authentication	
FIA_UAU.2	User authentication before any action
FIA_UAU.5-2	Multiple authentication mechanisms (IT environment)
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_MSA.1-2	Management of security attributes (IT Environment))
FMT_MTD.1-2	Management of TSF data (TOE)
Class FPT: Protection of TSF	
FPT_RVM_EXP_PFM.1	Partial Non-bypassability of the TSP by the platform
FPT_SEP_EXP_PFM.1	Partial TSF domain separation by the platform
FPT_STM.1	Reliable time stamps
Class FTP: Trusted Path/Channels	
FTP_ITC_EXP_ENV.1	Partial Inter-TSF trusted channel by the IT Environment

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL3 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

- Before enabling replication and/or distributed I&A mechanisms, the 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.
- The TSF and the user DUAs, remote trusted peers, and IT environment are configured for proper interoperation.
- Trusted users are non-hostile, appropriately trained and follow all guidance.
- 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.
- 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 Administrator access.
- 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.
- It is assumed that users will protect their authentication data

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL3 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL3 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” (as this term is defined in the CC and CEM) or “vulnerabilities” to objectives not claimed in the ST.
4. CA Directory depends on the IT environment:
    a. for protection of the audit records and provide a means for a superuser to access and read the audit information.
    b. 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.
    c. to provide a reliable time stamp for the TOE use.
    d. to 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
    e. to 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.

f. to work in concert with the TOE will provide a trusted channel using SSL between the TOE and its environment.

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

The CA Directory platform consists of the CA Directory server (DXserver), its supporting database (Ingres) and the administrator 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 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 provides only operational support to the DXserver and in its evaluated configuration 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 DXtools and JXplorer components are installed but are not used to provide the functionality specified in the ST.

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. *NOTE: Another instance of the DXserver was used 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.*

