ADOPTING THE DEFENSE MESSAGE SYSTEM (DMS): A GUIDEBOOK

FOR THE
OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM

April 2000

CONTRACT NUMBER DCA 100-95-C-0113

Prepared for
The Office of the Manager
National Communications System
701 South Court House Road
Arlington, VA 22204-2198

PREFACE

This paper is a high-level guide to inform National Communications System (NCS) member agencies that will be implementing the current version of the Defense Message System (DMS).[1] Normally, DMS is implemented by transitioning from the Automatic Digital Network (AUTODIN) or via an upgrade from an earlier version of DMS. Organizations need to determine whether they will be adopting or upgrading DMS. If an agency is required to do so, then this paper will assist in the process of adopting or upgrading DMS. The first section of the guide presents a brief background on AUTODIN and DMS, including a summary of the status of DMS implementation and a description of how DMS messages are transmitted. The second section covers key steps and recommendations for implementing DMS. The guide also offers several appendixes, including a detailed step-by-step plan for transitioning from AUTODIN to DMS, a guide for upgrading from earlier versions of DMS, and a tutorial on DMS security services.

With each new release, DMS incorporates improvements. To maximize DMS capabilities, users must understand the primary DMS components. The four main categories of components include message handling, directory, security, and systems management. Each component is essentially an “add-in” feature that departments and agencies can use in creating and adhering to appropriate operating policies. Therefore, DMS architecture varies according to each organization’s implementation plan.

Several issues must be taken into consideration when implementing the DMS system, including the following:

- The organization’s requirements for DMS (e.g., security, software, hardware, and infrastructure)
- Alternate DMS access methods
- Funding issues involved in installation.

[1] The current version of DMS is Version 2.1.

In addition to this document, several other documents detail how to integrate the DMS system into an organization. These documents (some of which are included as appendixes to this document) include the *Defense Message System (DMS) Product Plan* (Version 3.03; August 20, 1999), *Defense Message System Overview* (February 16, 1998), and *DMS Organizational Messaging Concept of Operations* (Updated April 30, 1999).

DMS is constantly evolving. Therefore, it is in the interest of organizational users to participate in shaping DMS requirements and functionality. Departments and agencies are encouraged to participate in upcoming DMS conferences and planning meetings. Through these meetings, organizational end users can receive current information on DMS updates and provide input on desired features for future versions of DMS. For information on upcoming meetings, see the DMS Conferences Web site [www.disa.mil/D2/dms/conferences.html].

This document is a Technical Information Bulletin (TIB). The advice and suggestions provided in this document are informative in nature and should not be considered directives or mandates. All DMS directives and mandates are coordinated through the Defense Information Systems Agency (DISA) DMS Program Management Office (PMO). Additional information on DMS can be found at the DISA DMS Web site [www.disa.mil/D2/dms/]. Information on the NCS can be found at the NCS Web site [www.ncs.gov].

TABLE OF CONTENTS

Page Number

LIST OF FIGURES

LIST OF TABLES

1.0 STATEMENT OF AND BACKGROUND ON THE ISSUE

To date, the transition from the Automatic Digital Network (AUTODIN) to the Defense Message System (DMS) has been an evolutionary process. However, as the cutoff date for AUTODIN service approaches, many agencies may find they require high-level guidance to assist with the impending transition and ensure that messaging services are not interrupted, delayed, or wrongly classified. This guide addresses these needs. Section 1 presents background information on DMS and AUTODIN. It also includes information on the expected dates for future DMS releases. Section 2 presents several key considerations that must be addressed in adopting DMS.

1.1 Purpose and Scope

DMS is a Department of Defense (DoD) and Defense Information Systems Agency (DISA) initiative. DoD is a member agency of NCS. Therefore, NCS has an interest in providing this guide to alert potential DMS users to suggested considerations for DMS adoption and transition. In addition to background information and key considerations, the guide also offers information on remote and mobile access to DMS. Additional information on transitioning to DMS, DMS upgrade procedures, and DMS security information is provided in the appendixes.

The advice and suggestions provided in this document are informative in nature and should not be considered directives or mandates. All DMS directives and mandates are coordinated through the DISA DMS Program Management Office (PMO).

The DISA DMS Web site [www.disa.mil/D2/dms] provides additional information on DMS. To facilitate DMS transition and adoption, the DMS Customer Information Services Web site [disa.dtic.mil/dms/cis/] was also created to provide feedback on user concerns. This site includes, but is not limited to, step-by-step instructions on how to use the various DMS capabilities, responses to frequently asked questions (FAQ), and a point of contact (POC) section listing contact information for the DMS PMO Management Team (see Table 1 for POC information).

Table 1. DMS Points of Contact

DMS Area	Point of Contact	E-Mail
Program Director	CAPT Jim Day	DMSWWW@ncr.disa.mil
Program Manager	Jerry Bennis	DMSWWW@ncr.disa.mil
Deputy Program Manager	Mary Sloper	sloperm@ncr.disa.mil
Allied Communications Publication (ACP) 120	Sherrill Adkins	adkinss@ncr.disa.mil
Acquisition (non-Lockheed Martin Corporation [LMC])	Melody Kebe, Common Message Processor (CMP)	kebem@ncr.disa.mil
Acquisition Engineering (Air Force Standard Systems Group [AF-SSG])	Michael Yue	hon.yue@gunter.af.mil
Acquisition Project Control (AF-SSG)	Tom Emerson	thomas.emerson@gunter.af.mil
Allies/North Atlantic Treaty Organization (NATO)	Art Dertke	Art.Dertke@osd.pentagon.mil
Automatic Message Handling System (AMHS)	Ken Fagan	fagank@ncr.disa.mil
AUTODIN/DMS Transition	Diana Marshall	marshald@ncr.disa.mil
Conferences	Melody Kebe, CMP	kebem@ncr.disa.mil
Contracting Officer (AF-SSG)	Christine Mitchell	christine.mitchell@gunter.af.mil
Customer Information Services	Irene Ivone	ivonei@ncr.disa.mil
Deployed Tactical	LTC Doug Rogalla	rogallad@ncr.disa.mil
Development Testing	Deborah Swift	swiftd@fhu.disa.mil
DMS Systems Engineer	Bill Arey	areyw@ncr.disa.mil
Directories	LTC Mike McHargue	mchargum@ncr.disa.mil
Emergency Action Messages (EAM)	LCDR Rhett Jaehn	jaehnrr@js.pentagon.mil
Engineering Manager	Mike Hanz	hanze@ncr.disa.mil
Firewalls	Steve O’Guin	oguins@ncr.disa.mil
Funding	Kim Davis	davis1k@ncr.disa.mil
Information Assurance Vulnerability Alert (IAVA) (POC 1)	MAJ Bill Garland	garlandw@ncr.disa.mil
IAVA (POC 2)	Ev Corcoran	corcorae@ncr.disa.mil
Implementation	Curtis Miller	miller2c@ncr.disa.mil
Implementation Group	Jerry Bennis	DMSWWW@ncr.disa.mil
Implementation Security Mgt	Tom Zmudzinski	zmudzint@ncr.disa.mil
Information Technology (IT) Overarching Integrated Product Team (OIPT) (Major Automated Information System Review Council [MAISRC])	Melody Kebe, CMP	kebem@ncr.disa.com

DMS Area	Point of Contact	E-Mail
Logistics & Training	Margot Alexander	alexandm@ncr.disa.mil
Medium Grade Service	Betsy Appleby	applebyb@ncr.disa.mil
Multilevel Information System Security Initiative (MISSI) Products	Mary Lin	linm@ncr.disa.mil
Operational Testing	Ken Wachsman	wachsmak@fhu.disa.mil
Operations/Global Service Manager	John Milton	miltonj@ncr.disa.mil
Operations Group	CAPT Jim Day	DMSWWW@ncr.disa.mil
Product & Integration	Barbara Keller	keller1b@ncr.disa.mil
Program Control	Melody Kebe, CMP	kebem@ncr.disa.com
Release 2.1 Manager	MAJ Bill Garland	garlandw@ncr.disa.mil
Release 2.2 Manager	MAJ Bill Garland	garlandw@ncr.disa.mil
Requirements	Jo Marie Coburn	coburnj@ncr.disa.mil
Service Management Products	Jay Mallard	mallardj@ncr.disa.mil
Tactical	John Nowakowski	nowakowj@ncr.disa.mil
Testing Manager	LT Mike Miley	mileym@ncr.disa.mil
Top Secret (TS) General Service (GENSER)	Alesia Jones-Harewood	harewooda@ncr.disa.mil
Web Pages	Melody Kebe, CMP	kebem@ncr.disa.mil
Year 2000 (Y2K)	Barbara Keller	kellerb@ncr.disa.mil

Source: DISA, DMS Customer Information Services Point of Contact Web site [www.disa.mil/d2/dms/poc.html], March 22, 2000.

1.2 DMS and AUTODIN

DMS is a flexible, secure system based on commercial off-the-shelf (COTS) software that will facilitate and coordinate development of an integrated, common-user message system for organizational users in DoD and supporting agencies.[2] It is a reliable organizational messaging system with a global integrated directory service that operates across multiple commercial vendor platforms. DMS provides multimedia messaging and directory services that will efficiently utilize the underlying Defense Information Infrastructure (DII) network and services. DMS is intended to replace AUTODIN and other incompatible, unsecured electronic mail (e-mail) systems and to standardize e-mail throughout DoD. Some of the benefits that will be available through DMS are listed in Table 2.

Table 2. Benefits of DMS

• Text and graphics • Multimedia attachments • Audio • Full-motion video • Photos • Imagery • Spreadsheets • Databases • Presentations	• P772 (formatted) messaging • Standardized National Security Agency (NSA)-certified encryption (security with FORTEZZA) • Digital signature (authentication with FORTEZZA) • Directory services (X.500) • Ability to generate both classified and unclassified messages/e-mail (if authorized) • Ease of handling; organizational messages and e-mail combined on same system

Sources: Booz·Allen & Hamilton, 1999; and U.S. Coast Guard, *Defense Message System (DMS Primer),* September 1997.

The DoD AUTODIN record message system has served the military, other government agencies, and allies for more than 30 years. However, the system is extremely expensive to operate and maintain, in both dollars ($750 million annually) and personnel. Its technology is outdated, technologically slow (operating at about 2.4 kilobits per second [kbps]), limited in its capabilities (especially in transmitting textual information), and quickly becoming unsupportable.

The current AUTODIN contract expired on December 31, 1999, and cannot be legally extended or effectively recompeted, although provisions for an AUTODIN extension that begins on this date are in place.[3] DMS was established by the Undersecretary of Defense for Acquisition and mandated by the Assistant Secretary of Defense (ASD) and the Intelligence Secretariats to be implemented by December 31, 1999. In an April 1999 memorandum, the Assistant Secretary of Defense for Command, Control, Communication, and Intelligence (ASD[C3I]) reemphasized that DMS was the designated messaging system for DoD and other NCS member agencies currently using AUTODIN. DMS will allow former AUTODIN users to take advantage of modern messaging technology. In a December 28, 1999, memo from the ASD(C3I), a three-

[2] DMS is also intended for use by individual users; however, this guide deals only with organizational users.

[3] Daniel Verton, "DMS Gaps Force DoD to Keep AUTODIN," *Federal Computer Week*, May 18, 1998; and Bill Murray and Gregory Slabodkin, "DoD Figures AUTODIN Must Run Until 2004," *Government Computer News*, June 15, 1998.

phase plan designated that all organizational messaging traffic must be transitioned from AUTODIN to DMS by September 30, 2003 (see Section 1.4 for more information).

1.3 DMS History

Requirements for DMS were originally recorded in *DMS Multicommand Required Operational Capabilities* (MROC 3-88; February 1989). *DMS Required Operational Messaging Characteristics* (ROMC; May 1993) provided more detailed (i.e., quantitative and qualitative) statements of the MROC 3-88 requirements. The Joint Staff validated both the MROC 3-88 and the ROMC.

In spring 1997, Military Communications Principals and Chief Information Officers (CIO) assessed DMS requirements to ensure that they supported the established DMS goal, convergence with commercial technology. From this assessment came the DMS MROC Change 2 (October 30, 1997), which increased user flexibility in implementing DMS capabilities and called for a DMS system consisting primarily of COTS products and services.

The primary objective of the DMS system is to reduce cost and staffing by eliminating the outdated AUTODIN system. The secondary objective is to provide tactical and allied messaging systems, build on available commercial products, and incorporate international standards. DMS will use COTS products to integrate the present military messaging system and e-mail into a single, writer-to-reader, multilevel secure messaging system capable of exchanging official messages and e-mail in the course of conducting business.

DMS is designed to run on the Defense Information System Network (DISN). It is not a network itself, but rather a system (because its components work together to provide messaging services) and an application (because to end users it appears simply as an icon on the computer screen similar to other applications). DMS is provided to end users through Microsoft Exchange (i.e., Outlook) and Lotus Notes. Lotus and Microsoft produce the DMS client-server software, which includes directory and security options not provided in commercial e-mail packages. DMS will eventually handle all classification levels from Unclassified to Top Secret.

1.4 Status of DMS Implementation

DMS implements and fields system capabilities through a series of coordinated product releases. Major Releases (e.g., DMS 3.0) correspond to attainment of significant program capabilities (e.g., Sensitive But Unclassified [SBU] Initial Operating Capability [IOC], Classified Messaging). Minor Releases (DMS 3.1) indicate system and product improvements within a baseline program capability. Table 3 presents past, current, and projected DMS product releases.

Table 3. DMS Product Releases

Release	Dates of Use	Major Features
DMS 1.0 and 1.1—Beta Deployment	6/1/97–10/31/97	• Capability to support full-scale deployment rates • Support for Unclassified messaging • Basic AUTODIN interoperability
DMS 2.0—Initial Organizational Messaging	7/1/98–2/1/99	• Support for MS Exchange 5.5, Outlook 98, and Domino 4.6 • Y2K compliance
DMS 2.1—Fully Functional Organizational Messaging	4/1/99–4/1/00	• Support for Secret But Unclassified and Secret messaging • Shared mail box • Multimail box • Proxy profiling user agent (PUA) and multiorganization PUA • Parallel FORTEZZA reader drivers
DMS 2.2—Organizational Messaging Enhancements	12/3/98–8/3/00	• Support for Outlook 2000 and Lotus R5 • PUA dissemination enhancements
DMS 3.0—Automated Access Controls	8/1/00–2/1/01	• Support for Top Secret, Sensitive Compartmented Information • Software FORTEZZA • Directory strong authentication
DMS 3.1—Intelligence and Tactical Unique	3/1/2000	• In development

Source: Booz·Allen & Hamilton, 2000.

As of January 15, 1999, more than 490,000 organizational users had been identified to receive DMS before AUTODIN closure. As of March 17, 2000, 240 Nonclassified Internet Protocol Router Network (NIPRNet) sites (96 percent of the total 251 planned) had been implemented, and 176 Secret Internet Protocol Router Network (SIPRNet) sites (92 percent of the total 192 planned) had been implemented. Table 4 presents the percentages of all planned DoD commissioned systems that had implemented DMS as of November 12, 1999.

