Defense Message System Messaging, Directory Services, and Security Services

Wayne DeLoria, DMS Integration Manager, DISA, D24

Alex Sharpe, Susan May, and Chris Bonatti, Booz·Allen & Hamilton Inc.

Abstract

This paper describes the technologies used in the Defense Message System (DMS) to provide messaging, directory, and security services. The basic architecture and functionality of each of the components involved in achieving the DMS architecture are described. Figure 1 depicts the components and protocols discussed in this paper.

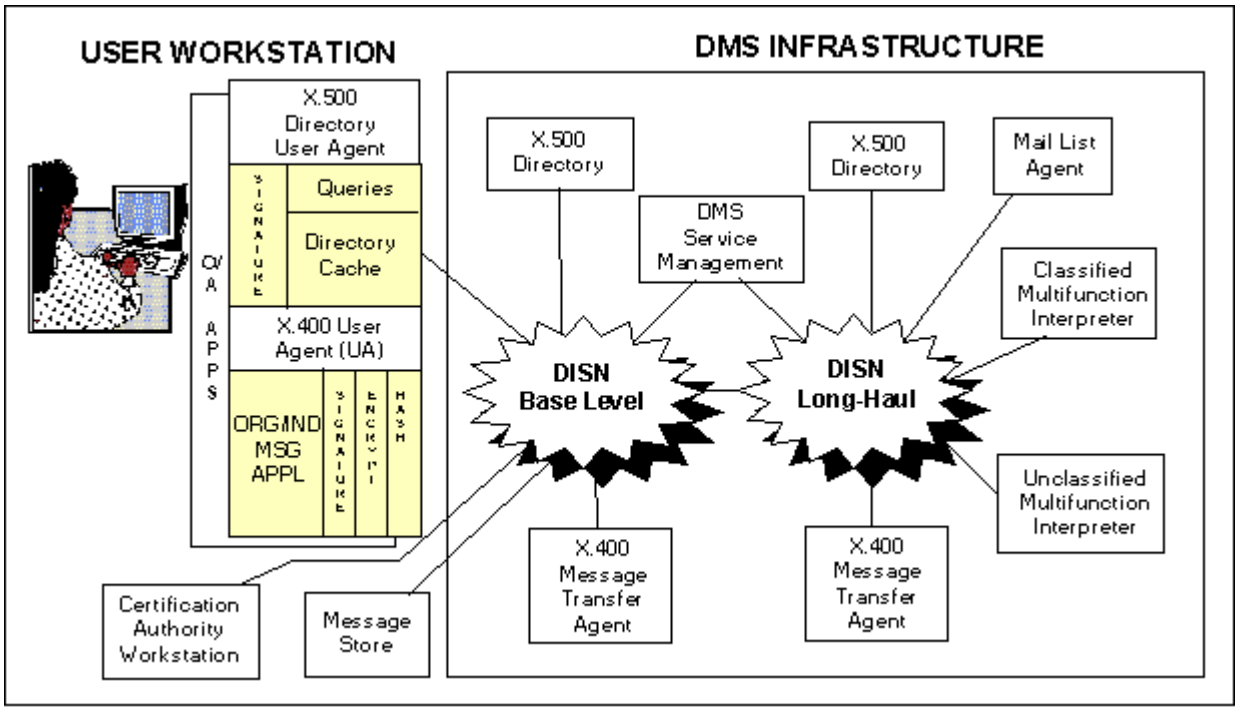

Figure 1. DMS Message Handling System

Overview

The DMS provides automated store and forward writer-to-reader messaging. The system is based on standardized military messaging among the allies using International Telegraph and Telephone Consultative Committee (CCITT) X.400 Recommendations, and CCITT X.500 series of recommendations to provide directory services to support military messaging. The DMS

X.500 Directory is the central repository for all naming, addressing, and contact information to support the DMS. This central repository includes DMS and non-DMS compliant components including AUTODIN and SMTP-based messaging. DMS X.500 Directory services support organizational and individual messaging within the DMS.