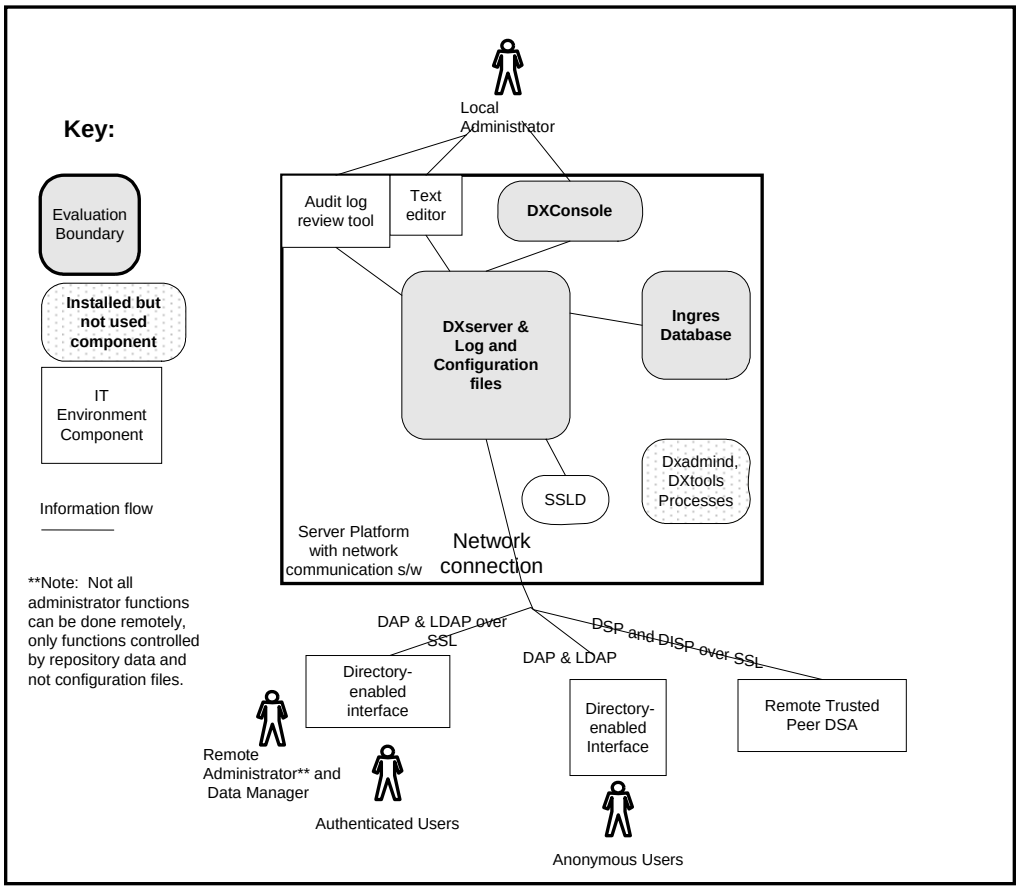

Figure 1. TOE Physical Boundary and the IT Environment

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- CA Directory r8.1 0608 (build 942) Security Target Version 2.6, dated April 29, 2007.
- *e*Trust™ Directory r8.1 Administrator Guide.
- eTrust™ Directory r8.1 0608 (build 942) Common Criteria Supplement For Administrator Guidance
- *e*Trust™ Directory r8.1 CM Reference
- *e*Trust™ Directory r8.1 User Guide
- *e*Trust™ Directory r8.1 Getting Started Guide.
- Release Notes r8.1 for build 942

7. IT Product Testing

At EAL3, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 3, the developer's test evidence must include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "must demonstrate that all security functions have been tested, and that all external interfaces to the TOE Security Function (TSF) have been tested.

7.1 Developer Testing

The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests (proven during independent testing). The evaluators determined that the developer's approach to testing the TSFs was appropriate for this EAL3 evaluation.
The overall goal of the CC test suite is to fully exercise the security features listed below. The coverage mapping between the evaluated security services and the test scripts is provided in CA eTrust™ Directory Test Coverage Analysis document.

Below is the configuration used for the Developers Testing. The TOE DSA box includes the Ingres db (in scope) and the SSLD (out of scope) though not depicted.

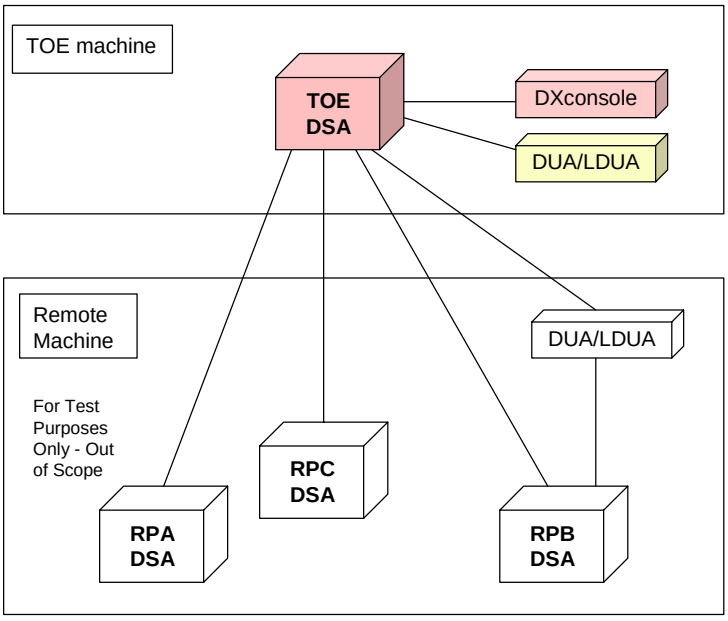

Figure 2. Testing Configuration.