Table 4. DoD Implemented DMS Systems As of November 12, 1999

Service/Agency	Planned Implementations: Percent Completed
Air Force	100
Army	87
Commanders in Chief (CINC)	100
Coast Guard	100
Defense Finance and Accounting Service (DFAS)	33
DISA	50
Defense Logistics Agency (DLA)	80
Defense Threat Reduction Agency (DTRA)	0
Marine Corps	87
Navy	95
National Imagery and Mapping Agency (NIMA)	25

Note: Percentages supplied by DoD.

ASD(C3I) announced a revised DMS transition plan when it became apparent that many services and DoD agencies would be unable to transition from AUTODIN to by December 31, 1999.[4] The revised plan calls for complete termination of AUTODIN directory transition hubs (DTH) by the end of fiscal year (FY) 2003. The plan consists of three phases with accompanying milestones (see Table 5):

- *Phase I*—Governs the transition of all general service (GENSER) traffic with no special category/special handling designator (SPECAT/SHD).

[4] ASD(C3I), "Revised Defense Message System Transition Plan," Memorandum for Director of Information Systems for Command, Control, Communications, & Computers (DISC4), Director, Space Information Warfare Command and Control (N6), Director, Command, Control, Communications, Computer and Intelligence (C4I) (USMC), Director, Headquarters (HQ) Communications and Information (AF/SC), and Director, DISA, December 28, 1999.

- *Phase II*—Governs the transition of GENSER traffic, including SPECAT/SHD traffic, to DMS. Milestones are linked to completion of the operational test and subsequent fielding decision (FD) for DMS 3.0. Release 3.0 fielding is currently expected in early calendar year (CY) 2001.
- *Phase III*—Governs the migration of special communities from legacy systems to DMS or other systems.

Table 5. DoD DMS Transition: Phased Approach

PHASE	DATES	MILESTONES
I	3/15/00	Services and DoD agencies will have greater than 50 percent of their Secret and below organizational accounts functional (CINCs are exempt).
	4/15/00	Services, CINCs, and DoD agencies will have greater than 50 percent of their Top Secret/Collateral organizational accounts functional and at least 50 percent of Top Secret (TS)/Collateral traffic transitional to DMS or dual-routed in DMS.
	5/15/00	Services, CINCs, and DoD agencies will have greater than 75 percent of their Top Secret/Collateral and below organizational accounts functional and at least 50 percent of TS/Collateral and below non-SPECAT/SHD GENSER traffic transitioned to DMS or dual-routed in DMS.
	8/15/00	Services, CINCs, and DoD agencies will have greater than 95 percent of their Top Secret/Collateral and below organizational accounts functional.
	9/15/00	Services, CINCs, and DoD agencies will have 100 percent of their Top Secret/Collateral and below organizational accounts operational and 100 percent of their non-SPECAT/SHD GENSER messaging transitioned to DMS.
II	FD + 4 months	100 percent of SPECAT/SHD-capable organizational accounts will be converted to Version 3 certificates, and at least 50 percent of SPECAT/SHD traffic will be transitioned to DMS or dual-routed in DMS.
	FD + 6 months	100 percent of DMS GENSER organizational user accounts will be fully operational with Version 3 certificates and 100 percent of GENSER messaging, including SPECAT/SHD messaging, will be transitioned to DMS.

III	In FY03	Development and operation of a final architecture for emergency action messaging, independent of DTHs will be completed.
	End of FY03	Services' tactical implementation of DMS will be completed.
	End of FY03	Interoperability transition of Allied and coalition partners from DTHs to an Allied interoperability gateway will be completed.

Source: Booz·Allen & Hamilton, 2000; and ASD(C3I), "Revised Defense Message System Transition Plan," Memorandum for Director of DISC4; Director, N6; Director, C4I (USMC); Director, HQ AF/SC; and Director, DISA, December 28, 1999.

1.5 DMS Components

Each department or agency that uses DMS is responsible for designing and implementing a DMS architecture and for creating and adhering to appropriate operating policies. An understanding of the flexible DMS architecture is vital to designing and implementing DMS. This section provides a functional description of the components necessary to implement DMS and outlines how a DMS message is processed.

DMS components are extensions of COTS products. The extensions consist of "bolt-on" or "add-in" features that are required to support unique DoD messaging specifications defined by the MROC. DMS integrates various COTS products that work together to create, secure, and transfer organizational messages. Most DMS components fall into one of four functional categories based on the service provided—message handling, directory, security, or systems management.

Message Handling

- *DMS User Agent (UA)*—The UA is the desktop software package that enables and facilitates each user's interface with DMS. It is a modified version of a COTS e-mail application, such as Microsoft Outlook or Lotus Notes, that has been approved and designated for use with DMS and subsequently adopted by the organization. DMS users compose, digitally sign, encrypt, transmit, receive, decrypt, and read messages via the UA.

- *Profiling User Agent (PUA)*—The PUA is a specialized UA used to distribute organizational messages on the basis of the message content or "profile." The profile is formulated via a list of keywords that are mapped to the names of individuals who should receive copies of a message. The PUA first verifies the integrity of the message and decrypts it. After profiling the message and copying it, the PUA reencrypts the message and forwards it to the Message Transfer Agent (MTA), as described below, for delivery.

- *Mail List Agent (MLA)*—The MLA allows DMS users to address messages to a group of predefined recipients via a single mail list name, which function similarly to the Address Indicator Groups (AIG) and Collective Address Designators (CAD) used in AUTODIN. The MLA copies the message, addresses each message with the name of an individual on the mail list, and routes the messages to the MTA for delivery.

- *Multifunction Interpreter (MFI)*—The MFI enables DMS interoperability with legacy AUTODIN users and Government departments and agencies by translating DMS protocols into those used by other systems.

- *Message Transfer Agent (MTA)*—The MTA, also called a message switch, relays message traffic from an originator to the recipients, prioritizes message transfer according to each message's grade of delivery, and provides audit trails for message delivery. The MTA application can be stored on the DMS server or a networked workstation, depending on the amount of DMS traffic.

Directory

- *Directory User Agent (DUA)*—The DUA application is also loaded onto each DMS user's workstation, typically as part of the UA. The DUA provides connectivity to the DMS X.400/X.500 directory, which stores the names and addresses of each registered DMS user and enables users to address and send messages to any DMS user.

- *Directory System Agent (DSA)*—The DSA stores the portions of the DMS X.400/X.500 directory (implemented via a hierarchical, distributed platform) that represent a given organization's network.

Security

- *FORTEZZA Card*—The FORTEZZA card is a peripheral device, roughly the size of a credit card, that is inserted into the Personal Computer Memory Card International Association (PCMCIA) slot on a user's workstation. It enables digital signatures and encrypts messages through the use of private keys and public certificates. The FORTEZZA card provides data confidentiality, data integrity, user non-repudiation, and user authentication services. It is a registered product of NSA's MISSI, which identifies interoperable security products capable of providing modular security for networked information systems.

- *Certification Authority Workstation (CAW)*—The CAW manages each organization's DMS X.400/X.500 directory certificates and programs FORTEZZA cards with a user's security profile, security certificates, and cryptographic key. In addition, it posts the user's public certificate to the DMS X.400/X.500 directory. The CAW is a certified NSA MISSI product.

- *High Assurance Guards (HAG)*—HAGs are NSA MISSI products that permit the transfer of Secret DMS messages over an unclassified network by securing the connection to the unclassified network and ensuring that each outgoing message is encrypted. By enforcing access controls, HAGs protect the higher domain from attacks originating in the lower domain. Under DMS guidelines, HAGs are implemented using a combination of hardware, software, and FORTEZZA cards.

- *Security Levels*—According to each department or agency's requirements, DMS currently can be implemented for one of two security domains: SBU or Secret. Messages can be transmitted to and from the Secret and SBU environments via HAGs, as described above. SBU message traffic is transported via NIPRNet. Secret message traffic is transported via SIPRNet.

Systems Management

- *Management Workstation (MWS)*—The MWS uses commercial monitoring and trouble-reporting tools to monitor and audit system activity, including directory activity. It ensures optimal system performance.

Other Key Architecture Elements and Considerations

- *DMS Server*—The DMS server, also called the groupware server (GWS), stores the mailboxes and directory information for each DMS user in its domain. The DMS server can be configured to provide capabilities found in groupware servers on the commercial market.

- *Local Control Center (LCC)*—An LCC facilitates DMS connectivity to DII. In routing message traffic through DII, the LCC performs functions similar to those of the AUTODIN Automated Switching Center (ASC). LCCs also monitor DMS components and provide administrative support to the organizations under their purview. Each department and agency is responsible for implementing and maintaining its own LCC or establishing an alternate means of connecting to the DII, as described below.

- *Dial-Up Access*—In lieu of establishing an LCC, which can be costly and can require extensive maintenance and support, departments and agencies can arrange for dial-up access to an LCC maintained by a military service branch or another department or agency. For the Secret and Top Secret or Collateral levels, dial-up access requires a Secure Telephone Unit III (STU-III) or a direct, secure local SIPRNet connection.

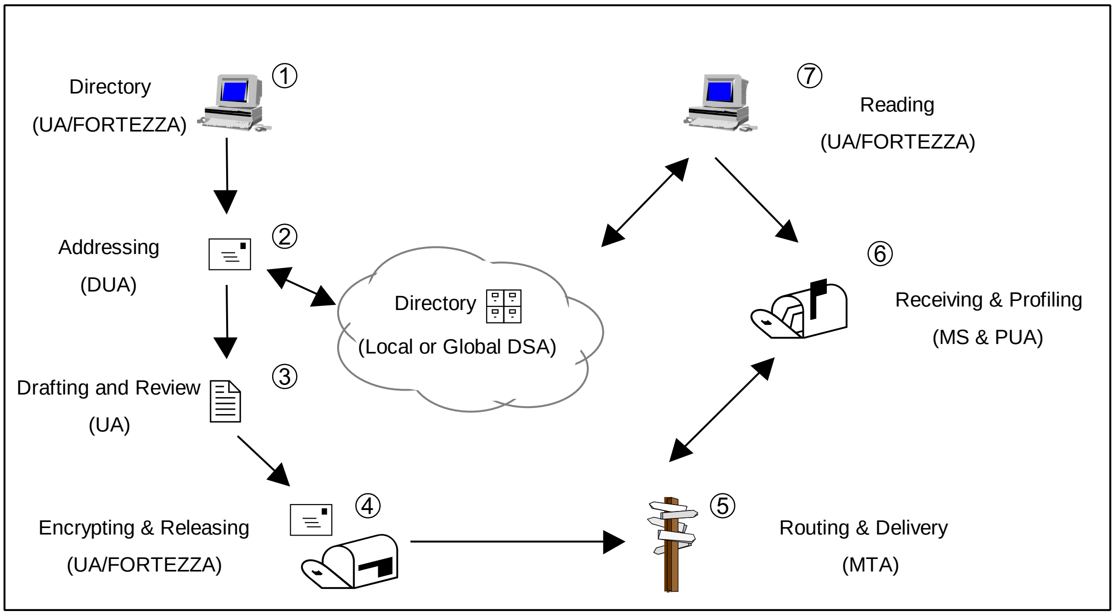
- *Plain Language Address (PLA) Naming Strategy*—Organizations transitioning to DMS are required to establish distinguished names and organizational identities for DMS users that are designated to send and receive messages from the AUTODIN. The distinguished name of each DMS organizational messaging user with release authority privileges must be associated with a PLA that identifies that individual or his or her organization to AUTODIN users.

For more details, see Appendix B, Transitioning to DMS.

1.6 DMS Message Transmission

Figure 1 depicts the transfer of a DMS message via the DMS components outlined above. Note that all message traffic begins and ends at the user's workstation and is accessed via the UA. The UA works with the other components seamlessly and is transparent to the user. The graphic provides a general view of DMS architecture, which may vary slightly according to each organization's implementation plan. For example, an organization's DMS architecture may include a PUA and HAG. Figure 1 illustrates the sequential steps in the DMS process.

Figure 1. DMS Message Flow



Note: MS=Message Store.
Source: DISA DMS Web site [www.disa.mil/D2/dms], 1999.

1. Each DMS user logs into the network via the UA. The log-in process includes a user name, password, and a FORTEZZA card, which decrypts messages and verifies digital signatures. If the FORTEZZA card is not inserted, the UA does not function.

2. The DUA, located with the UA on the user's workstation, addresses the message by interacting with the organization's DSA.

3. The user drafts and reviews the message via the UA.

4. The message is encrypted and the FORTEZZA card applies a digital signature. Once the message is ready for release, it is sent to the organization's MTA.

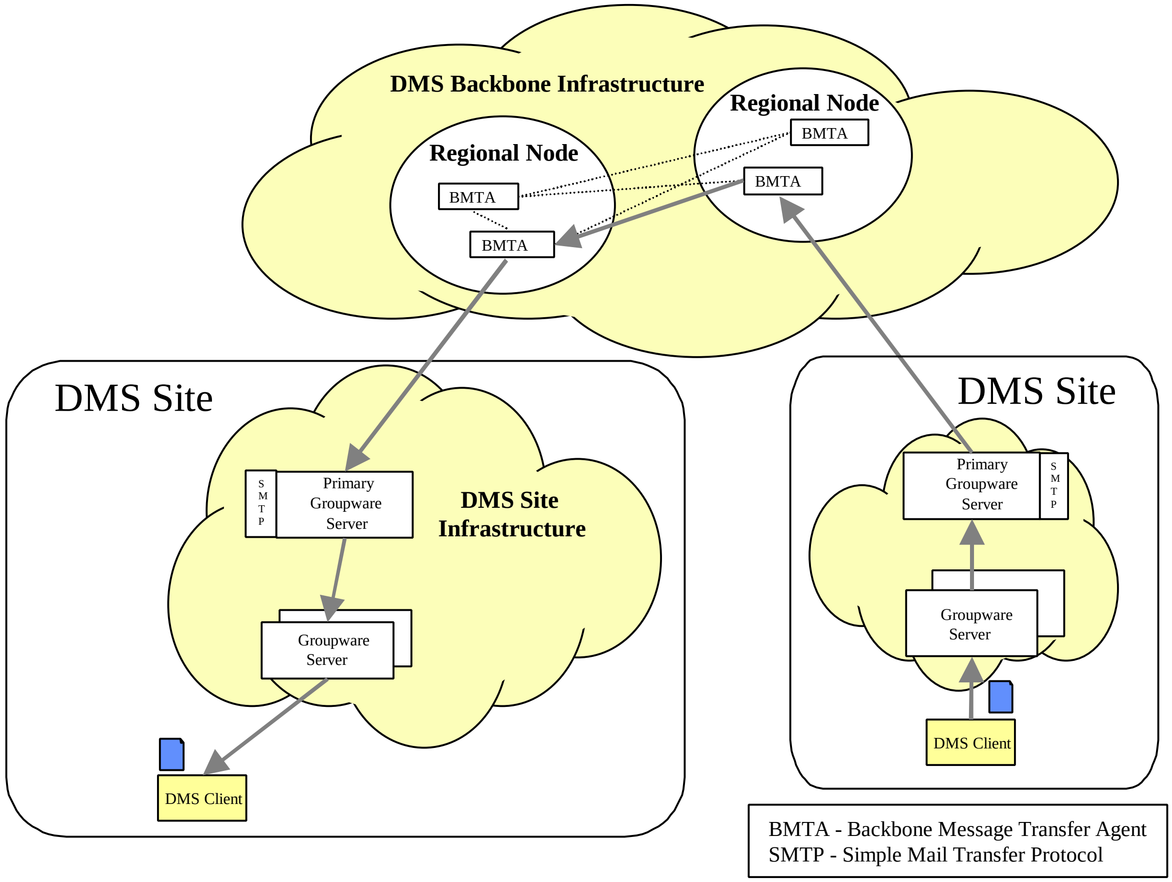
5. The MTA stores and forwards the message based on the message's designated grade of delivery and works with the interconnected switching system (i.e., the Message Transfer System [MTS]).

