Full Service Directory

1. Introduction

A Full Service Directory (FSD)is a physically distributed, logically centralized repository of dynamic data that is used to manage the entire enterprise-computing environment. In order to develop an enterprise infrastructure, it is necessary to construct a strong set of directory services that serves as the foundation of the IT infrastructure. In the evolving IT environment, directories provide that point at which security, applications, and other network services converge to create a seamless distributed computing environment.

A FSD is required for users, applications, and network services to locate and utilize each other on the network. In a directory service, each object is identified and retrieved based upon identified attributes, one example being the name of the object. A FSD is a hierarchical database that will store system information, will support resources (e.g. white pages, PKI Certificate Repository), and the replication of data. It provides a simple means of naming, finding, accessing, and protecting resources over both space and time.

Full Service Directories allow centralized administration of networks and applications across integrated global geographically separated networks. The result is improved reliability, reduced administrative costs, and refined Quality of Service features such as Single-Sign-On Authentication. The successful deployment of an integrated DON IT environment requires the concept of developing and maintaining a centralized logical nerve center for the entire enterprise – i.e., a Full Service Directory.

2. The Current Environment

Currently, the Navy and Maine Corps computer networks are composed of hundreds, if not thousands of individual legacy networks. Command networks are seldom integrated from a command standpoint, let alone an integrated system that incorporates all the environments in which the Navy operates (In-Conus, Out-Conus, and Afloat Networks) across a Horizontally Integrated global network. The DON must be capable of incorporating current legacy systems with new architectures as they are deployed. It will be necessary for service providers to establish and manage a means to centrally manage Common Support Applications, Cooperative Work Applications, Mission Applications, and Application Support Services. Such a centralized Full Service Directory will not only integrate applications but the network hardware such as switches , to create a Directory Enabled Network within a the DON IT environment. There are commercial products with varying capabilities of providing this capability, alone or in coordination with other products.

3. Full Service Directory (FSD)

The concept of a FSD expands the role of a directory to enable every data object in the directory to be secured, monitored, controlled and automated. It becomes the repository of common enterprise information, providing an infrastructure that enables users to be identified and tracked throughout the enterprise, without having this information embedded into any one system. It should not be an application, or in the network, or in the firewall. This information is then accessed by all network, security and application services. For example, making security a core component of the infrastructure moves responsibility from many different applications into a single infrastructure that can be properly maintained and managed at reduced cost.

Perceived benefits of a Full Service Directory include:

Security	Elimination of numerous authentication and access mechanisms
Policy	Elimination of incremental policy implementation by individual departments
Quality of Service	Establishment of common business rules for access to data and applications
Administration	Reduced management and administration costs
Personalization	Establishes and maintains a single digital user profile for each user that fosters improved and seamless access to applications and systems across the enterprise.

The FSD is an "active" vs a "passive" environment that incorporates event driven functionality into the directory and is an essential component required for Directory-guided IT. A FSD automatically manages the relationships between objects, controlling how objects interact with other objects as well as the systems that use those objects. The directory schema must be global in nature and be scaleable to meet the needs of the Naval enterprise. Incorporation of a FSD into the Naval infrastructure will require the ability to integrate the FSD with other applications and directories. This includes, but is not limited to, combining many heterogeneous directories and applications into a single metadirectory infrastructure.

At the heart of the FSD is the concept of creating digital user constructs also known as a "digital persona". Digital persona contains information such as name, title, phone number, PKI Certificates, command, network access policies/parameters, etc. A digital persona can be used to define an individual's identity on the network based on geography, security, access privileges, and technical knowledge. Once created, depending on the type of network environments, digital persona allow users to roam from one PC to another while maintaining a familiar interface. Preferences such as menu choices and desktop configuration are associated with each individual's unique user profile rather than with specific workstations. Additionally, digital persona will control network assets such as priority of bandwidth and depending on the infrastructure, can even dictate the programs that a user has access to when they log into workstations.