DMS also uses the Message Security Protocol (MSP) to provide writer-to-reader security. MSP is an encapsulation protocol that supports the security services of the DMS. MSP will be supported by a variety of security components designed to operate in different security environments. These security products are being provided as part of the Multilevel Information System Security Initiative (MISSI).

DMS Components

The implementation of DMS focuses on the following components: for messaging, the DMS User Agent (DMS-UA), Message Store (MS), Message Transfer Agent (MTA), Profiling User Agent (PUA), Mail List Agent (MLA), and the Multi-Function Interpreter (MFI). Directory services are provided by the DMS Directory System Agent (DSA), the Directory User Agent (DUA), the Administrative Directory User Agent (ADUA), and for security, the Certification Authority Workstation (CAW).

DMS-UA. The DMS-UA is a DMS-specific implementation of the ACP 123 Military Messaging UA. The US Supplement specifies that a standardized Application Program Interface (API) be implemented to allow different messaging-enabled applications (e.g., Electronic Data Interchange [EDI], Records Management) to access DMS services.

PUA. The Profiling User Agent (PUA) is a special type of DMS-UA configured to automatically perform onward distribution of received organizational messages based on preregistered message characteristics.

MLA. The MLA is a specialized device that expands a Mail List (ML) on behalf of a user. A user composes a message with the name of the ML and forwards it to that of the MLA. The MLA then expands the address field of the message to that of the ML member, including the necessary processing to maintain writer-to-reader security.

MFI. The MFI's chief function is translation of messages between ACP 123 protocols and other non-DMS message systems (e.g., ACP 127, SMTP/MIME). The MFI provides a means to maintain interoperability with existing systems while ensuring communications with non-DoD entities such as the commercial sector.

DMS DUA and DSA. The DUA is an application layer process that represents a user in accessing the Directory. DUAs interact with the Directory by communicating with the DSA, which is another application layer process. DSAs collectively retain a physically distributed, but logically centralized, data store—the DIB. The DSAs cooperate to provide the overall directory service. By design, virtually any DUA can access virtually any DSA. DMS DUAs also provide additional features to assist users in composing queries and interpreting responses to provide security services, and to locally cache directory information. In the DMS architecture, any

component requiring X.500 Directory service can implement a DUA. The most common implementation of the DUA will be in conjunction with the DMS UAs. The UA requires information from the X.500 Directory in order to address messages. The DUA obtains this information from the X.500 Directory and supplies it to the UA in support of message preparation.

ADUAs are DMS DUAs enhanced to provide directory administrators the ability to modify X.500 Directory entries. The Update Authorities use the ADUA in combination with the Update Authority Components and/or Message Preparation Directory (MPD) applications to manage, modify, add, and delete X.400, SMTP, and AUTODIN information contained in the DMS X.500 Directory. ADUA applications will reside on the Certificate Authority Workstation (CAW) to perform distributed directory and security management tasks. The ADUA integrated with the MWS will manage the Directory and analyze the Directory's performance.

CAW. The CAW, as part of the infrastructure of the DMS, is the focal point for certificate and key management. The CAW is the tool used by the Certificate Authority to perform Fortezza card creation and management functions, create X.509 certificates and post them to the X.500 Directory, post Certificate Revocation Lists (CRLs), and distribute Compromised Key Lists (CKLs).

The CAW software is operated on a trusted platform with two Fortezza readers, one for the Certificate Authority's card and the other for the user's card being programmed. Along with the CAW software, a local database is maintained for all future reference of personalities and certificates. Additional information regarding users may also be included in this database. In general, the CAW is expected to reside in a physically protected facility and to be operated on a normal business hour basis.

DMS Messaging: ACP 123 Development ACP 123 defines the services, protocol, and procedures required to support electronic messaging for allied defense. To this end, ACP 123 defines a Military Message Handling System (MMHS) based on the X.400 Message Handling System (MHS) recommendations and adopts the extensions made by the NATO STANAG 4406. It also specifies a number of detailed functional requirements to be considered when implementing and operating the DMS components.