The evaluator determined that the vendor successfully tested the security functions identified in Section 6.1 of the ST. The test coverage included:

- All the security-relevant functions of the product that were claimed in the ST
  - Audit Generation and Selection,
  - Access Control over Repository Data,
  - Identification and Authentication,
  - Security Management (including Password),
  - Partial protection of the TSF and
  - Partial Protected Data Transmission.
- Exercised all external interfaces.
  - DXconsole subsystem
    - Local Console: Operating Memory Management
    - Local Console: DAP
  - DXserver subsystem
    - Directory Network Interface
      - DAP
      - LDAP
      - DISP
      - DSP
  - Configuration files (tested for self protection only)

Several re-runs and iterations of the functional tests and re-verification of test results were required before the evaluation team was satisfied with the operation of the test harness, manual procedures, and the presentation of test results. The re-runs were NOT a result of bugs or deficiencies in the TOE functionality. However, they were required to meet the ATE_FUN, ATE_COV, and ATE_DPT work units. A thorough verification of the final developer's test and test results was accomplished by the evaluation team prior to entering into the independent testing exercise.

As a final note, it was discovered that the developer's original tests for DSA DSP SSL authentication failure handling were found to be insufficient. The evaluation team developed new test cases to take their place that did sufficiently test the requirement and ran these new tests (9a& 9b), instead of the original tests, during the independent testing exercise. The evaluator has also forwarded the test cases to the vendor for inclusion in their test plan.

7.2 Evaluator Independent Testing

The evaluator devised the test plan that included all the information needed for someone to be able to reproduce the tests. Each subdivision of tests included a section that talked about responsible individuals, applicable CEM units, required resources, evaluator procedures, test setup, tests, and a place to take notes and record actual results. The detailed information about the test and results is in *CA eTrust™ Directory r8.1 0608 (build 942) Test Plan and Report V1.0*. The following is an overview.

The evaluation team performed the following activities during testing:

1. Installation of the TOE in its evaluation configuration (ADO_IGS.1)
2. Verification of the TOE Installation and configuration (Encompasses all of the below)
3. Execution of all the developer's functional tests (ATE_IND.2)
    - ensure the coverage of the security features,
    - gain confidence in the developer's test results, and
    - ensuring TOE is in a properly configured state
    - Dropped original DSA DSP SSL authentication failure handling test cases
4. Independent Testing (ATE_IND.2)
    - **Test Independent 1:** Password-Retries Parameter Reset to 3
    - **Test Independent 2:** Add & Remove Security Role
    - **Test Independent 3:** DXconsole Modify Static Access Control Rules
    - **Test Independent 4:** Superuser Can Modify Dynamic Access Control Rules
    - **Test Independent 5:** Test 5 became obsolete due to version changes. Instead of renumbering all documents the test was just dropped.
    - **Test Independent 6:** Verify Pwd Authentication Mechanism – No access list
    - **Test Independent 7:** Verify Pwd Authentication Mechanism – List Added
    - **Test Independent 8:** Modify Static Access Control – Failure Case
    - **Test Independent 9A and 9B:** DSP SSL Authentication LDAP & DAP- Failure Case. Substitutes for the original DSA DSP SSL authentication failure handling vendor tests.
    - **Test Independent 10:** Domain Separation and Reference Mediation tests
    - **Test Independent 11:** Ingres Database Self Protection Test
5. Vulnerability Testing (AVA_VLA.1)
    - **Test Penetration 1:** Vulnerability Scan Against TOE Host Machine
    - **Test Penetration 2:** Verify Superuser Password Suspend (DXconsole)

The evaluator recorded and saved test results. The saved results include audit trails, vulnerability scans, directory listing, observed information into the Test Outcome section of the Test Plan and/or archived for each test. All raw information was saved into a separate location for later reviewing. The results of the automated tests were saved for reviewing between expected and actual results.

The evaluator chose to run all of the automated and manual test procedures that the developer used. This was chosen to ensure that all the security functions were thoroughly tested within the time frame allotted as well as the complicated nature of the product. Independent testing was minimized due to this decision.