The FSD should provide the following basic functions/services:

a) the ability to store network data in a hierarchical, distributed database providing centralized management and high levels of security;

b) the ability to separately manage components of the directory to provide for fault tolerance and acceptable levels of availability.

c) the ability for users, devices, applications, services, to discover and consume this data;

d) the ability to provide authentication and authorization to the data maintained in the FSD and also to other resources/services on the network;

e) the ability to proactively build and manage relationships between objects within the FSD. This would include the ability to find any object; group data based on (multiple) arbitrary hierarchies, and group objects into collections.

f) the ability to manipulate objects based on membership in any collection or hierarchy. These object relationships are created automatically;

g) the ability to administer and manage object metadata which is derived from the explicit ownership of the object, the object's participation in hierarchies that have explicit and inherited permissions (and based on rules and policies established for the object itself, within the directory) and for the hierarchies and collections to which that object claims membership.

h) the ability to enable location independence. This is defined as the ability for users to connect to the network from any computing device while maintaining their own personal preferences and settings for similar computing devices and applications. This includes the storage and replication on behalf of the user of application preferences, personal address books, bookmarks, profiles, security keys, and other services that provide a user specific environment. For application support, this would include the object's definitions, attributes, and methods. Distributed applications can be managed and modified centrally via the directory. Applications can find components by searching the directory instead of knowing the physical location of these components. The digital persona is one of the means by which location independence could be incorporated.

i) the ability to provide an integrated directory environment that supports industry initiatives (e.g. Directory Enabled Networking) and also comply with industry open standards (e.g. LDAP), and forward looking to proposed standards (e.g. DSML).

j) the ability to "transparently" integrate with the other DON directory service initiatives. This can be defined as the ability to connect with and copy/move/modify objects between the FSD and these DON directories.

k) the ability to integrate with other major commercial applications and directory tools such as PeopleSoft, SAP, Microsoft Exchange, Lotus Notes, Novell GroupWise, Netscape Enterprise Messaging Server.

the ability to support a Naval white pages service that will allow users within the DON environment to locate other users and retrieve information such as email addresses, PKI certificates, and phone numbers. The white pages shall be an integrated segment of the overall FSD.. Currently, this white pages service is being provided by the Navy/Marine Corps White Pages (N/MC-WP) directory. The N/MC-WP consists of several servers physically distributed in four key locations; NCTAMS LANT (Norfolk, VA), NCTAMS PAC (Wahiwa, HI), NCTAMS EURCENT (Naples, IT), SSC SD (San Diego, CA), and other potential shore sites. N/MC-WP servers will also be fielded to selected afloat units in CY00. The authoritative source for data in the N/MC-WP Directory originates from existing Navy and USMC Service/Clamancy email directories. A process and agreement is in place between the Program Office and the Authoritative Sources to consolidate and share directory data. Additionally, there is a MOA between the Navy and DISA that currently allows for a replication agreement between the DISA PKI Directory Server and the N/MC-WP Master Server for the purpose of replicating Naval employee PKI Certificate data from these DISA Servers to the N/MC-WP Master Server and subsequently merging this data with user objects in the N/MC-WP directory.

l) the ability to interoperate with other Services and Agencies. The FSD that is designed and built shall support industry standards based practices allowing inorganic directories to be merged and incorporated into the FSD as needed. Examples of this include US Air Force, Defense Information Services Agency (DISA), etc.

4. Product Consideration

The following requirements provide a more detailed description of the functions that should be exhibited in a FSD:

Requirement	Comments
1. Platform Availability	– Must be portable to multiple different operating systems including the most common ones such as Windows NT, Unix, Sun/Solaris, Linux, etc.
2. Product Deployment / Scalability	– Scalable to support large numbers of objects (~1 billion objects in a single directory database). – Should be a product that has proven operational performance.
3. Application/Protocol Support	– Ability to integrate industry standard protocols for developing directory including but not limited to: LDAP, ADSI, XML, HTTP, etc. – Support for Java and Java components (i.e. Java Beans)
4. Client Access	– Support for common client operating systems including but not limited to MS DOS, MS Win 3.1, MS Win 9X, MS Win 3.51/4.0, OS/2, Unix, Linux. – Common Standards supported (e.g. LDAP v2.0 & v3.0)

5. Directory Management	– Full-featured web enabled commercial tool set for directory and enterprise management. (e.g. SNMP, LDAP, and HTTP-Based management)
	– Desired administration capabilities:
	  – User access restricted by time, place, or connection method (e.g., Radius, VPN, etc)
	  – Drag and Drop movement of objects/rights within tree to other portions of the tree via directory

6. Database Manipulation	– Capability to:
	  – Post information to directory via policy set up by administrator
	  – Ability to dynamically publish directory information (e.g. HTML, XML/XLS)
	  – Support for self-service posting functions (e.g. control down to individual attribute level including users ability to add / remove themselves from lists without operator intervention.) E-business functions and self-service immediacy on web.
	  – Mechanism for change notification that survives name changes (e.g. receive changes from specific user after object is renamed) such as double backlinked objects including X.500 aliases