ACP 123's scope is limited to the services, protocol, and procedures that affect interoperability in MMHS domains. It does not address messaging between individuals. It also defines only the services and protocols contained in the Application Layer of the Open Systems Interconnection (OSI) reference model.

ACP 123 expands on X.400 to define the Military Messaging Elements of Service, procedures, and protocols. By defining these in common among the allies, participating nations avoid introducing gateways to translate between different message formats and protocols. Use of internationally available messaging and directory standards maximizes the use of commercial off-the-shelf (COTS) products and nondevelopmental items (NDI). Military messages are exchanged within X.400 envelopes, enabling the use of commercial Message Transfer Systems (MTS) to carry military traffic.

The DMS Program Management Office (PMO) is now addressing the use of ACP 123 within the US DoD by developing the US Supplement, which addresses a number of issues specific to the implementation of ACP 123 in the United States.

ACP 123 US Supplement. The ACP 123 document identifies numerous technical and procedural issues that require further refinement for each nation. The DMS addresses these issues in the US Supplement to ACP 123 (US Supplement 1). The US Supplement details message release procedures, onward distribution procedures, individual messaging, operating signals, use of alternative delivery mechanisms, system management, records management, staffing policies, registration, directory services and security. The ACP 123 US Supplement 1 provides this additional detail for the Department of Defense (DoD), including services and agencies (s/a's) and other participating federal agencies. The supplement defines major technical specifications and procedures as follows:

- Message Release Procedures---Drafting of organizational messages, staffing within an organization, and formal release by an organizational release authority (as depicted in Figure 2)

- Onward Distribution Procedures---Procedures for distributing messages within an organization to the appropriate action officers Individual

- Messages---Individual message exchanges between DoD personnel are marked "individual" in the message heading

- Operating Signals---ACP 131 Q and Z signals are indicated through easily understood strings (e.g., "Minimize Considered")

- Use of Alternate Delivery Mechanisms---Support for message redirection by indicating an alternate recipient

- System Management---Maintenance of a 30-day audit log for all components

- Records Management---All messages originated, stored, or received in DMS are federal records, managed in accordance with Code 36 of Federal Regulation (36 CFR) Subchapter B

- Staffing Policies---Policies for ensuring 24-hour operation or arranging for backup recipients

- Registration---Procedures for registration of X.400 O/R Names, object identifier values, and certification authorities.