6. The MTS works with the MTA to route message traffic. When the UA is available, it routes the messages forwarded to it by the MTA to the UA. If an organization has implemented a PUA, the PUA receives the message and distributes it based on the message information.

7. The user accesses and reads his or her mail by logging into the UA. The FORTEZZA card decrypts the message and verifies its digital signature.

Figure 2 shows how DMS sites connect with the DMS backbone to provide messaging to users outside the organization. DISA owns and operates the DMS backbone infrastructure, which is part of DISN, and routes the message through a contained network once it is outside the originating organization's purview. Note that this figure depicts only the standard transfer of a message from one DMS client to another DMS client. See the *DMS Organizational Messaging Concept of Operations* for further details and other implementation configurations.

Figure 2. DMS Architecture



Source: DISA, *DMS Organizational Messaging Concept of Operations*, Section 3.3, "DMS Organizational Messaging," April 30, 1999 (Update).

1.7 DMS Organizational Messaging Transition

Several key steps are required for successful transition from AUTODIN messaging to DMS. Some of these steps are the responsibility of the service providers, and others are the responsibility of the organizational end users. Table 6 briefly summarizes these steps.

Table 6. Steps for a Successful DMS Transition

Step/Title	Status	Responsibility
I. Construction of a stable DMS infrastructure	DMS backbone is in place	DISA
II. Installation and stabilization of local site components	Local sites are installed Not all local sites are stabilized	DISA and organizational end users
III. Creation of organizational user accounts (OUA) with FORTEZZA cards for AUTODIN PLAs and redirection of the PLA to the MFI	OUAs are still being developed	DISA
IV. Transition of AUTODIN collectives to DMS mail lists	Transition is incomplete	DISA
V. Installation of HAG to support Secret-only users and Unclassified-to-Secret messaging	Policy is still being developed Guards are still being installed	DISA
VI. Establishment of new operational procedures using DMS instead of communication centers	New procedures are still being developed	DISA

Source: Booz·Allen & Hamilton, 2000.

The next section of this document provides a high-level discussion of DMS. It addresses three major considerations for organizational end users: requirements, including security considerations; alternative access methods; and funding considerations.

2.0 TECHNICAL ANALYSES OF AND RECOMMENDATIONS ON THE ISSUE

As an agency considers or undertakes a transition from AUTODIN to the current version of DMS, or from an earlier version of DMS to the current one, it must carefully consider several issues, from validating the requirements to funding the transition. Section 2.1 offers a high-level checklist for determining DMS requirements. Section 2.2 considers alternative access methods for DMS. Section 2.3 addresses funding considerations and depicts a sample configuration for implementing DMS. Finally, Section 2.4 presents conclusions and recommendations. After departments and agencies thoroughly read and understand this section, they are encouraged to use Appendix B, Transitioning to DMS, which offers detailed guidance for transitioning messaging systems from AUTODIN to DMS. Also recommended is Appendix C, Upgrading DMS, which contains detailed information on upgrading from earlier versions of DMS.

2.1 Requirements Analysis

The first step in DMS implementation is to assess DMS requirements. Is DMS implementation required for the target agency? What level of security is required? What are the software, hardware, and infrastructure requirements? Sections addressing these and other requirements follow.

2.1.1 Assessment of Current Messaging Environment

An agency must implement DMS if it currently uses AUTODIN or an earlier version of DMS. If an agency depends on AUTODIN for messaging, it is imperative to implement DMS because AUTODIN is scheduled for termination (see Section 1.0 for details and dates). If an agency is using an earlier version of DMS, then upgrading is necessary to take advantage of current DMS capabilities.

If an agency is not currently using AUTODIN or DMS and is not expected to have any future requirement for DMS, DMS implementation may be unnecessary. For confirmation, the agency’s Management Information Systems (MIS) Department should contact the DMS Department at DISA (e-mail: DMSWWW@ncr.disa.mil).

2.1.2 Security Level Requirements

Perhaps the most important factor in assessing DMS requirements is the determination of security level requirements. An agency must be certain that any DMS implementation will be capable of ensuring the security of its messages. The current version of DMS supports SBU and Secret security levels.[5]

Both SBU and Secret security levels can be handled via NIPRNet. However, higher levels (available in future releases) will require access to SIPRNet. HAGs will support Unclassified messaging between the NIPRNet and SIPRNet DMS messaging domains. Access to SIPRNet increases the complexity and cost of DMS implementation. DMS security is provided by a combination of public key infrastructure (PKI), FORTEZZA, and DII defense in depth. For more details on this issue see Appendix D, DMS Security Services.

2.1.3 Messaging Hardware and Software Requirements (Including FORTEZZA and Infrastructure Requirements)

Implementing DMS requires choosing appropriate software, hardware, and infrastructure components. Table 7 shows the product, platform, and operating system baseline for the current version of DMS. Platforms annotated with an asterisk (*) are supported as fielded legacy platforms and are not recommended when designing new systems. Details on minimum requirements (e.g., amount of memory, hard disk) can be found in each DMS product’s system design architecture document.

[5] DMS 3.0 will also support Top Secret, Sensitive Compartmented Information (TS SCI).

Table 7. DMS Products

Product	Platform	Operating System
User Components		
Microsoft Exchange Client: Outlook 98	Intel PC 586+	Windows 95/98, NT 4.0
Microsoft Exchange 5.5 Server	Intel PC 586+ DEC Alpha	NT 4.0
Lotus Domino 4.6 Server	Intel PC 586+	NT 4.0
Lotus Notes 4.6 Client	Intel PC 486 (Win95 only) & 586+	Windows 95/98, NT 4.0
Xerox PUA	HP 9000/700* & D220	HP/UX 10.2
FORTEZZA Cards	GroupTech & Spyrus ("Purple") Cards	N/A
Infrastructure Components		
Data Communications, Limited (DCL) Message Switch MTA	HP 9000/800* & D220 Sun Microsystems	HP/UX 10.2 Solaris 2.5.1
DCL Directory Services DSA	HP 9000/800* & D220 Sun Microsystems	HP/UX 10.2 Solaris 2.5.1
DCL Directory Services Administrative Directory User Agent (ADUA)	Intel 486+	Windows NT 4.0
HAG Version 2.2.1	Intel, Proprietary	Proprietary
CAW Version 3.1	Intel, Proprietary	SCO, Proprietary
CipherNET Registrar Version 3.1, CMUA Version 1.0	Intel 486+	NT 4.0
Commpower MFI	HP 9000/700* & D220	HP/UX 10.2
Commpower MLA	HP 9000/700* & D220	HP/UX 10.2
Management Work Station (Computer Associates, Remedy, Oracle)	HP 9000/700* & D220	HP/UX 10.2

* Fielded legacy systems supported; not recommended for new systems.
Source: Booz·Allen & Hamilton, 2000.

2.2 Contingency Access to DMS[6]

In some instances, an agency may not be required or able to set up an LCC because of limitations on DMS requirements or funding. Currently, two alternatives to establishing an LCC provide access to DMS. The first solution is remote access. Limited funding for DMS implementation usually (but not always) drives this solution. The second alternative is mobile access. Mobile access is used during planned or sudden mobile activities, such as planned troop movements or unplanned relocation to sites with no direct access to an LCC.

2.2.1 Remote Access

Remote access takes two forms: remote DMS and roaming user. Remote DMS is a full-spectrum messaging capability to send and receive official e-mail established for eligible DMS users who do not have, or do not choose, direct connectivity to an LCC. To provide connectivity to these customers, several agencies and services provide remote DMS. Remote DMS allows remote dial-up access to DMS for traveling users and those who require DMS but have no LCC.

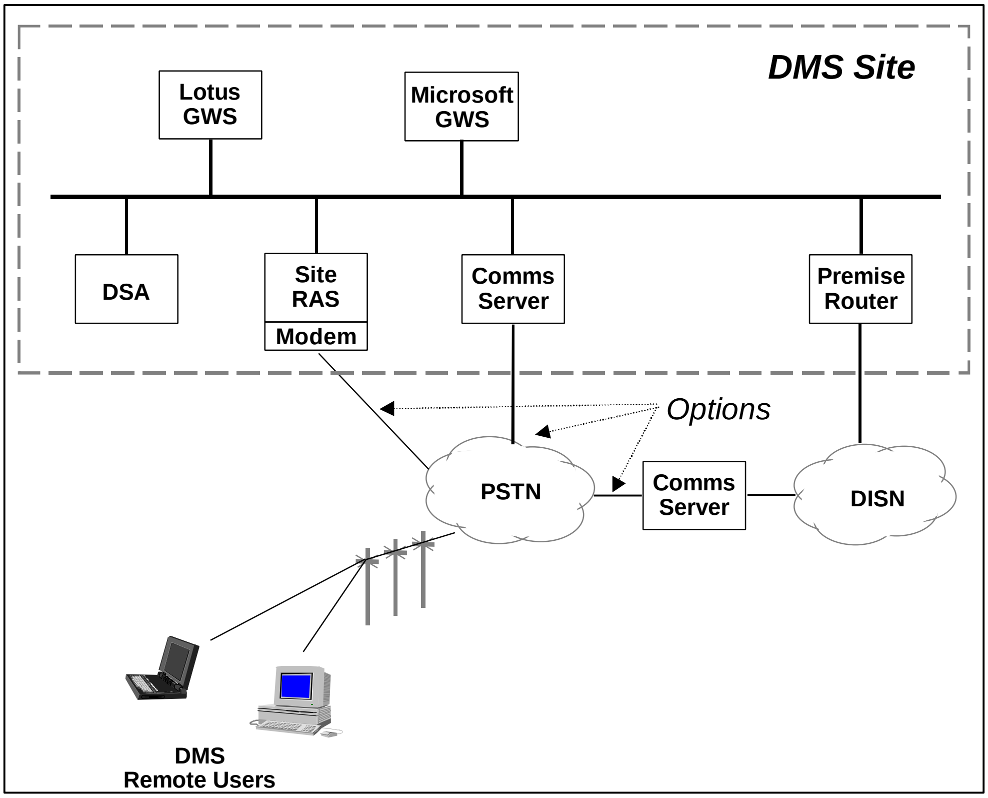
Roaming user connectivity is for users who are not at their desk but are at their normal duty site and need access to DMS from another workstation in the enclave. To users, the remote client is the same as a client physically located on the local network except for the dial-up connection. Additional procedures and software are required for establishing the dial-up connection whenever DMS messages are to be sent or received. Users connect via dial-up with the communications server, which may be an infrastructure or a site resource.

DISN currently provides infrastructure-level remote access capability for both Unclassified and Secret users. DISN is accessible over the public switched telephone network (PSTN), the Defense Switched Network (DSN), and other systems. Site-level remote access can also be provided using similar equipment or by using a modem connected directly to a dedicated remote access server (RAS). In both situations users must have their own FORTEZZA cards to send or

[6] DISA, *DMS Organizational Messaging Concept of Operations,* Section 2.6, "Remote Access Services," April 30, 1999 (Update).

receive messages that require a signature and for encryption or decryption. The architecture for providing remote access to DMS users is shown in Figure 3.

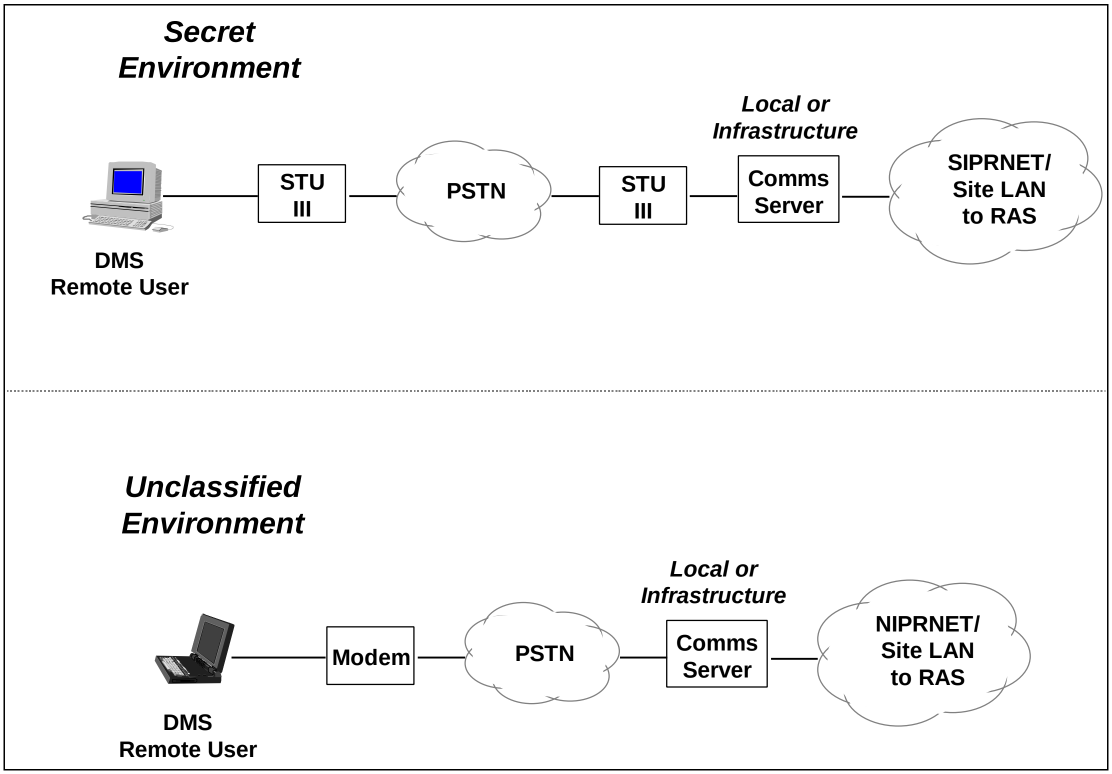
Figure 3. DMS Remote User (Dial-Up) Connectivity



Source: DISA, *DMS Organizational Messaging Concept of Operations*, Section 2.6, "Remote Access Services," April 30, 1999 (Update).

DMS users in the Secret domain use STU-III technology for a dial-up capability, and those in the Unclassified domain use the secure access control system (SACS), to provide link encryption between the Classified messaging client and the SIPRNet communications servers. These processes are depicted in Figure 4.

Figure 4. Remote Client Dial-Up Connections



Source: DISA, *DMS Organizational Messaging Concept of Operations*, Section 2.6, "Remote Access Services," April 30, 1999 (Update).

Roaming user access resembles a commercial roaming client model; users log onto any workstation on their local area network (LAN) and access their DMS mail. With server-based storage, users can access their DMS server from other workstations in a local DMS enclave and send or receive messages. Vendor products vary, however, in achieving this capability.

