CONCEPT FOR IMPLEMENTING A GLOBALLY DISTRIBUTED X.500-BASED DoD DIRECTORY

David Gaon

Karol Eller, William Free, and Frank Ogden
Booz•Allen & Hamilton Inc., Bethesda, MD

ABSTRACT
The Defense Information Systems Agency (DISA) is leading an effort to develop and implement an electronic directory to support the Department of Defense (DoD). This DoD Directory will be based on the CCITT X.500 recommendations and will facilitate voice, data (including messaging), imagery, and video communications. The initial operating capability for the DoD Directory is planned for 1995 to meet a validated requirement for an X.500 directory to support the Defense Message System (Reference 1). Continued trends in computer processing and data storage provide DoD with economical alternatives for integrating existing paper-based and proprietary electronic directories.

INTRODUCTION
The mid-1990s provide the Department of Defense (DoD) with a window of opportunity for implementing communication services that are consistent with the technological evolution expected to the year 2005. An integrated electronic directory is one opportunity for advancing the Defense Information System into the next century.

The DoD-wide electronic directory initiative is part of the Defense Information Systems Agency (DISA) Integrated Communications Architecture (ICA) planning process. The goal of the ICA is to integrate the telecommunication architectures belonging to the Services and agencies and the Defense Communications System (DCS) into one integrated network. Primary ICA planning objectives include reducing information exchange costs, improving user satisfaction, and ensuring effective mission accomplishment.

The planned DoD electronic directory system, the DoD Directory, is based on the evolving X.500 recommendations of the Consultative Committee for International Telegraph and Telephone (CCITT) (Reference 2). Two reasons for implementing an X.500-compatible directory are the inclusion of X.500 in Version 3 of the Government Open Systems Interconnection Profile (GOSIP) and the validated requirement for an X.500 directory.

REQUIREMENTS
The DoD Directory is based on a set of validated requirements and common architectural guidelines. The Statement of Requirements (SoR) for the DoD Directory establishes these requirements and guidelines (Reference 3). The Joint Staff is currently staffing the SoR through the Commanders in Chief, Services and agencies for validation. Key requirements and guidelines for the Directory are summarized in the following paragraphs.

The directories supporting DoD today range from paper telephone books to non-standard electronic directories supporting various sets of users. The X.500-based DoD Directory will integrate existing paper and electronic directories to facilitate voice, data (including messaging), imagery and video communications among humans and/or computer processes. The initial operating capability (IOC) and final operating capability (FOC) for the directory are planned for 1995 and 2000, respectively.

The DoD Directory will be accessible to all DoD personnel 24 hours a day. Users will access the Directory through a common, user-friendly interface, with built-in help functions. The Directory will include unclassified and classified information up to the Secret level. Therefore, mechanisms and procedures will be in place to store and protect directory information. Specific security services will be implemented to account for users having different levels of clearances and need-to-know and the various levels of classified information contained in the Directory.

The DoD Directory will operate with selected non-DoD X.500 directories, such as directories of allied organizations. It will interface with these directories through trusted interfaces to ensure security. The DoD Directory will allow for changes to its information content, configuration, and access control. These changes will be made by certain authorized users and/or directory administrators. In addition, directory components will provide information necessary to carry out system management and administration functions.

50.3.1
U.S. Government work not protected by U.S. copyright
DoD-unique requirements dictate enhancements to components developed to the CCITT X.500 recommendations. Examples of these requirements include supporting "MINIMIZE," DoD-specific user interfaces (to include requirements include supporting "MINIMIZE," DoD-specific user interfaces (to include supporting use through a telephone), facilitating a supplemental "help desk," the capability to add and delete arbitrary database entries, strong authentication and access control management, local caching capabilities, usage-sensitive billing, responding within one second from the local DoD Directory Information Base and 15 seconds from the remote DoD Directory Information Base, and the capability to request deferred response to be sent to a temporary store.

ARCHITECTURE AND OPERATION

The basic concept of an X.500-based directory is shown in Figure 1. Directory users, either humans or computer processes, access directory information through a Directory User Agent (DUA). The DUA then communicates with one or more Directory System Agents (DSA) to retrieve or modify directory information. The DUAs and DSAs are software application processes that communicate according to two X.500-defined protocols, the Directory Access Protocol (DAP) and the Directory System Protocol (DSP). The total set of information held by the directory is called the Directory Information Base (DIB). Typically, a portion of the DIB is associated with each DSA.

The DoD DUA will combine X.500-defined DUA functionality with additional DoD-defined requirements. The DoD DUA will be tailored to meet unique DoD requirements for management and administration, user authentication, security, and local caching of information. During the early operational phase, special DoD DUAs will be fielded to allow telephone access to the Directory for users without computer access. The DoD DSA's primary role is to process requests from the DUAs. Other DoD DSA functions relate to authentication, access control, and management and administration.