7. Data Retrieval Functionality	– Automatically direct and return queries to the correct database store. – Support for multiple access methods including LDAP, HTTP, ADSI, ODBC, XML.
8. Naming and Reference	– Guarantee that all names are globally unique including an automatic means to prevent developer and user

	mistakes in creating and using names – Support for aliases including surviving changes in the renaming of objects that the aliases reference. – Authentication via an alias – Automatically maintaining alias references when names change – Support for LDAP v3 including auxiliary classes, LDAP DNS (X.500), DC Component Naming (X.500)
9. Authentication	– Password must be verified without traversing wire unencrypted. – Support for multi-factor authentication (e.g. smart cards, certificates, biometrics, etc) – Support for grading authentication and limiting access based on access point (e.g. user properly logging in from airport kiosk may have limited access email, but not company database) – Support for DoD PKI X.509 v3 Certificate authentication – Support for authentication of external applications – Support for Single Sign On or minimally password synchronization – Support permitting the creation of new object types that can authenticate to the directory
10. Access Control	– Recognition of multiple levels of authority (e.g. users being supervisors over entire trees down to being supervisors of only one attribute of only one particular user) – Recognize boundaries of authority (e.g. down to directory container as the lowest level) – Ability for users to add themselves to a directory group without being an owner of the list and without being able to modify other user's membership – Should not have any access methods that circumvent the access control mechanism. – Support independent control of objects in the directory
11. Cryptographic Support	– Automatic issuance of key pairs – Include Public Key Infrastructure supporting X.509 and PKIS v2.0 – Support third party PKI Software (e.g. Entrust, Netscape, etc.) – Certificate Authority software along with ability to produce / mint certificates. – Seamless support for emerging cryptographic technologies (e.g. moving from RSA to Elliptic Curve without rewriting applications)

	– Support multiple key pairs for a given user. – Support for SSL RFC and LDAP Mandatory Authentication Mechanisms (Key Lengths) – Support for PKCS.
12. Auditability and Disaster Recovery	– Auditing operations protected and separated from administrative functions. – All operations in the directory are independently operated. – Audit information exportable. – Utility for configuring auditing policies. – Auditing system support for non-directory objects (e.g. file systems). – Directory has ability to be backed up, restored, while directory is online and functioning. – Auditing system is Orange Book compliant.
13. Database Integrity	– Provide transactional writes. – Ability to repair database while directory is operating / online. – Support name relationships. – Automatic protection for name relationships including circumvention via custom applications (e.g. prevent invalid name relationships from being created). – Support and automatic protection for external database name relationships. – Support for moving subtrees within the database.
14. Database Protection and Reliability	– Ability for directory database to be distributed. – Ability for distributed components (segments) to be rejoined without a limit on the number of segments. – Ability to authenticate to multiple servers. – Support for splitting instances of a datastore into multiple datastores. – Ability for joining separate directories (not to be confused with components). – Security policies are independent of segment boundaries. – Ability to conduct database distribution operations on operational databases. – Support replication of data. – Automatically direct queries to surviving copies of data. – Ability to avoid data collision on system wide directory (e.g. unique datastamp) – Support transitive replication – not all changes have to be made to master copy. – Ability for a single server to store multiple instances of

	different parts of the overall datastore.
15. Schema	– Product should include support for schema discovery. – Support real time schema changes without the need to reboot system. – Support real time schema change without requiring users online to re-login. – Product should support X.501, X.520 and X.521 schemas – Support schema changes when connected to any Directory Agent – Protection for schema extension / change only to those users with rights to the root of the tree.
16. Directory Object Caching	– Ability to place data close to where it is used. – Ability to refresh cached copies of replicated objects. – Authentication to cached objects. – Support X.501 XREF's (External References)
17. Federation	– Support X.501 Federation – Support the joining of information from different Authoritative Sources. – Support the merging of disparate directories
18. Policy Support	– Support dynamic application of policies (e.g. user does not have to re-login for policy change to take place) – Configurable Policy Architecture.
19. Security	– Evaluation connected in a network setting. – Objects within directory can be designated as security principal (e.g. Grant a firewall object access to a user object).
20. Directory Access Methodologies	– Support LDAP v2.0 and LDAP v3.0 including auxiliary classes – Support JNDI and JDBC. – Support ODBC – Support HTTP – Support ADSI – Support DNS – Support DHCP – Support XML via XSL – Support DAP or DAP derivatives