2.2.2 Mobile Access

A tactical or mobile DMS solution is a customized DISA service. DISA will work with any agency or service to tailor DMS services to provide a unique mobile DMS solution.[7] Because hardware, software, and infrastructure requirements vary from situation to situation, it is not

[7] An initial test deployment by the Air Force was viewed as impractical due to the unacceptable size and weight of the hardware required (see Daniel Verton, "AF Users Say DMS is Not Light or Lean Enough," *Federal Computer Week*, June 14, 1999).

possible to give a detailed solution here. One aspect of mobile DMS that DISA has specified is the use of FORTEZZA cards. Table 8 below details the guidelines for mobile FORTEZZA card usage.

Table 8. Use of FORTEZZA Card in a Mobile Environment

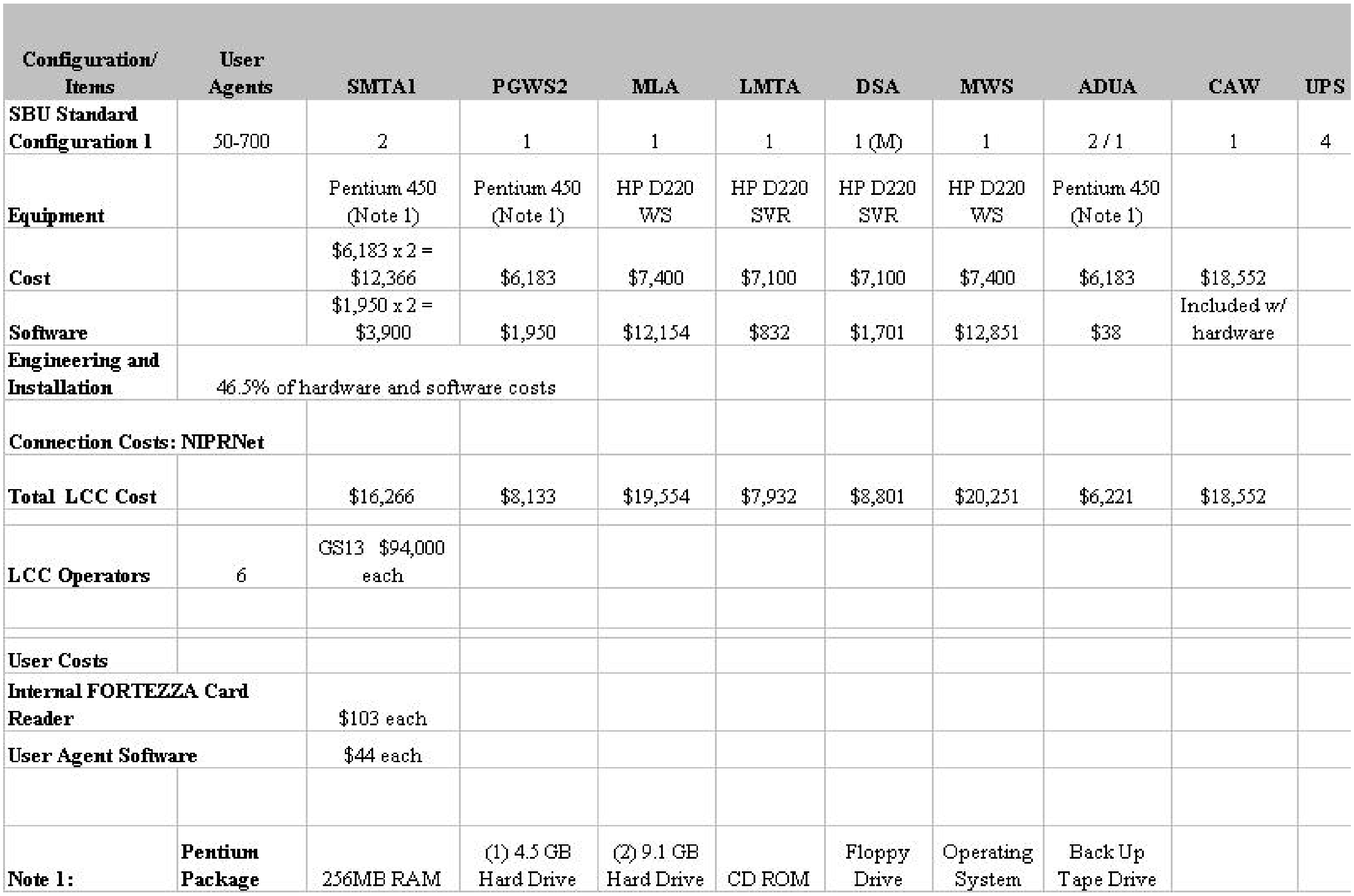
Capability	Mobile user capability must be limited to users having an operational requirement to process classified information outside the secure enclave.
Approval	Mobile users must be approved in writing by their department or agency to process classified information outside an approved facility.
Architecture	Mobile users must use FORTEZZA-enabled devices to access the classified enclave through a boundary (type 1 encryption) device recognized by NSA. Dial-in access through the boundary device must be based on more than one authentication technique.
Environment	Mobile users must be aware of their surroundings and ensure unauthorized individuals cannot view classified information on the computer's display. Mobile users must not print classified information when outside a classified enclave. Hardened chassis or Tempest requirements may apply, depending on the level of classification, location, and type of operating facility.
Field Storage of the FORTEZZA Card	The FORTEZZA card must be stored in its plastic case (in a lockable plastic bag, if needed). The mobile user must keep the FORTEZZA card in the storage case on his or her person or stored in a manner that minimizes the possibility of loss, unauthorized use, or tampering.
Card Classification	When users travel, FORTEZZA cards are classified only when inserted in the reader and unlocked by the personal identification number (PIN).
Removing FORTEZZA for Classified Card from Classified Enclave	Users with an operational requirement to remove the FORTEZZA card from a classified enclave must be authorized by the cognizant Designated Approving Authority and reminded of their responsibility to safeguard the card outside the secure enclave. Users who have additional requirements to conduct For Official User Only (FOUO)/SBU-level transactions outside an environment approved for Secret operation must be issued a separate FOUO/SBU-only FORTEZZA card.

Source: DISA, *DMS Organizational Messaging Concept of Operations*, "Attachment 2: Operational Procedures for FORTEZZA Card Utilization," DMS Release 2.1 Products, October 24, 1999 (Update).

2.3 Funding Considerations

When planning for DMS, one must consider the funding issues surrounding installation. Tables 9 and 10 show sample configurations for DMS implementation on both NIPRNet and SIPRNet systems. The tables include information such as costs of purchasing software and hardware, installation, and annual operations. Both of these installation charts are for departments or agencies with 50 to 700 user agents. The basic Pentium package is the same for both networks, as is the equipment on which DMS operates. Also, the connection costs for both networks are the same (i.e., $14,112). Note that if the department or agency installs only a SIPRNet system and not a NIPRNet system, it will have to incur the labor costs (i.e., $564,000) shown in Table 9. These tables do not represent installation costs simply for a DMS upgrade. For details on upgrading versions of DMS, see Appendix C.

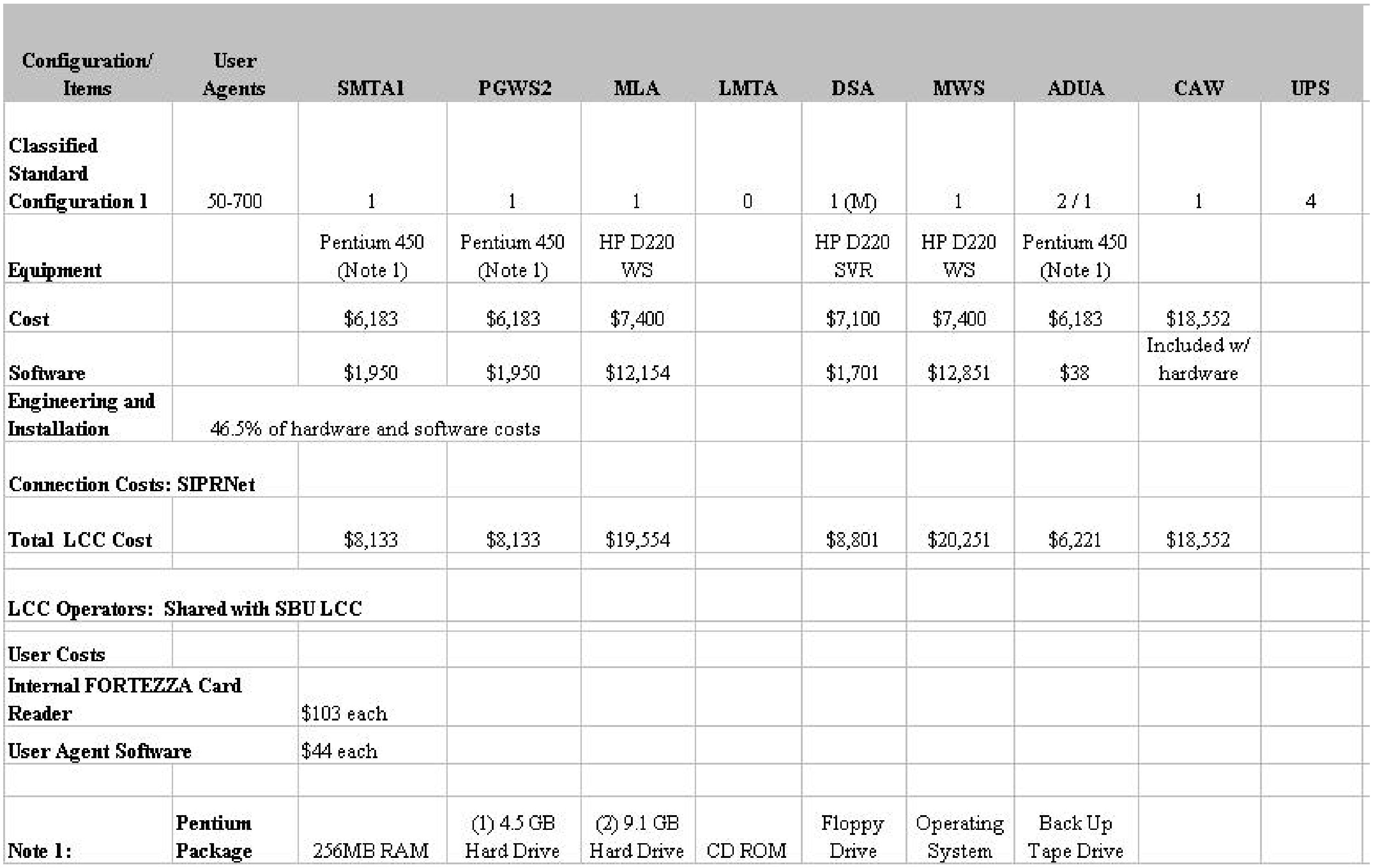
Table 9. Estimated Cost of Installing a DMS NIPRNet Infrastructure



Configuration/ Items	User Agents	SMTA1	PGWS2	MLA	LMTA	DSA	MWS	ADUA	CAW	UPS
SBU Standard Configuration 1	50-700	2	1	1	1	1 (M)	1	2 / 1	1	4
Equipment		Pentium 450 (Note 1)	Pentium 450 (Note 1)	HP D220 WS	HP D220 SVR	HP D220 SVR	HP D220 WS	Pentium 450 (Note 1)		
Cost		$6,183 x 2 = $12,366	$6,183	$7,400	$7,100	$7,100	$7,400	$6,183	$18,552	
Software		$1,950 x 2 = $3,900	$1,950	$12,154	$832	$1,701	$12,851	$38	Included w/ hardware	
Engineering and Installation	46.5% of hardware and software costs									
Connection Costs: NIPRNet										
Total LCC Cost		$16,266	$8,133	$19,554	$7,932	$8,801	$20,251	$6,221	$18,552	
LCC Operators	6	GS13 $94,000 each								
User Costs										
Internal FORTEZZA Card Reader		$103 each								
User Agent Software		$44 each								
Note 1:	**Pentium Package**	256MB RAM	(1) 4.5 GB Hard Drive	(2) 9.1 GB Hard Drive	CD ROM	Floppy Drive	Operating System	Back Up Tape Drive		

ADUA – Administrative Directory User Agent
CAW – Certification Authority Workstation
DSA – Directory System Agent
GB – Gigabyte
LMTA – Local Message Transfer Agent
MB – Megabyte
MLA – Mail List Agent
PGWS – Primary Groupware Server
MWS – Management Workstation
UPS – Uninterruptible Power Supply
RAM – Random Access Memory
ROM – Read-Only Memory
SMTA – Subordinate Message Transfer Agent
SVR – Server
WS – Workstation

Table 10. Estimated Cost of Installing a DMS SIPRNet Infrastructure



Configuration/ Items	User Agents	SMTA1	PGWS2	MLA	LMTA	DSA	MWS	ADUA	CAW	UPS
Classified Standard Configuration 1	50-700	1	1	1	0	1 (M)	1	2 / 1	1	4
Equipment		Pentium 450 (Note 1)	Pentium 450 (Note 1)	HP D220 WS		HP D220 SVR	HP D220 WS	Pentium 450 (Note 1)		
Cost		$6,183	$6,183	$7,400		$7,100	$7,400	$6,183	$18,552	
Software		$1,950	$1,950	$12,154		$1,701	$12,851	$38	Included w/ hardware	
Engineering and Installation	46.5% of hardware and software costs									
Connection Costs: SIPRNet										
Total LCC Cost		$8,133	$8,133	$19,554		$8,801	$20,251	$6,221	$18,552	
LCC Operators: Shared with SBU LCC										
User Costs										
Internal FORTEZZA Card Reader		$103 each								
User Agent Software		$44 each								
Note 1:	**Pentium Package**	256MB RAM	(1) 4.5 GB Hard Drive	(2) 9.1 GB Hard Drive	CD ROM	Floppy Drive	Operating System	Back Up Tape Drive		

ADUA – Administrative Directory User Agent
CAW – Certification Authority Workstation
DSA – Directory System Agent
GB – Gigabyte
LMTA – Local Message Transfer Agent

MB – Megabyte
MLA – Mail List Agent
PGWS – Primary Groupware Server
MWS – Management Workstation
UPS – Uninterruptible Power Supply

RAM – Random Access Memory
ROM – Read-Only Memory
SMTA – Subordinate Message Transfer Agent
SVR – Server
WS – Workstation

2.4 Conclusions and Recommendations

This guide is intended to assist NCS member agencies that will be implementing DMS through a transition from AUTODIN or an upgrade from an earlier version of DMS. As the expiration date of the AUTODIN system approaches, services and agencies need to begin the transition to ensure that messaging services are not interrupted, delayed, or wrongly classified. DMS provides a reliable, integrated common-user message system for organizational users in DoD and supporting agencies. The DMS global integrated directory service operates across multiple commercial vendor platforms, and the system efficiently utilizes the underlying DII network and services.

With each subsequent DMS release, the system will incorporate improvements in its baseline program capability. DMS users should become familiar with the primary components of the DMS system to implement its full capability. The four categories of components are message handling, directory, security, and systems management. Each component is essentially an "add-in" feature that departments and agencies choose to utilize in creating and adhering to appropriate operating policies. Therefore, DMS architecture will vary according to each organization's implementation plan.