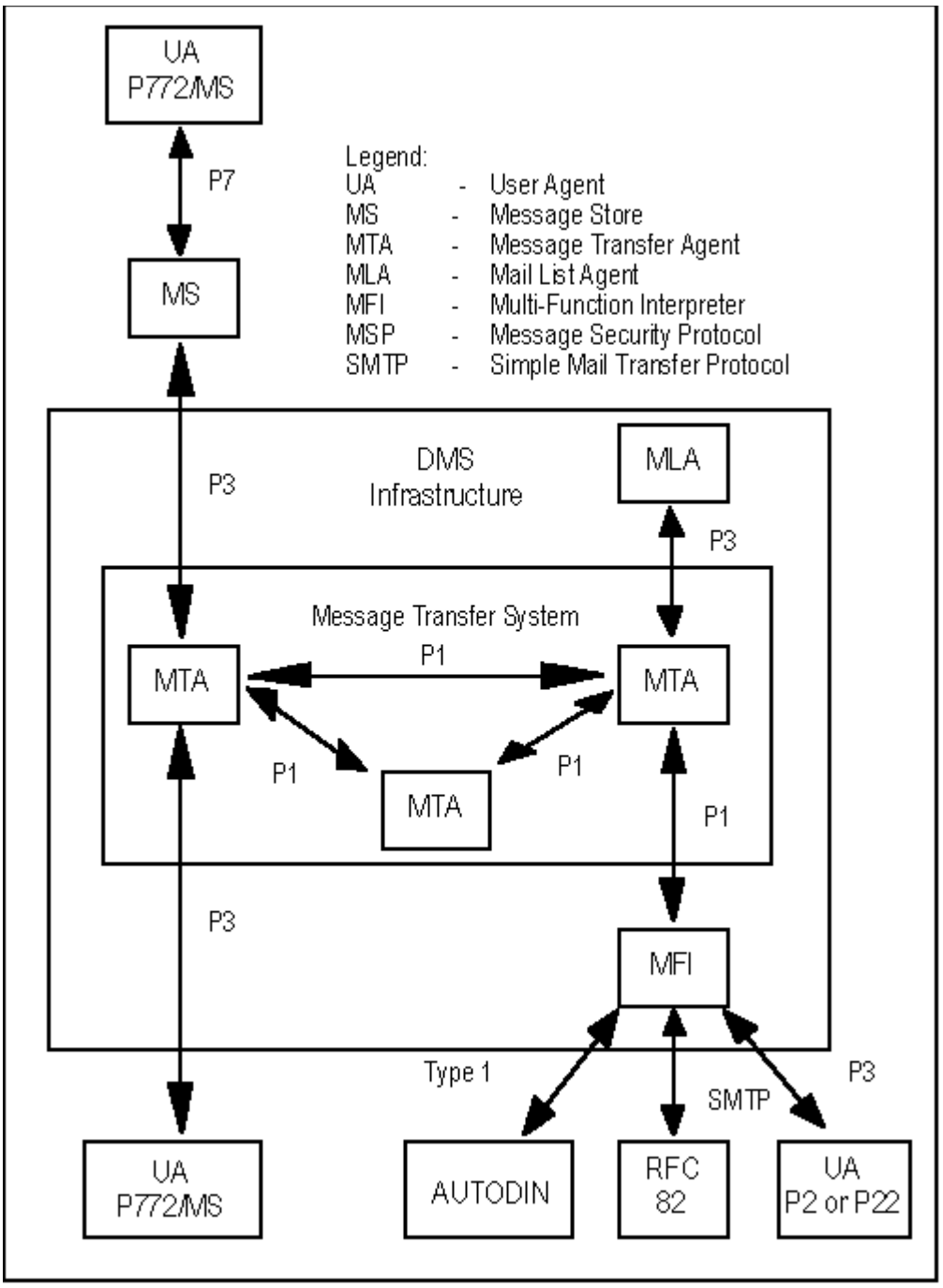

Figure 2. Message Drafting and Release Process Example

DMS Directory Services

The DMS Directory provides a means by which users of DMS and other DoD communications services may, in a user- friendly manner, obtain information about another user or service.

The ACP 133, which is currently under development, defines the directory services, protocol and procedures required to support electronic messaging initially, and other applications in the future. The ACP 133 will describe a DoD Directory based upon the CCITT X.500 series of recommendations.

The DMS Directory is the basis for providing consolidated DoD Directory services in the future for many applications in addition to electronic messaging. The DoD X.500 Directory will provide the naming and addressing "glue" that will allow a more integrated set of DoD applications, such as those for procurement and human resources, to interact using the X.400 application layer transport network. Through the usage of Application Programming Interfaces (APIs), the X.500 Directory will provide addressing and routing information that is essential to the use of automated, computer- based processes. Today, this routing information must be manually configured and periodically updated.

The DMS X.500 Directory will be a distributed service provided by Directory System Agents (DSA), that hold the directory information in the Directory Information Base (DIB). Users access the Directory through DUAs residing in user workstations and in other components that need access to the X.500 Directory, such as the MLA and the MFI. Most DUAs are only allowed to read directory information while others, called Administrative DUAs (ADUA) are allowed to modify the contents of the directory. The DMS X.500 Service uses the Directory Access Protocol (DAP) for operations between DSAs and DUAs, and the Directory Operational Binding Management Protocol (DOP), Directory Information Shadowing Protocol (DISP), and the Directory System Protocol (DSP) for operations between DSAs.