Many alternatives exist for distributing the directory information. To satisfy the requirement for an operational X.500 capability by 1995, a somewhat centralized DSA/DIB configuration is recommended (Reference 4). This concept consists of several DSAs (each containing the entire DoD DIB) strategically distributed (for survivability reasons) throughout the world. These DSAs will be fully synchronized and each may serve a geographical population. This is only an initial approach and positions DoD for the subsequent evolution to a more hierarchically distributed architecture by the FOC time frame. A preferred hierarchically distributed architecture contains multiple DSAs arranged in a hierarchical pattern. As shown in Figure 2, the Directory will include one or two Top-Level DSAs, several Regional DSAs, and many Base-Level DSAs, each containing portions of the DIB relevant to their local applications. This architecture draws from the advantages of the distributed architecture (such as, simplicity of administration and management, replication and synchronization of data bases, and security) and reduces the disadvantages of the centralized architecture (such as, susceptibility to single-point failures, increased demand on supporting transport networks, and higher memory and processing powers needed at one site). It is also consistent with other trends in DoD communications, such as the regional consolidation of Defense Telecommunications.

The X.500 recommendations define five operations to support interrogation and retrieval of directory information: Read, Compare, List, Search, and

![Figure 1 Concept of a Distributed X.500-Based Directory.](image)
Abandon. There are also operations to support changes to directory information. These operations will be used to support various types of directory queries. For example, a user can combine List and Search operations to browse directory information. Other types of operations and services may be developed specifically for the DoD Directory. For example, a DoD directory administrator may need a Deferred Update capability to allow the DUA to hold an update until a user-specified execution time.

The DoD Directory will facilitate voice, data, imagery and video communications among DoD entities. This gives rise to many different usage scenarios for the Directory. Such scenarios include a human user retrieving the telephone number of another user, an X.400 application process accessing the Directory for the messaging addresses of a group of DoD personnel, and an administrator modifying information in the DIB. Figure 3 shows the process involved for a user to access the DoD Directory to retrieve another user’s telephone number.

The threats, counter threats, and required security services identified for the DoD Directory are shown in Figure 4. Anticipated threats include the unauthorized observation of directory information flow (data monitoring), the unauthorized modification of the information being transmitted (data modification), masquerading as a valid user (deception) to gain access to the Directory, gleaning intelligence about DoD users by analyzing the flow and pattern of Directory user (traffic flow analysis), preventing use of the Directory by overt and covert actions (denial of service), and collecting data from the Directory that, when aggregated, may result in a higher classification (data aggregation). Strategies for securing the Directory include implementing separate classified and unclassified directories, or using multi-level secure systems; auditing all directory interrogations; implementing various levels of authentication and access control; and assigning DISA responsibility for centralized security oversight.
MANAGEMENT AND ADMINISTRATION

DISA will centrally manage and administer the DoD Directory. Common directory management and administration functions are configuration management, fault isolation and repair, performance management, security management, and accounting. DISA may delegate some or all of these responsibilities to DoD Services and agencies for portions of the Directory domain. The DoD Directory domain will be structured to facilitate management and administration. It will include all Directory components, objects and attributes of the DIB, and services provided by the Directory. DoD rules and regulations will be established to ensure standard and common practices and a well-defined service.

The recommended management domain concept for the DoD Directory is hierarchical. The central control element is the DISA Operations Center, which will coordinate overall management policy for the Directory. Management functions will be distributed below the DISA Operations Center into areas, such as DISA Europe and DISA Pacific, and regions within each area. Further distribution of management functions can be made to the bases and installations in each region. This management domain structure is pictured in Figure 5. The basic management concepts, including staffing and funding, are similar to DISA principles and arrangements used to manage the DCS.

IMPLEMENTATION ACTIVITIES

Figure 6 shows the major activities required to achieve a fully electronic DoD Directory by the 2000 time frame. Planned activities for the DoD Directory include defining directory schema (i.e., the rules governing the structure of the DIB and the representation of directory information), developing component specifications, conducting proof of concept tests, and preparing transition plans.

The use of artificial intelligence and knowledge-based learning systems is being investigated for supplementing the security, management, performance, and user interface functions of the DoD Directory.
CONCLUSION

Continued trends in computer processing and data storage provide DoD with economical alternatives for automating the various paper-based directories within DoD and integrating proprietary electronic directories to improve performance, efficiency, and customer satisfaction. DoD is committed to implementing an initial X.500-based DoD Directory capability by the 1995 time frame and a fully electronic Directory by the year 2000. Increased user awareness and industry cooperation are essential to the success of this effort.

REFERENCES


FIGURE 5 DoD Directory Hierarchy Domain Concept

FIGURE 6 DoD Directory Major Activities

50.3.5