Several issues must be taken into consideration when implementing the DMS system, including the following:

- The organization's requirements for DMS (e.g., security, software, hardware, and infrastructure)
- Alternate DMS access methods when establishing an LCC is not a requirement or an option
- Funding issues involved in installation.

Along with this document, departments and agencies that will be transitioning from AUTODIN to DMS, or be upgrading from a previous DMS version, are also encouraged to read and understand several other documents that detail how to integrate the DMS system into an organization. These documents (some of which are included as appendixes to this document) include the *Defense Message System (DMS) Product Plan* (Version 3.03; August 20, 1999), *Defense Message System Overview* (February 16, 1998), and *DMS Organizational Messaging Concept of Operations* (Updated April 30, 1999).

Lastly, departments and agencies are encouraged to participate in upcoming DMS conferences and planning meetings. Through these meetings, organizational end users can receive the latest updates on the DMS transition and can inform DISA, DMS team leads, and product vendors of unique requirements for future versions of DMS. For information on upcoming conferences and meetings, see the DMS Conferences Web site at [www.disa.mil/D2/dms/ conferences.html].

APPENDIX A

ACRONYMS AND ABBREVIATIONS

A

ACC	Area Control Center
ACP	Allied Communications Publication
ADUA	Administrative Directory User Agent
AF	Air
AFRC	Air Force Reserve Component
AFIWC	Air Force Information Warfare Center
AIG	Address Indicator Group
ANG	Air National Guard
AMHS	Automated Message Handling System
AMPE	Automated Message Processing Exchange
AOR	Area of Responsibility
ASC	Automated Switching Center
ASDC3I	Assistant Security of Defense for Command, Control, Communications and Intelligence
ASM	Area System Manager
AUTODIN	Automatic Digital Network

B

BGWS	Bridgehead Gateway Server

BLII	Base Level Infrastructure Initiative
BMTA	Backbone Message Transfer Agent

C

C	CONFIDENTIAL
C4I	Command, Control, Communications, Computers and Intelligence
CA	Certification Authority
CAD	Collective Address Designator
CAW	Certification Authority Workstation
CCPL	Compliant Certified Products List
CDC	Central Directory Component (for the Message Conversion System)
CIO	Chief Information Officer
CINC(s)	Commander(s)-in-Chief
CITS	Combat Information Transport Services (USAF)
CKL	Compromised Key List
CMP	Common Message Processor
CNO	Chief of Naval Operations
COE	Common Operating Environment
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial-off-the-Shelf

CRI	Collective Routing Indicator
CRL	Certificate Revocation List
CSP	Common Security Protocol
CY	Calendar Year

D

DCL	Data Communications, Limited (Vendor)
DDA	Domain Defined Attribute
DFAS	Defense Finance and Accounting Service
DIB	Directory Information Base
DII	Defense Information Infrastructure
DII CC	Defense Information Infrastructure Control Concept
DISA	Defense Information Systems Agency
DISC4	Director of Information Systems for Command, Control, Communications and Computers
DISN	Defense Information Systems Network
DIT	Directory Information Tree
DLA	Defense Logistics Agency
DMDS	DMS Message Dissemination System (USMC)
DMS	Defense Message System
DN/DDN	Distinguished Name/Directory Distinguished Name

DoD	Department of Defense
DoN, DON	Department of the Navy
DSA	Directory System Agent; Digital Signature Algorithm
DSSCS	Defense Special Security Communications System
DSN	Defense Switched Network
DTH	DMS Transition Hub
DTRA	Defense Threat Reduction Agency
DUA	Directory User Agent

E

EAM	Emergency Action Message
EC	Enabling Capability; Electronic Commerce
EFA	Engineering Field Activity (USN)
E-Mail	Electronic Mail
EoS	Elements of Service

F

FAQ	Frequently Asked Question
FD	Fielding Decision
FL	Format Line
FLA	Flexible Local Architecture
FOUO	For Official Use Only

FTP	File Transfer Protocol
FY	Fiscal Year

G

GAL	Global Address List
GB	Gigabyte
GDSA	Global Directory System Agent
GENSER	General Service
GOSC	Global Operations and Security Center(s)
GSM	Global System Manager
GSU	Geographically Separated Units
GWS	Groupware Server

H

HAG	High Assurance Guard
HQ	Headquarters

I

IAVA	Information Assurance Vulnerability Alert
IC	Intelligence Community
ICDMO	Intelligence Community DMS Management Office
IDUA	Integrated Directory User Agent
INE	In-line Network Encryption

IOC	Initial Operating Capability
ISDN	Integrated Services Digital Network
ISSO	Information System Security Officer
IT	Information Transfer/Technology
IW	Information Warfare

J

JANAP	Joint Army Navy Air Force Publication
JCCC	Joint Communications Control Center
JCS	Joint Chiefs of Staff
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System

K

Kbps	Kilo Bits Per Second
KEA	Key Exchange Algorithm

L

LAN	Local Area Network
LCC	Local Control Center(s)
LDSA	Local Directory Service Agent
LMC	Lockheed Martin Corporation
LMFS	Lockheed Martin Federal Systems

LMTA	Local Message Transfer Agent
LSM	Local System Manager

M

MAG	Medium Assurance Guard
MAISRC	Major Automated Information System Review Council
MAN	Metropolitan Area Network
MAPI	Mail Application Program Interface
MB	Megabyte
MCS	Message Conversion System
MDS	Message Dissemination System (USMC)
MDT	Message Distribution Terminal
MEK	Message Encryption Key
MFI	Multi-Function Interpreter
MIS	Management Information Systems
MISSI	Multi-level Information System Security Initiative
ML	Mail List
MLA	Mail List Agent
MROC	Multi-command Required Operational Capability
MS	Message Store; Microsoft®

MSP	Message Security Protocol
MTA	Message Transfer Agent
MTS	Message Transfer System
MWS	Management Work Station

N

NAB	Notes Address Book
NATO	North Atlantic Treaty Organization
NCS	National Communications System
NCTAMS	Naval Computer and Telecommunications Area Master Station
NCTC	NAVCOMTELCOM (Naval Computer and Telecommunications Command)
NCTS	Naval Computer and Telecommunications Station
NIMA	National Imagery and Mapping Agency
NIPRNet	Non-classified Internet Protocol Router Network
NOC	Network Operations Center (USMC)
NSA	National Security Agency
NTP	Network Time Protocol; Naval Telecommunications Procedures

O

OIPT	Overarching Integrated Product Team
OMNCS	Office of the Manager, National Communications System
O/R	Originator/Recipient

ORA	Organizational Registration Authority
ORAR	Originator Requested Alternate Recipient
OU	Organizational Unit
OUA	Organizational User Account
	P
P1	X.400 Message Transfer Protocol
P42	Message Type for MSP
P772	Military Message Type (X.400 with military extensions)
PAA	Policy Approving Authority
PAB	Personal Address Book
PAP	Password Authorization Protocol
PC	Personal Computer
PCA	Policy Creation Authority
PCMCIA	Personal Computer Memory Card International Association
PGWS	Primary Groupware Server
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLA	Plain Language Address
PMO	Program Management Office
POC	Point of Contact

POP	Point of Presence
PPP	Point to Point Protocol
POM	Program Objectives Memorandum/Manual
POTS	"Plain Old Telephone System"; the normal commercial or base telephone service
PSTN	Public Switched Telephone Network
PUA	Profiling User Agent

Q

QOS	Quality of Service

R

RA	Release Authority
RAM	Random Access Memory
RAS	Remote Access Service/Server
RDN	Relative Distinguished Name
ROM	Read-Only Memory
ROMC	Required Operational Messaging Characteristics
ROSC	Regional Operations and Security Center(s)
RSAR	Recipient Specified Alternate Recipient
RSM	Regional System Manager

S

S	Secret

SA	System Administrator
SACS	Secure Access Control System
S/A	Service/Agency
S/C	Secret/Confidential
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SDA	System Design Architecture
SDD	Secure Data Device
SHA	Secure Hash Algorithm
SHD	Special Handling Designator
SIC	Subject Indicator Code
SIPRNet	Secret Internet Protocol Router Network
SMI	Security Management Infrastructure
SMTA	Subordinate Message Transfer Agent
SMTP	Simple Mail Transfer Protocol
SMS	Service Management Station
SNMP	Simple Network Management Protocol
SOA	Separate Operating Activities (USAF)
SOP	Standard Operating Procedure
SPECAT	Special Category

SRA	Sub-Registration Authority
SRAM	Static Random Access Memory
SSG	Standard Systems Group (USAF)
STE	Secure Terminal/Telephone Equipment
STIG	Security Technical Implementation Guidelines
STU-III	Secure Telephone Unit - III
SVR	Server

T

TCP/IP	Transmission Control Protocol/Internet Protocol
TF	Task Force
TIB	Technical Information Bulletin
TS	Top Secret

U

U	Unclassified
U.S., US	United States
UA	User Agent
UCDC, U-CDC	Unclassified [portion of the] Central Directory Component
UPS	Uninterruptible Power Supply
USCG	U.S. Coast Guard
USMCEB	U.S. Military Communications and Electronics Board

UTC	Coordinated Universal Time*

V

V	Version
VPN	Virtual Private Network

W

WAN	Wide Area Network
WESTHEM	Western Hemisphere
WS	Workstation

X

Y

Y2K	Year 2000

Z

*This is the correct English wording. The abbreviation "UTC" was the result of a compromise between the French "TUC" (for "Temps universal coordonné") and the English "CUT".

APPENDIX B

TRANSITIONING TO DMS

Note

This appendix reproduces exactly Appendix B from Defense Information Systems Agency, *DMS Organizational Messaging Concept of Operations,* DMS Release 2.1 Products, October 24, 1999. This material is reproduced for reference purposes.

Table of Contents

List of Figures

List of Tables

SECTION I

Organizational Messaging During AUTODIN Transition

B.1 Introduction

The purpose of this appendix is to provide guidance and understanding to organizations transitioning their messaging system to the DMS. The information provided in this appendix is divided into two sections. Section I provides a basic overview of the transition scenarios and implementation approaches for fielding DMS Release 2.1 products. The concepts and implementation approaches outlined in this section are based on the DMS Release 2.1 architecture outlined in paragraph 1.3.3 of the DMS Organization Messaging CONOPS. Section II of this document provides a more detailed guide for transition strategies and implementation concepts.

B.1.1 DMS Release 2.1 Implementation Options

The R2.1 DMS transition architecture will support Top Secret Collateral (TS/C) and Secret and below messaging for users on the SIPRNET and unclassified messaging services for users connected to the NIPRNET. The High Assurance Guard (HAG) will support Unclassified messaging between the DMS Secret and below and Unclassified messaging domains. Top Secret DMS messaging is provided to a *"top secret only"* user domain that is connected via a virtual private network that uses the SIPRNET as the underlying network infrastructure. Only top secret message traffic is supported within the DMS TS/C domain. DMS products installed within the TS/C domain support top secret message exchange between users within the top secret enclave. Each of the messaging domains will be connected to the AUTODIN. The connectivity to AUTODIN will be restricted to only allow the exchange of messages within the classification capabilities of each supported messaging domain. The DMS Release 2.1 transition architecture will support four basic transition options. These supported implementation options are listed below:

a. Option - 1 Split Domain Secret and Below Messaging Support

Secret and below messaging support between DMS users within the SIPRNET enclave and support for outbound secret and below messaging connectivity to AUTODIN

Support for the delivery of classified message traffic from AUTODIN to recipients within the SIPRNET enclave

Unclassified messaging support between DMS users within the NIPRNET enclave with support for inbound and outbound unclassified messaging connectivity to AUTODIN

Unclassified messaging support between DMS users within the SIPRNET enclave and the NIPRNET enclave via the use of a Guard

b. Option – 2 Single Domain Secret and Below Messaging Support

Secret and below messaging between DMS users within the SIPRNET enclave with support for inbound and outbound secret and below messaging connectivity to AUTODIN

Unclassified messaging support between DMS users within the SIPRNET enclave and the NIPRNET enclave via the use of a Guard

c. Option - 3 Unclassified Messaging Support

Unclassified messaging between DMS users within the NIPRNET enclave with support for inbound and outbound unclassified messaging connectivity to AUTODIN

Unclassified messaging support between DMS users within the SIPRNET enclave and the NIPRNET enclave via the use of a Guard

d. Option – 4 Top Secret Collateral Messaging Support

Top Secret Collateral messaging between DMS users within the TS/C enclave with support for inbound and outbound unclassified messaging connectivity to AUTODIN

Section II of this appendix expands the above implementation options into four transitional architectures types that include a stand alone TS/C implementation approach and multiple Guard implementation scenarios and message distribution options between the SIPRNET and NIPRNET messaging enclaves.

B.1.2 Plain Language Address (PLA) Naming Strategy

Organizations transitioning to DMS are required to establish distinguished names and organizational identities for DMS users that are designated to send and receive messages from the AUTODIN. The distinguished name of each DMS organizational messaging user with release authority privileges must be associated with a PLA that identifies that individual or his organization to AUTODIN users. There is an option of using an existing PLA or assigning a new PLA for this purpose. When an organization's existing PLA is used, AUTODIN subscribers will route messages to the organization's DMS recipients by addressing messages to the organization's existing PLA and a Routing Indicator (RI) that is assigned to a MFI located in the organization's servicing DTH. Organizations that elect transition options that involve split delivery of classified and unclassified messages to the DMS SIPRNET and NIPRNET enclaves will be assigned a classified and an unclassified RI that will be used along with the selected PLA for routing messages.

Alternatively, new PLA(s) may be assigned to correspond to an organization's assigned DMS organizational messaging release authorities. In either option (existing PLA or new PLA approach), the implementing organization can develop a transition strategy that associates multiple DMS distinguished names to a single PLA or select an implementation approach that associates a single distinguished name to a unique PLA. DISA recommends the multiple distinguished name to single PLA approach. Figure

B-1 illustrates the distinguished name to PLA association and directory structure for the recommended PLA naming strategy.