Directory information will be organized and structured in a manner to facilitate access and operation of the DMS. This is called the Schema. The DMS Schema includes elements necessary to meet DMS-specific requirements (e.g., alternate recipients and security information), and those defined in the X.500 standards.

The DMS X.500 Directory will support consolidation of several naming and addressing databases, such as those used for the AUTODIN and SMTP messaging, into a consolidated, distributed database that can be managed using X.500 protocols. These protocols allow timely updates to the data to be performed in a decentralized manner. In addition, the data may be replicated across several DSAs through the use of Shadowing Agreements. Shadowing Agreements dictate services that provide for a more reliable directory service, and facilitate localized data access. Shadowing Agreements, defined in X.500 (1993), are a formal specification of what information (the unit of replication or shadow subject) in the DIT will be shadowed, and how frequently updates will occur. This information is passed between DSAs using the X.500 protocols.

One important function of the DMS X.500 Directory is support for DMS security requirements. DMS Security Policy requires that each DMS user is uniquely identified because this unique identity is the basis for all accountability, ensuring system security. The DMS X.500 Directory facilitates the storage of the items (e.g., certificates) pertaining to the unique identification of individuals using the DMS.

DMS Security

DMS is designed to improve the level of security of existing systems while reducing cost and increasing operational efficiency. The most notable change is DMS' movement towards placing security close to the user to provide security on a writer-to-reader basis versus the traditional approach of securing the communications backbone by link encryption and physical protection. This has a number of overriding benefits. First, the security burden is removed from the underlying network, thereby providing users the operational advantage of using any communications backbone, throughout the world, to achieve the required connectivity. Second, it provides the option of outsourcing network services based on operational and cost effectiveness. This security philosophy also minimizes the risk of compromise by protecting messages between users so nobody else can read or alter the message.

DMS security is designed to be fast, inexpensive, and operationally effective with minimum staffing. DMS security is a force multiplier that reduces the risk of compromise while meeting changing operational environments.

Initial deployment of DMS will address only SBU information. Security services for this type of traffic will be provided by MISSI Phase 1 products. MISSI Phase 1 MSP security service is provided by the Fortezza Crypto Card. The Fortezza Crypto Card is a Personal Computer Memory Card International Association (PCMCIA) peripheral that contains the processor, algorithms, and cryptographic material necessary to support personalized security services. Organizations must designate selected individuals as release authorities. These release authorities are empowered to submit formal military messages on behalf of their organizations by applying the organization's digital signature to a message. Fortezza Crypto Cards are also assigned to each individual who requires use of MISSI Phase 1 services.

DMS security makes full use of public key cryptography to solve the traditional key management problem of requiring an infrastructure to physically distribute key material throughout the network.

Traditional key management is paper-based and labor intensive. DMS security creates and distributes "certificates" that are unclassified and in electronic form so that they can be transmitted between users or stored in Directories to facilitate distribution. Any users in the DMS can then use these unclassified certificates to form a cryptographic key unique to them. This reduces cost by minimizing personnel requirements and by eliminating the need for cleared personnel to handle and account for the material. It provides greater interoperability by allowing any user in the system to communicate with any other user without any prior relationships.

DMS makes extensive use of digital signatures. This allows recipients to validate the authenticity of received messages and allows them to control who can release messages for the organization. This denies an adversary the ability to disrupt operations (e.g., friendly fire or denial of service) by masquerading as a valid user, sending false messages, or retransmitting previous messages.

Digital signatures also provide the Government the ability to perform electronic commerce and legal transactions. Current business process is very labor intensive and paper based. Digital

signatures coupled with other technology like EDI allow for business and legal transactions to be performed faster and cheaper. Digital signatures provide for authentication of the involved parties, prevent undetected alteration of the transaction, and provide electronic records.