The evaluator checked the actual results of the evaluation team run of the Developer's tests and found that the results did match the expected results. With the automated tests the evaluator relied on the developer's test reports/output logs to help in the comparison. The evaluator compared the evaluation team results to the developer team results using different tools to include unix diff tools, visual inspection, and ultra compare software product for windows. Visual ASCII text and Hex (Ultra Compare) verification was done when differences were found. Discrepancies or questions were then forwarded to the developer for explanation. All

discrepancies were satisfactorily answered by the vendor. Most of the differences were based on timing issues between the syncing of the TOE and remote database.

The independent tests were all run and the results validated successfully. These tests were devised to cover aspects of identification and authentication, security management, audit, partial TOE self protection, and partial protected data transmission. Independent tests 6, 7, 8, 9, 11 also were designed to cover vulnerability testing.

The evaluation team also ran a vulnerability scan using Nessus vulnerability scanner. The scanner The Vulnerability Scan by Nessus found 14 vulnerabilities: 1 high and 13 Medium:

- All of the Nessus found vulnerabilities are related to OS setup
- Evaluator verified with Developer that none of these identified vulnerabilities would have any affect on the product.
- Evaluator verified with Developer that the recommended changes required/recommended (by Nessus) to mitigate these vulnerabilities would not affect the operation of the TOE. The TOE does not use snmp, finger, telnet (telnetd), rsh, rexecd, multicast, or HTTP for this configuration.
- Developer provided a consolidated list of the ports required for TOE operation to support verification/assertion that the vulnerabilities would have no affect on the TOE directly.

Though none of the vulnerabilities were found to affect the TOE operation, the known vulnerabilities could be exploited to bypass the IT environments (OS) security policies and thus open up a vulnerability to the TOE. While these vulnerabilities are outside the scope of the evaluation, it is expected that the customer will install the OS in a secure manner, following the Solaris and Sun Sparc Administrator manual and Sun support website, install latest security critical patches to the operating system and database software, harden OS in accordance with the recommended procedures by Sun for the Solaris 9 OS, and close/disable all network ports that are not being used. The customer is advised to check the SUN support web site for any restrictions on specific patches to components of the IT environment.

Under unusual circumstances a patch to the TOE may also be required to address compatibility issues with a specific operating system or database patch. The customer is advised check the CA support web site for any restrictions on specific patches to components of the TOE.

The whole of the independent testing was successful based on the outcomes of the installation and successful identification of the correct TOE, developers test re-run results/verifications, independent tests results, and vulnerability test outcomes/mitigations.

7.3 Strength of Function

Strength of Function was demonstrated for the password-based authentication mechanisms to be SOF-medium, as defined in Part 1 of the CC. Specifically, the local authentication mechanism demonstrated adequate protection against attackers possessing a moderate attack potential. An overall SOF-medium rating is warranted as the TOE provides the identification and authentication mechanisms to protect the TSF data for all users (network interface) and administrative personnel (DXConsole interface).

The TOE depends on the strength of the passwords used to authenticate access by its users. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. The strength of function (SOF) requirement applies to the password based authentication mechanisms identified in FIA_UAU.5-1: part a) and b). This is constrained by the Password Management function identified in Section 6.1.4 of the ST and applies to the FIA_AFL.1 and FIA_SOS.1 SFRs. The password mechanism is the weakest authentication mechanism used for this TOE.

The TOE enforces a password policy that constrains passwords to a minimum of 8 characters with a mix of at lower case, upper case, numeric, and special characters (FIA.SOS.1). In addition, accounts are temporarily disabled for an administratively (superuser) defined lockout delay (1 minute or greater) after the failed login attempt threshold (5 or less) being achieved (FIA_AFL.1). This lockout delay is enforced on all users, including superuser, of the TOE. The SOF metric of resistance of greater than 1 month to password guessing attacks applies for this authentication mechanism.

7.4 Vulnerability Analysis

The developer, verified by the evaluator, searched for publicly known vulnerabilities specifically related to the TOE. There were 2 publicly-known vulnerabilities specific to the evaluated version of CA Directory were found. Both were found not relevant to the evaluated product as the evaluated configuration did not use the affected module or protocol.