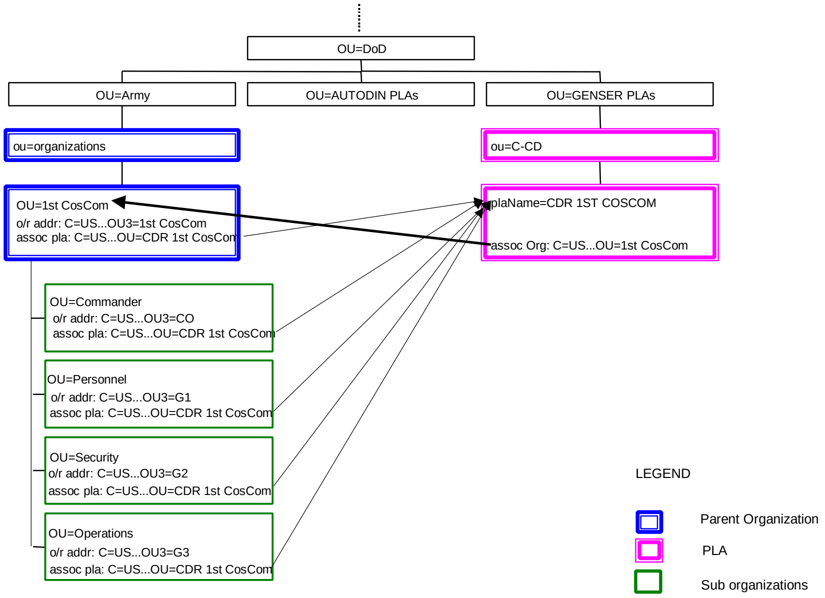


Figure B.1-1 PLA-DN Association

B.1.2.1 Centralized and De-Centralized Message Distribution

Organizations that elect Secret and below and Unclassified transition strategies will have the option of receiving incoming DMS messages directly into the mailboxes of designated organizational users or having all incoming messages arrive first at a centralized distribution point, such as a PUA or other such device, before final delivery. The term “centralized delivery” is associated with the PUA delivery option. De-centralized delivery refers to a message delivery approach that requires delivery directly to an organizational user’s mailbox. Both of these two options are supportable by the DMS Release 2.1 PLA naming strategies. However, the centralized delivery approach will provide the greatest implementation flexibility for supporting messaging between the SIPRNET and NIPRNET enclaves using the Guard. Initially, DMS release 2.1 will only support de-centralized delivery to TS/C users.

B.1.2.2 Dual Delivery and Single Delivery

An organization may need assurance that it receives all messages intended for it during the AUTODIN to DMS transition. Consequently, the organization may elect to have delivery of messages to both its AUTODIN delivery point and its DMS delivery point. This is referred to as dual delivery and can be carried out in two different ways. It can be effected by using two destination PLAs, the existing AUTODIN PLA and a new DMS transitional PLA, to validate that all messages received at its AUTODIN delivery point are also received at the DMS mailbox. Dual delivery may also be effected with a single PLA by using the Message Conversion System (MCS) dual delivery feature if the originator of the message involved is authorized use of the DMS, or by requesting message originators to insert a single PLA twice with different RI sideroutes. The MCS feature, if available to the AUTODIN user, will automatically sideroute the PLA with two different RIs – one indicating the AUTODIN recipient and the other indicating the responsible MFI. The MCS dual delivery option is limited by restrictions on the numbers of RIs a dual delivery recipient may have and the limited processing capacity of the MCS system. As a result of these limitations, the MCS dual delivery approach should be implemented only as an interim short term transition solution.

Also note, dual delivery for collective members is effected by the organization's PLAs remaining in the AUTODIN collective for a specified transition period after the organization's DMS DN has been added to the equivalent DMS collective (e.g. a Mail List).

An organization may elect instead to use only one destination corresponding to its DMS mailbox. This option is defined as single delivery or a hard-cutover transition approach.

B.1.3 DMS Addressing Strategies

The following addressing strategies are provided as general guidance to the DMS message originator to ensure proper delivery of Secret and below and Unclassified messages. It involves message delivery and receipt options for DMS organizations split between two domains (NIPRNet and SIPRNet), DMS organizations with releasers separate and unique from the organization, and organizations desiring dual delivery (i.e., AUTODIN and DMS) of messages during transition. Also, for additional information, see Appendix C (C.2.5.1 Messaging Across Security Domains).

Note: For information on MSP 3.0 transitional directories, see Appendix C (C.2.4.3 Directory Structure and Naming). It discusses utilization of the (n) appended to DNs for Unclassified users and the (s) appended to DNs for Secret users.

1. Split Domain – Two Unclassified Organizational DNs

If an organization wishes to communicate Unclassified messages between the two SIPRNet and NIPRNet domains within its own organization, it will need two Unclassified DNs. One DN will correspond to a mailbox in its SIPRNet domain and the other to a mailbox in its NIPRNet domain. This will allow entities on the SIPRNet to send and receive Unclassified mail.

An organization with the two Unclassified organizational DNs described in the last paragraph will need to provide a distinction between the two in the spelling of the DN. The DN that should be addressed to officially receive Unclassified incoming organizational mail should have something that distinguishes it as so. Otherwise a message originator does not know which DN to use as the address.

2. Replies in Split Domains

These types of organizations can occur in two instances: organizations split across security domains, and organizations fronted by a PUA. It is important to ensure replies get to the correct organizational delivery point (or how to make the "Reply To" function work)

a. For a Releaser with a DN Different than the Official Organizational DN

An organizational releaser must select the Element of Service (EOS) called Reply Recipients, i.e., the "Reply To" function, upon message origination and place the organization's name and address in it (the organization might be a PUA or shared mailbox). This enables replies to his/her message to return to the organization's official entry point instead of returning to the organizational releaser's mailbox.

b. For a Split Domain

For a split domain, all incoming Unclassified message traffic is set to arrive only at the NIPRNet domain. If an Unclassified message transmitted from the organization's SIPRNet domain is replied to, it will return to the SIPRNet domain. If this reply must return not to the originator but to the NIPRNet domain, then the original message must have the "Reply To" function set to do so.

3. Dual Delivery – Sending a DMS message to a Dual Delivery Organization

When sending a message from DMS to an organization that requires dual delivery during transition, the DMS message originator must ensure that both the organization's AUTODIN address and DMS address are placed in the "TO" line. Both addresses can be found under the AUTODIN PLAs subtree directory entry for that organization. The AUTODIN PLA address is an entry under this subtree and the DMS address is contained in its "See Also" attribute.

B.1.4 DMS Release 2.1 Option One (Organizations with a presence on Both Classified and Unclassified LANs)

This option is for use by an organization that receives and sends its Secret/Confidential (S/C) messages from its DMS Secret domain. It receives from AUTODIN its Unclassified (U) messages at its DMS Unclassified domain. Both the organization's Secret and Unclassified domains send Unclassified messages to AUTODIN. The majority, about 75%, of the organizations transitioning fall into this category. The figure below is an example of the messaging architecture for use by such organizations. Note that this example does not use a PUA for DMS centralized message delivery. The architecture also allows for dissemination of Unclassified message traffic through the Guard.

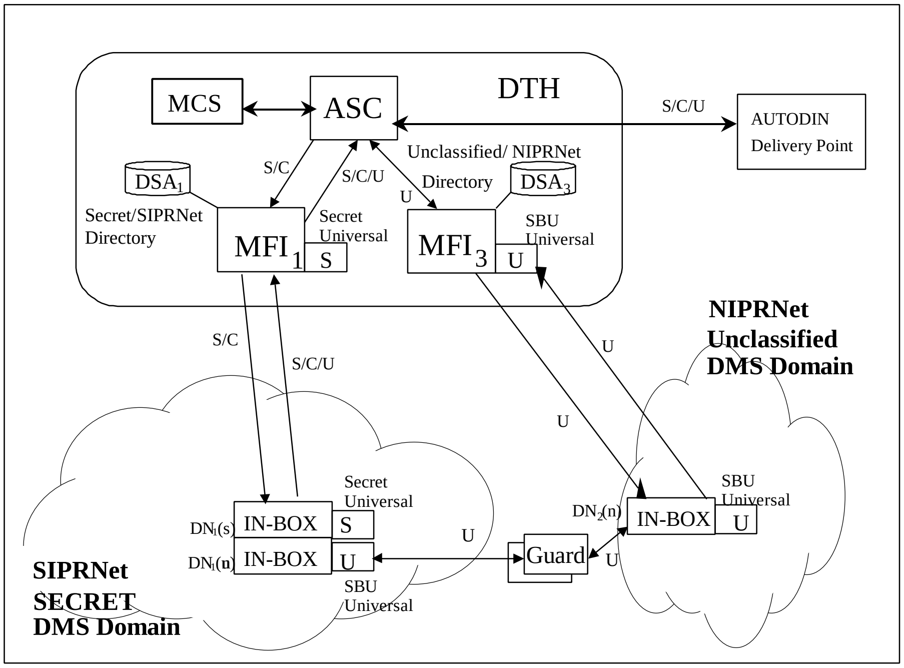


Figure B.1-2 Transition Architecture for Organizations Using Classified (SIPRNet) and Unclassified (NIPRNet) LANs

Inbound (AUTODIN-to-DMS) Message Flow

The organization receives its Secret and Confidential (S/C) messages from AUTODIN via MFI$_1$ to its Secret domain. MFI$_1$ uses its Secret universal (Secret Domain FORTEZZA personality) to deliver S/C messages to the Organization's Secret domain primary groupware server. The message recipients are represented as an organizational in-box corresponding to DN$_1$(s).

All Unclassified message traffic from AUTODIN is received via MFI$_3$ to the DMS Unclassified domain. MFI$_3$ uses its SBU universal (Unclassified Domain FORTEZZA personality) to deliver messages to the Organization's Unclassified primary groupware server. The recipients are represented here as an organizational in-box corresponding to DN$_2$(n) for the Unclassified Domain. Onward delivery of Unclassified messages through the Guard to the Secret domain is possible.

Outbound (DMS-to-AUTODIN) Message Flow

An organizational releaser in the Secret domain must use the appropriate DN$_1$(s) to send outbound (DMS-to-AUTODIN) Secret, Confidential, and Unclassified messages to MFI$_1$. The organizational releaser must use a Secret universal (Secret Domain FORTEZZA personality) to send S/C/U messages to MFI$_1$ because MFI$_1$ only has a Secret universal (Secret Domain FORTEZZA personality) to decrypt the message. MFI$_1$ then forwards the message to AUTODIN.

An organizational releaser in the Secret domain can send Unclassified messages to recipient(s) in the Unclassified domain via the Guard. It can send Unclassified messages from its in-box labeled as DN$_1$(n) using the SBU universal to its own organizational Unclassified NIPRNET domain in-box, DN$_2$(n).

DN$_2$(n) releases its outbound (DMS-to-AUTODIN) Unclassified messages to MFI$_3$ using its SBU universal (Unclassified Domain FORTEZZA personality) to decrypt the message. MFI$_3$ then forwards the message to AUTODIN. An organizational releaser in the Unclassified Domain can send Unclassified messages to recipient(s) in the Secret Domain. It can send to the organization's own Secret Domain Unclassified in-box denoted by DN$_1$(n) in the figure.

B.1.5 DMS Release 2.1 Option Two (Organizations on Classified LANs)

This option is for use by an organization that sends/receives S/C/U (or S/C only) message traffic from/at its Secret domain. About 20% of the total number of DoD organizations transitioning populate this category.

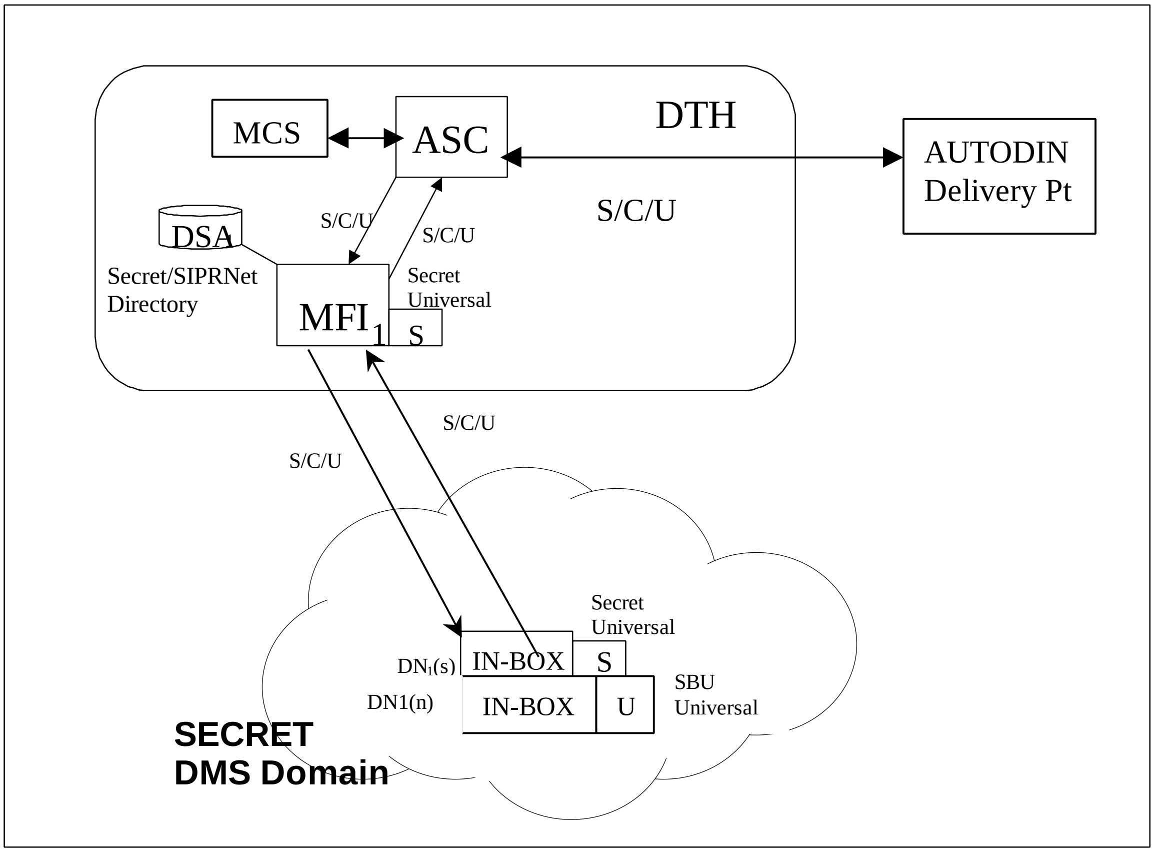


Figure B.1-3 Transition Architecture SIPRNet Only

Inbound (AUTODIN-to-DMS) Message Flow

This organization receives its Secret, Confidential or Unclassified (S/C/U) (or S/C only) messages from AUTODIN via MFI$_1$ to its Secret DMS domain. The MFI$_1$ uses its Secret universal to deliver the S/C/U messages to the organization's primary groupware server. The recipients are represented here as an organizational in-box corresponding to DN$_1$(s).

Outbound (DMS-to-AUTODIN) Message Flow

The organizational releaser may originate Secret, Confidential or Unclassified (S/C/U) (or S/C only) messages for that organization. Since this organization is only in an Unclassified domain it can only send messages to recipient(s) that have an Unclassified identity (SBU universal). All outbound messages must either be sent to AUTODIN recipient(s), remain within the Unclassified Domain, or be sent through the guard to an organization's Unclassified identity in the Secret Domain. Note that an organization that sends/receives Unclassified traffic may require the use of a second DN (e.g. DN1(n) to send Unclassified messages to Organizations who are only on Unclassified LANs (DMS Release 2.1 Option Three). All AUTODIN bound S/C/U (or S/C only) message traffic is delivered to the MFI$_1$ using the Secret universal (Secret Domain FORTEZZA personality) to decrypt the message. The MFI$_1$ then forwards the traffic to AUTODIN.

B.1.6 DMS Release 2.1 Option Three (Organizations on Unclassified LANs)

This option is for use by an organization that sends/receives only Unclassified message traffic from/at its Unclas domain. About 5% of the total number of DoD organization transitioning populate this category.