Identification and Authentication. Authentication ensures the identity of someone or something in a communication. Authentication is the means of countering the threat of masquerade, which can directly lead to compromise of any of the fundamental security objectives. Authentication enables a recipient to verify that a message is from a legitimate source. This capability prevents an organization from acting on false information.

Nonrepudiation. This service prevents either the writer or the reader from denying a transmitted message. Thus, when a message is sent, the reader can prove that the message was in fact sent by the alleged writer. Similarly, when a message is received, the sender can prove that the message was actually received by the correct reader. DMS message security is structured to ensure that the message recipient creates an automatic audit trail for receipt of the message. In the case of nonreceipt, for whatever reason, the DMS message originator will know. This audit trail provides direct proof that the message was received. This saves time and money because it decreases the requirement for staff follow-on actions. It eliminates the current practice of asking recipients to acknowledge receipt by preparing a return message.

Confidentiality. Confidentiality services protect against information being disclosed to unauthorized parties. DMS provides a secure environment in which the confidentiality of both message writer and reader is protected. Opportunities to breach security are minimized by bringing the message directly to the desktop. Otherwise, each additional person who handles a message (message center, mail room, courier, clerical staff) introduces a chance for inadvertent or intentional breach of security due to loss, reproduction, or alteration of the document.

Integrity. Integrity protects against unauthorized modification, insertion, and deletion of a single message, a stream of messages, or selected fields within a message. An integrity service ensures that messages are received as sent, with no duplication, insertion, or modification. DMS provides a secure environment in which the integrity, or "completeness" of the message is preserved and protected.

Access Control. This service allows only authorized users to send and receive DMS messages. Control can be based on the enforcement of specific access rules or on the identity of the potential user. Authorization is the granting of rights, by the owner or controller of a resource, for others to access that resource. Access control is a means of enforcing authorization.

DMS will employ controls that prevent unauthorized users from accessing information or resources. When the user attempts to access information or a resource, that user's authorization for the requested access is checked and validated. Unauthorized users are denied access. With DMS, only certain infrastructure staff (e.g., those who program the Fortezza cards, those who manage the mail list agents, or who update MTA tables) require security clearances. In addition, the clearance level is reduced from the TS/SCI level to collateral Secret.

Access controls placed on system resources prevent unauthorized users from manipulating the DMS. For example, only certain authorized individuals can manipulate routing tables. This ensures that the DMS is always under friendly control.

Event Handling and Security Audit. DMS has an audit capability that provides a detailed record of system activity to facilitate reconstruction, review, and examination of the events surrounding or leading to possible compromise of sensitive information or denial of service. DMS event handling and security audit also increase an adversary's risk of detection, thereby reducing their willingness to initiate a hostile action against DMS.

Unauthorized activities on a system are typically discovered through the review of the audit trail. The DMS security audit information will provide reliable information that will aid in the discovery and investigation of violations or attempted violations of DMS security policy. The DMS security audit will track and document logins, program initiations, file accesses, file deletions and all actions by users with root privileges (i.e., computer operators and system administrators).

Conclusion

The DMS is making extensive use of recognized international standards to move the allies towards a common messaging system, including the use of Directory and security technology. DMS is leading many changes at the national and international level to form a common messaging backbone that is reliable, cost effective, and secure. Products, standards, and technologies developed under DMS can easily be applied to the commercial sector.

References

Allied Communications Publication (ACP) 123, November 1994.

ACP 123, US Supplement, March 1995.

CCITT Recommendations X.400-X.420, Data Communication Networks, Message Handling Systems, IXth Plenary Assembly, Melbourne, 14-25 November 1988.

CCITT Recommendations X.500-X.521, Data Communication Networks, Directory, IXth Plenary Assembly, Melbourne, 14-25 November 1988.

DISA, DMS Program Management Office, DMS Functional Requirements Document (FRD), 23 December 1993.

DISA, DMS Security Policy Working Group, DMS Security Policy, December 1994.

DISA, DMS Integration Working Group, DMS Directory Implementation Guidelines—Draft, May 1995.