The following public domain sources were used to identify and search for relevant vulnerabilities:

- Common Vulnerabilities and Exposures (CVE)
- Internet Search using Google
- National Vulnerability Database (NVD)
- CA Support Connect
- Security Focus

Two vulnerabilities discovered could possibly affect the TOE operation but were determined to not applicable. These are:

- CVE-2005-3653 iGateway affects the DXmanager module of eTrust Directory 8.1. DXmanager is not installed and out of scope for the evaluation. Also applies to the HTTP interface which is not an interface to the TOE.
- CVE-2004-0079 OpenSSL. V8.0 build 109 or higher has been built with OpenSSL 0.9.7d to avoid possible vulnerability via OpenSSL.

The assumed level of expertise of an attacker for all the threats is proficient with access to specialized equipment and public information. The specific threats that the TOE is designed to counter are listed in section 3.2.1 of the ST.

8. Evaluated Configuration

The evaluated version of the CA Directory is r8.1 0608, internally identified as build 8.1.942, for the Sun Solaris platform.

CA provides delivery of this product's components through the CA web site using the ESD process. Specific installation instructions for obtaining product are in the CC guidance supplement.

TOE and IT Environment components identification

	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;
Hardware	SUNW Ultra-250
	UltraSPARCII (2 CPUs) processor
	296MHz processor speed
	512MB (Physical Memory)
	(2- 8GB drive on an internal SCSI)
	CDRom drive

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.

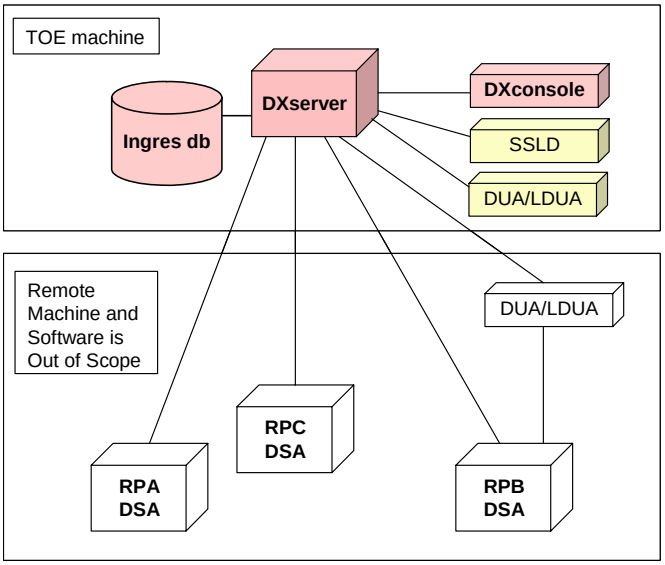

Figure 3. TOE's physical scope by product components used

9. Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 2.2 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL3 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_CAP.3	CM Documentation
ACM_SCP.1	CM Scope
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.2	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Life Cycle Support
ATE_COV.2	Test Coverage Analysis
ATE_DPT.1	Test Depth Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_MSU.1	Misuse Analysis
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

10. Validator Comments/Recommendations

The original CA Directory product was upgraded to a new software release (r8.1 SR8 vs r8.1 SR1) version during the evaluation. CA, when finalizing the product, changed the term SR8 to 0608 (build 942). Therefore, the product's official version is r8.1 0608 (build 942). The evaluators provided an analysis of the differences of the upgraded version. Each enhancement/fix was first analyzed to determine if it was security related. Each security related enhancement/fix was then analyzed as to what impact it had on all the documentation and evidence. All evidence was updated and re-evaluated prior to any of the ATE work units were started.

The version upgrade was customer driven, but did resolve a vulnerability issue identified during the SOF/VLA evaluation. The main security enhancement was the capability to enforce the superuser (eDirectory role) to authenticate prior to having access to the DXconsole from the local host platform. A second enhancement was the introduction of enforcing the time delay authentication failure handling on the superuser role. These enhancements, combined with the already existing authentication functionality of the TOE, fulfilled the requirements for the SOF-Medium claim.