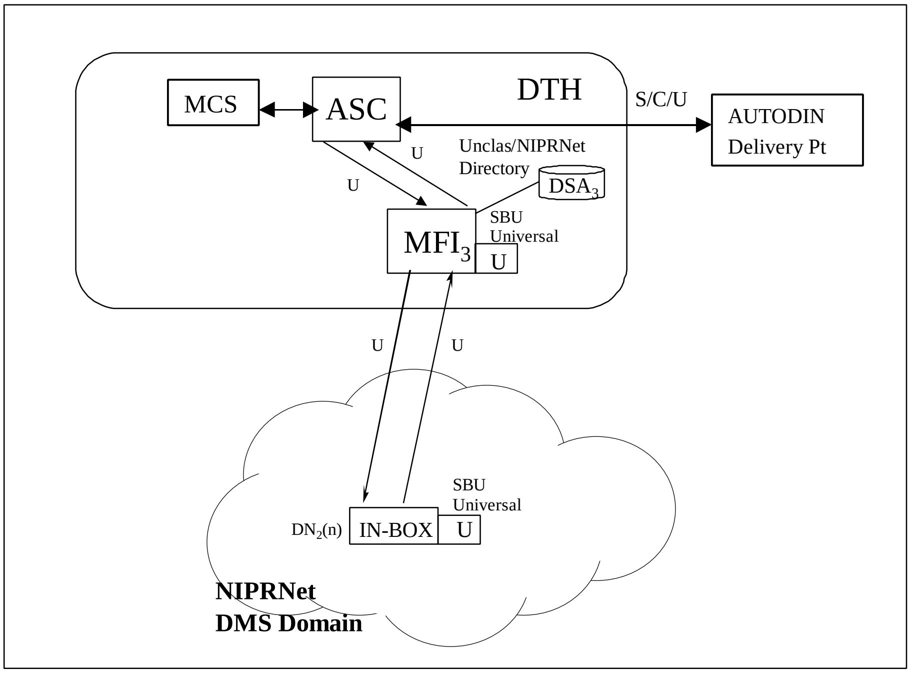


Figure B.1-4 Transition Architecture NIPRNet Only

Inbound (AUTODIN-to-DMS) Message Flow

This organization does not receive any classified traffic. Its Unclassified messages are received from AUTODIN via MFI_3 to its Unclassified DMS domain. The MFI_3 uses its SBU universal to deliver the messages to the organization's primary groupware server. The recipients are represented here as an organizational in-box corresponding to DN_2(n).

Outbound (DMS-to-AUTODIN) Message Flow

The organizational releaser may originate only Unclassified messages for the organization. Since this organization is only in an Unclassified domain it can only send messages to recipient(s) that have an Unclassified identity (SBU universal). All outbound messages must either be sent to AUTODIN recipient(s), remain within the Unclassified Domain, or be sent through the guard to an organization's Unclassified identity in the Secret Domain. All AUTODIN bound message traffic is delivered to the MFI_3 using the SBU universal (FORTEZZA personality) to decrypt the message. The MFI_3 then forwards the traffic to AUTODIN.

B.1.7 DMS Release 2.1 Option Four (TS/C Messaging on Classified LANs)

This option is for use by an organization that sends/receives only TS/C message traffic from/at its Top Secret domain. Less than 5% of the total number of DoD organization transitioning populate this category.

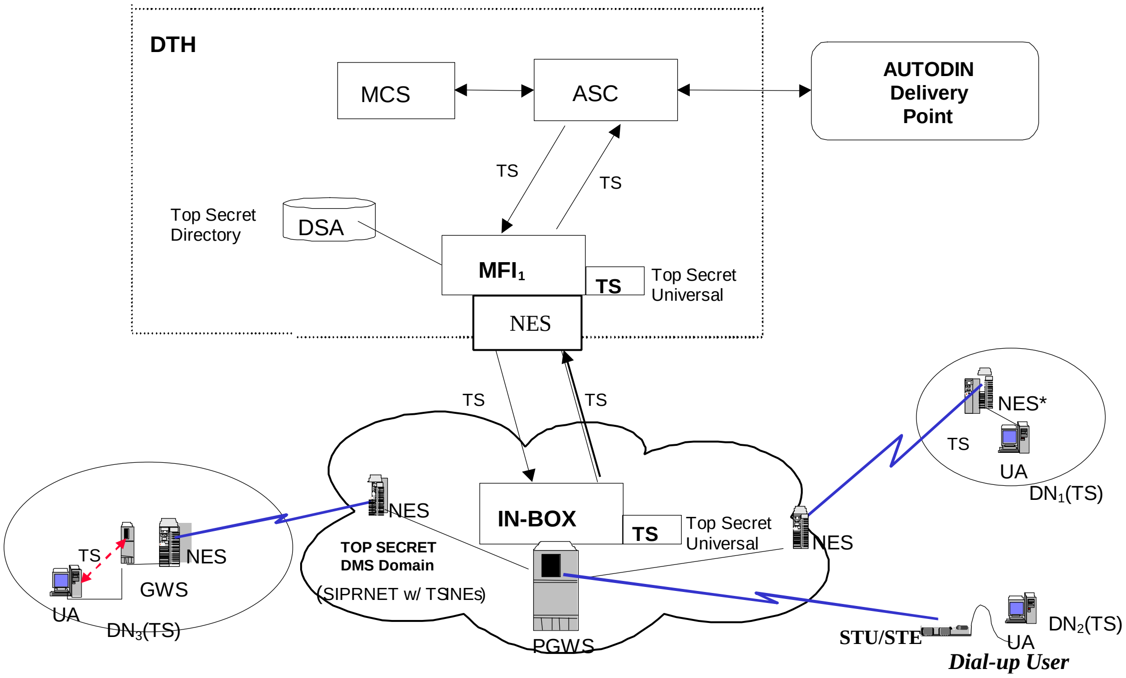


Figure B.1-5 Transition Architecture TS/C Only

Inbound (AUTODIN-to-DMS) Message Flow

This organization only receives TS/C traffic. Its TS/C messages are received from AUTODIN via MFI$_1$ to its TS/C DMS domain. The MFI$_1$ uses its TS universal to deliver the messages to the organization's supporting groupware server. The AUTODIN has been modified to deliver "TS/C" only traffic to MFI$_1$. The TS/C recipients typically access their groupware server mail boxes via dial-up connections to download received messages. The TS/C recipients typically use STU IIIs to provide secure access to the server to download and decrypt incoming messages. However, TS/C users may also receive service via either directly connected groupware servers or stand alone UAs.

Outbound (DMS-to-AUTODIN) Message Flow

The organizational releaser may only originate TS/C messages for the organization. Since this organization is only in a “TS/C only” domain, it cannot send messages to recipient(s) in the Secret and below and Unclassified domains. All outbound messages must either be sent to AUTODIN recipient(s) or remain within the TS/C domain. All AUTODIN message traffic is delivered to the MFI_1 using the TS/C universal (FORTEZZA personality) to sign and encrypt the message. The MFI_1 then forwards the traffic to AUTODIN. Assigned TS/C certificates on the recipient’s FORTEZZA card are used to sign and encrypt outgoing messages and decrypt incoming messages.

B.1.8 Additional Delivery Options from AUTODIN

For an unspecified period of time, during transition to DMS, organizations have the option to receive “dual delivery” of AUTODIN messages.

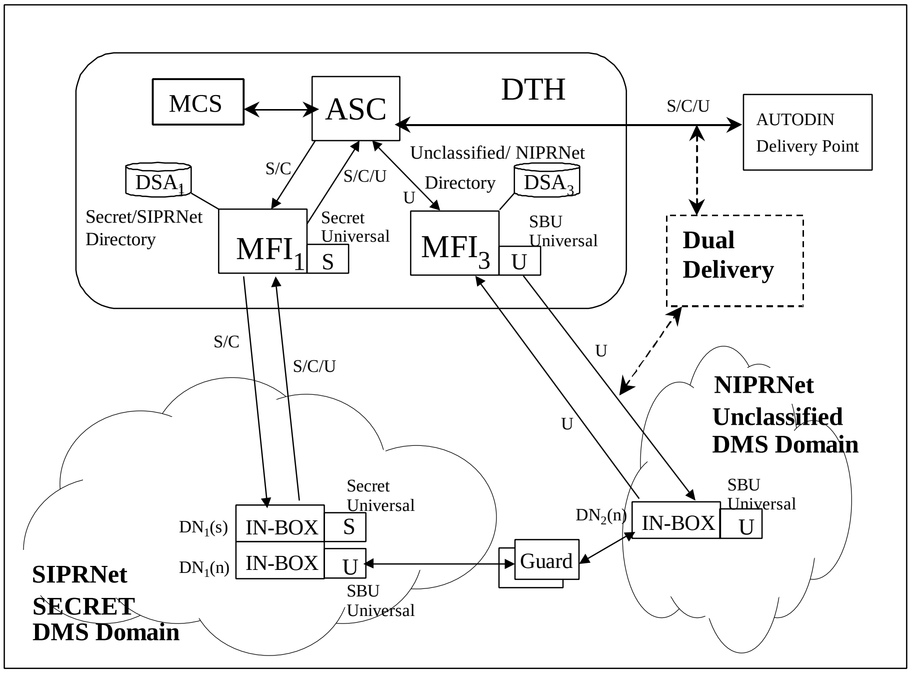


Figure B.1-6 Example of Dual Delivery of Unclassified Traffic

B.1.9 Authorized MCS Users

If the organization is an authorized user of the MCS system, for PLA to RI conversion, then the organization may request dual delivery of messages to their AUTODIN PLA by security level. This is accomplished in the MCS system by placing an additional RI in each message of the selected security level, which would point to the DMS MFI for delivery to DMS. While operating in this mode the organization would get two deliveries, one to their AUTODIN commcenter and one to their DMS primary groupware server in-box for access by a client.

This method will dual deliver **ONLY** *messages which pass through the MCS* for PLA processing, **NOT** *all* messages. AUTODIN corespondents originating messages to your organization whose messages do not address the MCS for PLA processing will not be dual delivered unless the messages are manually dual routed as described below in the paragraph titled “Non MCS Users”.

B.1.10 Non MCS Users

If the organization is not an authorized user of the MCS system, then dual delivery can be accomplished by having the organization's users or correspondents insert its PLA twice. Once normally and once with the DMS MFI RI as a sideroute and include the DMS MFI's RI in the header of the message. Each message addressed in that way will be delivered to both the AUTODIN commcenter and to the DMS MFI for delivery to the organization's primary groupware server for delivery to a UA.

SECTION II

Target DMS Transition and Implementation Planning Guidance

B.2 DMS Release 2.1 Architectures

The transition architectures contained in this section of Appendix B have been included so transitioning users will be better able to plan their transition efforts. Some of the architectures contain a High Assurance Guard to enable Unclassified messaging between Unclassified NIPRNet and Secret SIPRNet domains.

B.2.1 Transitional Messaging Architectures

Along with a system of PLA addressing, an appropriate transitional messaging architecture is part of successful message delivery during transition. The transitional messaging architecture type is based on where an organization “lives;” whether it lives on both an Unclassified LAN and a Classified LAN known as a “split organization”, whether it lives on a Classified LAN, or whether it lives on an Unclassified LAN.

There are three general types of organizational architectures with sixteen (bulleted below) specific architectural subtypes available for organizations to use for transition to DMS. They are briefly summarized below. Help in ascertaining the best-fit architecture for a given organization’s needs follows in the next section beginning with the questionnaire.

B.2.1.1 Type A Transitional Messaging Architecture

Type A: For an organization that splits its messaging between Classified and Unclassified LANs. This transition architecture type is for use by an organization that receives and sends its Secret/Confidential (S/C) messages from its DMS Secret domain. It receives from AUTODIN its Unclassified (U) messages at its DMS Unclassified domain. Both the organization’s Secret and Unclassified domains send U messages to AUTODIN. The majority, about 75%, of the organizations transitioning fall into this category. If needed, DMS can further disseminate Unclassified message traffic that was delivered from AUTODIN to the Unclassified domain via a Guard to a final destination in the DMS Secret domain.

- SubType A(1): For an organization that uses centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

- SubType A(2): For an organization that uses centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

- SubType A(3): For an organization that uses de-centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

- SubType A(4): For an organization that uses de-centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

B.2.1.2 Type B Transitional Messaging Architecture

Type B: For an organization that communicates solely on a Classified LAN.

SubType B(1): This transitional architecture type is for use by an organization that sends/receives S/C/U message traffic from/at its Secret domain. About 20% of the total number of DoD organizations transitioning populate this category.

- SubType B(1)a: For an organization that uses centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

- SubType B(1)b: For an organization that uses centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

- SubType B(1)c: For an organization that uses de-centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

- SubType B(1)d: For an organization that uses de-centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

SubType B(2): This transitional architecture type is for use by an organization that sends/receives S/C message traffic ONLY at its Secret domain. Less than 5% of the total number of DoD organizations transitioning populate this category.

- SubType B(2)a: For an organization that uses centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

- SubType B(2)b: For an organization that uses centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.
- SubType B(2)c: For an organization that uses de-centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.
- SubType B(2)d: For an organization that uses de-centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

B.2.1.3 Type C Transitional Messaging Architecture

Type C: For an organization that communicates solely on an Unclassified LAN. It sends/receives unclassified message traffic ONLY. This type comprises about 5% of the total number of DoD organizations transitioning to DMS.

- SubType C(1): For an organization that uses centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.
- SubType C(2): For an organization that uses centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.
- SubType C(3): For an organization that uses de-centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.
- SubType C(4): For an organization that uses de-centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

B.2.2 Organizational Questionnaire

The transition strategy selection process begins by filling out the following questionnaire, labeled Table B.2-1. The questionnaire's purpose is to point to the best Secret and below and Unclassified transition architecture and PLA naming strategy for an organization based on the answers given. The transition strategy is based in part the choice of centralized/de-centralized organizational DMS message distribution. Other factors that influence the organization's transition strategy are classification levels of organizational messages sent and received, the organization's use of Top Secret, Secret high and/or Unclassified LANs, and the preference for either a dual (both to AUTODIN and DMS) or single (to DMS only) organizational message delivery approach.

Table B.2-1 Organizational Questionnaire

Item No.	Do You:	Yes	No
(Pick Only ONE Distribution Option, 1 or 2:)			
1.	Plan to use centralized distribution (such as a PUA or message center) for incoming organizational messages?		
2.	Plan to use decentralized distribution (direct delivery to an in-box) for incoming organizational messages?		
(Pick Only ONE Unclassified Message Reception Option, 3, 4, or 5:)			
3.	Receive most or all of your Unclassified organizational messages at your Unclassified (NIPRNET) domain?		
4.	Receive most or all of your Unclassified organizational messages at your Secret (SIPRNET) domain?		
5.	Not receive Unclassified messages?		
(Pick Only ONE Classified Message Reception Option, 6 or 7)			
6.	Receive Secret and Confidential organizational messages at your Secret (SIPRNET) domain?		
7.	Not receive Secret and Confidential organizational messages, only Unclassified messages?		
(Pick Only ONE Unclassified Message Generation Option, 8, 9, 10, or 11:)			
8.	Send most or all of your organizational Unclassified messages from your Unclassified (NIPRNET) domain?		
9.	Send most or all of your Unclassified organizational messages from your Secret (SIPRNET) domain?		