CA also dropped the "eTrust" nomenclature of the product during the finalization of the evaluation. The ST, VR, and VPL were updated to reflect the product as CA Directory r8.1 0608 (build 942). However, references to vendor documents, evaluator developed reports (ETR and test report), and the evidence list contained in the ST, still contain the "CA eTrust" nomenclature to match the evidence that has been archived.

The validator wants to reiterate that the end user is responsible to harden OS in accordance with the recommended procedures by Sun for the Solaris 9 OS and close/disable all network ports that are not being used. The customer is advised to check the SUN support web site for any restrictions on specific patches to components of the IT environment. This guidance is also reflected in the CC Guidance Supplement.

In the evaluated configuration the superuser's security management functions requiring the use of the DXconsole can only be performed on the machine that the TOE is running on. The remote DXconsole support was disabled. Based on the evaluated configuration the ability to review the audit trail logs would technically need to be done accomplished on the TOE machine as well. This may be an unrealistic expectation for some environments. The end user could export the audit logs to removable media for verification on another machine or set up the OS to securely allow for the reviewing of the text files remotely. The end user is responsible to ensure that changes made to the OS, in support of the operational environment, don't impact the operational TOE and evaluate the associated risks that such changes may introduce.

The following is a summary of the discussion held at the FVOR about SSL use.

The SSL protocol utilizes Public Key Cryptography (PKI) which is based on the use of key pairs and X.509 certificates. Each key pair is comprised of a private key and a public key. The private key is known to and held by only by the owner of the key. The public key can be made publicly available to anyone and wrapped in an X.509 certificate.

The CA Directory server retains and manages its key pair at the server end. The client manages its keys at the client end. During SSL handshake operations, private keys are never sent over the wire. Public keys may be sent over the wire. The CA Directory Server product also includes a key generation application called the DXcertgen Tool. However, DXcertgen Tool and key generation are outside the scope of the evaluation.

11. Security Target

The Security Target for CA Directory r8.1 0608 (build 942) is titled *Security Target for CA Directory r8.1 0608 (build 942), Version 2.6* [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Criteria Evaluation Methodology
DAP	X.500 Directory Access Protocol
DBMS	Database Management System
DISP	X.500 Directory Information Shadowing Protocol
DSA	Directory System Agent
DSP	X.500 Directory System Protocol
DUA	Directory User Agent
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
I&A	Identification and Authentication
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LDUA	LDAP Directory User Agent
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OS	Operating System
PP	Protection Profile
SASL	Simple Authentication and Security Layer
SFR	Security Functional Requirement
SOF	Strength of Function
SSLD	SSL Daemon
ST	Security Target
TOE	Target of Evaluation
UDDI	Universal Description, Discovery, and Integration
VR	Validation Report

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://niap.nist.gov/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- CA Inc. (http://www.ca.com/).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004.
- [CCEVS3] Guidance to Validators of IT Security Evaluations, Version 1.0, February 2000.
- [CCEVS4] Guidance to Common Criteria Testing Laboratories, Draft, Version 1.0, March 2001.

Other Documents

- [ST] Security Target for CA Directory r8.1 0608 (build 942), Version 2.6, April 29, 2007.
- CA eTrust™ Directory r8.1 0608 (build 942) Common Criteria Supplement For Administrator Guidance Final V 1.0, dated April 13, 2007.
- Evaluation Technical Report for a Target of Evaluation Volume 1: Evaluation of the ST CA eTrust™ Directory version 8.1 0608 (build 942) for the Sun Solaris Platform Security Target Version 2.6, April 29 2007, ETR Version 2.2, April 29, 2007.
- EAL3 ON-SITE TESTING, Computer Associates eTrust™ Directory r8.1 0608 (build 942) For Sun Solaris Platform, EAL 3 Evaluation, Version 1.0 Final, April 26, 2007.