Item No.	**Do You:**	**Yes**	**No**
10.	Send Unclassified organizational messages from both your Unclassified (NIPRNET) and Secret (SIPRNET) domains?		
11.	Not send Unclassified messages?		
(Pick Only ONE Classified Message Generation Option, 12 or 13:)			
12.	Send Secret and Confidential organizational messages from your Secret high (SIPRNET) domain?		
13.	Not send Secret and Confidential organizational messages, only Unclassified organizational messages?		
(Pick only ONE Delivery Option, 14 or 15:)			
14.	Desire dual message delivery to both old AUTODIN address and new DMS address until confident about DMS delivery?		
15.	Desire message delivery to only one address, the DMS address, during transition?		
If Item No. 14 was answered Yes, then pick only ONE Dual Delivery Option, 16 or 17:			
16.	Desire to use a transitional PLA for dual delivery?		
17.	Desire to use a transitional RI (via MCS dual delivery service or manual address)?		
Items You answered Yes to: *(e.g., items 2, 3, 7, 8, 13, 14, 16)*			

B.2.3 Best Fit Transition Architecture

The next item in the process, after completing the questionnaire, is to refer to the following table. Table B.2-2 provides a best-fit transition architecture and PLA Naming Strategy based on the answers from the questionnaire. The full description of the transition architecture is provided in the referenced section.

Table B.2-2. Best Fit Transition Architecture and PLA Naming Strategy

Best Fit No.	If you answered Yes to item number(s):	Then, use the following Transition Architecture:	And, use the following PLA Naming Strategy: Refer to Table B.2-3	Explanation, Go To Section:
1)	1, 3, 6, 8/9/10, 12, 14, 16	A(1)	N1	B.3.1
2)	1, 3, 6, 8/9/10, 12, 14, 17	A(1)	N2	B.3.1
3)	1, 3, 6, 8/9/10, 12, 15	A(2)	N3	0
4)	2, 3, 6, 8/9/10, 12, 14, 16	A(3)	N4	0
5)	2, 3, 6, 8/9/10, 12, 14, 17	A(3)	N5	0
6)	2, 3, 6, 8/9/10, 12, 15	A(4)	N6	0
7)				
8)				
9)				
10)				
11)	1, 4, 6, 9, 12, 14, 16	B(1)a	N1	0
12)	1, 4, 6, 9, 12, 14, 17	B(1)a	N2	0
13)	1, 4, 6, 9, 12, 15	B(1)b	N3	0
14)	2, 4, 6, 9, 12, 14, 16	B(1)c	N4	0

Best Fit No.	If you answered Yes to item number(s):	Then, use the following Transition Architecture:	And, use the following PLA Naming Strategy: Refer to Table B.2-3	Explanation, Go To Section:
15)	2, 4, 6, 9, 12, 14, 17	B(1)c	N5	0
16)	2, 4, 6, 9, 12, 15	B(1)d	N6	0
17)	1, 5, 6, 11, 12, 14, 16	B(2)a	N1	0
18)	1, 5, 6, 11, 12, 14, 17	B(2)a	N2	0
19)	1, 5, 6, 11, 12, 15	B(2)b	N3	0
20)	2, 5, 6, 11, 12, 14, 16	B(2)c	N4	0
21)	2, 5, 6, 11, 12, 14, 17	B(2)c	N5	0
22)	2, 5, 6, 11, 12, 15	B(2)d	N6	0
23)	1, 3, 7, 8, 13, 14, 16	C(1)	N1	0
24)	1, 3, 7, 8, 13, 14, 17	C(1)	N2	0
25)	1, 3, 7, 8, 13, 15	C(2)	N3	0
26)	2, 3, 7, 8, 13, 14, 16	C(3)	N4	0
27)	2, 3, 7, 8, 13, 14, 17	C(3)	N5	0
28)	2, 3, 7, 8, 13, 15	C(4)	N6	0

Note that in some cases items 8/9/10 were listed concurrently. In these instances any one of the options 8, 9, or 10, can be selected.

B.2.4 PLA/RI Naming Strategy

The PLA/RI naming strategy in Table B.2-3 is based on choice of (1) centralized or de-centralized message distribution, (2) dual or single message routing, and, (3) DMS Transitional PLA or original AUTODIN PLA. These transition options are further defined in Paragraph B.1.2.

Table B.2-3 PLA/RI Naming Strategy

PLA/RI Naming Strategy No.	Delivery Strategy	Required PLA Value	Required RI Value	Delivery Point
N1 (transitional PLA)	Dual Routing to Centralized Distribution Point	DMS Transitional PLA Original AUTODIN PLA	DMS Destination RI (MFI) AUTODIN Destination RI	Organization's DMS PUA Organization's AUTODIN Comm Center
N2 (transitional RI)	Dual Routing to Centralized Distribution Point	Original AUTODIN PLA	DMS Destination RI (MFI) AUTODIN Destination RI	Organization's DMS PUA Organization's AUTODIN Comm Center
N3 (hard cutover)	Single Routing to Centralized DMS Distribution Point	Original AUTODIN PLA	DMS Destination RI (MFI)	Organization's DMS PUA

PLA/RI Naming Strategy No.	Delivery Strategy	Required PLA Value	Required RI Value	Delivery Point
N4 (transitional PLA)	Dual Routing to De-Centralized Destination	DMS Transitional PLA Original AUTODIN PLA	DMS Destination RI (MFI) AUTODIN Destination RI	Organization's DMS in-box (shared mailbox) Organizational Roles' in-boxes (writer-to-reader) Organization's AUTODIN Comm Center
N5 (transitional RI)	Dual Routing to De-Centralized Destination	Original AUTODIN PLA	DMS Destination RI (MFI) AUTODIN Destination RI	Organization's DMS in-box (shared mailbox) Organizational Roles' in-boxes (writer-to-reader) Organization's AUTODIN Comm Center
N6 (hard cutover)	Single Routing to De-Centralized DMS Destination	Original AUTODIN PLA	DMS Destination RI (MFI)	Organization's DMS in-box (shared mailbox) Organizational Roles' in-boxes (writer-to-reader)

B.3 Transitional Messaging Architectures

This section contains descriptions of the specific messaging architectures that an organization can elect to use based on its messaging needs and the transition strategy derived from Table B.2-2 in section 0.

B.3.1 Transition Architecture SubType A(1):

Type A: For an organization that splits its messaging between Classified and Unclassified LANs. This transition architecture type is for use by an organization that receives and sends its Secret/Confidential (S/C) messages from its DMS Secret domain. It receives from AUTODIN its Unclassified (U) messages at its DMS Unclassified domain. Both the organization's Secret and Unclassified domains send U messages to AUTODIN. The majority, about 75%, of the organizations transitioning fall into this category. If needed, DMS can further disseminate Unclassified message traffic that was delivered from AUTODIN to the Unclassified domain via a Guard to a final destination in the DMS Secret domain.

- SubType A(1): For an organization that uses centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

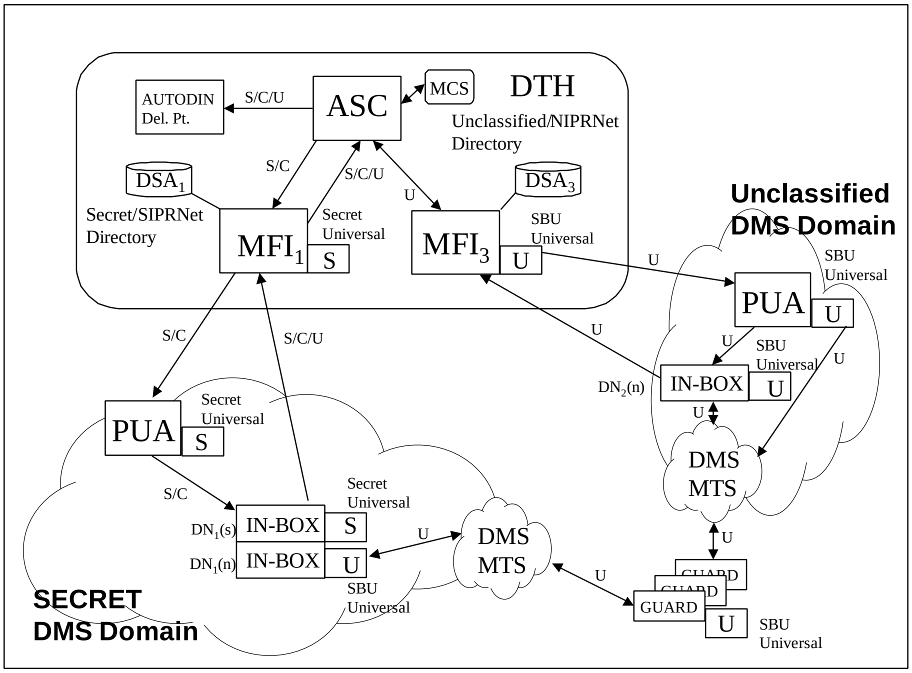


Figure B.3-1 Organizational Transition Architecture SubType A(1)Inbound (AUTODIN-to-DMS) to organization's AUTODIN delivery point

The organization elected to have dual delivery of messages and as such will receive a duplicate copy in its AUTODIN delivery point of all messages sent to its DMS mailboxes.

Inbound (AUTODIN-to-DMS) to DMS message flow

A Type A(1) organization receives its Secret and Confidential (S/C) messages from AUTODIN via MFI_1 to its Secret domain. MFI_1 uses its Secret universal (Secret Domain

FORTEZZA personality) to deliver S/C messages to the DMS Secret organizational PUA.

All Unclassified message traffic from AUTODIN is received via MFI$_3$ to the DMS Unclassified domain. MFI$_3$ uses its SBU universal (Unclassified Domain FORTEZZA personality) to deliver messages to the organization's Unclassified PUA. The PUA can further disseminate Unclassified messages through the DMS MTS and the Guard to the organization's Secret domain Unclassified in-box corresponding to DN$_1$(n).

Outbound (DMS-to-AUTODIN) from DMS message flow

An organizational releaser in the DMS Secret domain must use DN$_1$(s) to send outbound (DMS-to-AUTODIN) Secret, Confidential, and Unclassified messages to MFI$_1$. The organizational releaser must use a Secret universal (Secret Domain FORTEZZA personality) to send S/C/U messages to MFI$_1$ because MFI$_1$ only has a Secret universal (Secret Domain FORTEZZA personality) to decrypt the message. MFI$_1$ then looks up DN$_1$(s)'s PLA for placement into the "From" line (Format Line 6) of the translated AUTODIN message. MFI$_1$ gets PLAs for the "To" and "Info" lines (Format Lines 7 and 8) from the MFI's DDA field. MFI$_1$ completes the translation and forwards the message to AUTODIN.

An organizational releaser in the DMS Secret domain must send two Unclassified messages if it has recipients in both AUTODIN and in the DMS Unclassified domain. The releaser must use the Secret universal (Secret Domain FORTEZZA personality)/Secret DN$_1$(s) to send to AUTODIN and a SBU universal (Unclassified Domain FORTEZZA personality)/Unclassified DN$_1$ to send to DMS Unclassified domain recipients. The organizational releaser uses the Unclassified organizational entity name, DN$_1$(n), to send Unclassified messages via the DMS MTS and the Guard directly to its organizational Unclassified domain in-box, DN$_2$(u), or it can route the message via the PUA.

DN$_2$(n) releases its outbound (DMS-to-AUTODIN) Unclassified messages to MFI$_3$ using its SBU universal (Unclassified Domain FORTEZZA personality). MFI$_3$ looks up DN$_2$(n)'s PLA to place into the "From" line (Format Line 6) of the translated AUTODIN message. MFI$_3$ gets PLAs for the "To" and "Info" lines (Format Lines 7 and 8) from the MFI's DDA field. MFI$_3$ then forwards the message to AUTODIN.

B.3.2 Transition Architecture SubType A(2):

Type A: For an organization that splits its messaging between Classified and Unclassified LANs. This transition architecture type is for an organization that receives and sends its Secret/Confidential (S/C) messages from its DMS Secret domain. It receives from AUTODIN its Unclassified (U) messages at its DMS Unclassified domain. Both the organization's Secret and Unclassified domains send U messages to AUTODIN. The majority, about 75%, of the organizations transitioning fall into this category. If needed, DMS can further disseminate Unclassified message traffic that was delivered from AUTODIN to the Unclassified domain via a Guard to a final destination in the DMS Secret domain.

- SubType A(2): For an organization that uses centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

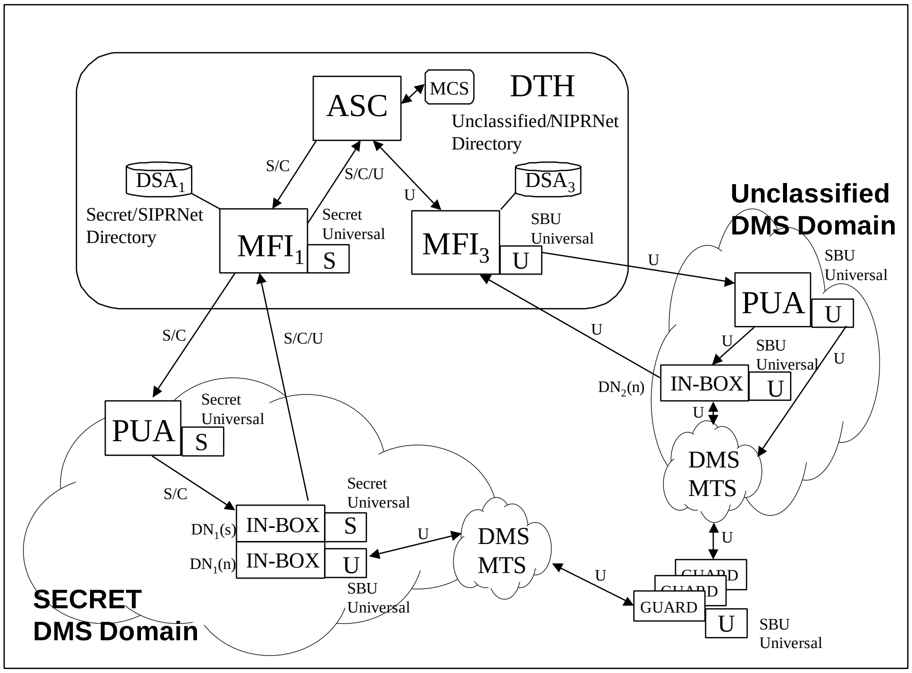


Figure B.3-2 Organizational Transition Architecture SubType A(2)

Inbound (AUTODIN-to-DMS) to DMS message flow

A Type A(2) organization receives its Secret and Confidential (S/C) messages from AUTODIN via MFI$_1$ to its Secret domain. MFI$_1$ uses its Secret universal (Secret Domain FORTEZZA personality) to deliver S/C messages to the DMS Secret organizational PUA.

All Unclassified message traffic from AUTODIN is received via MFI$_3$ to the DMS Unclassified domain. MFI$_3$ uses its SBU universal (Unclassified Domain FORTEZZA personality) to deliver messages to the organization’s Unclassified PUA. The PUA can further disseminate Unclassified messages through the DMS MTS and the Guard to the organization’s Secret domain Unclassified in-box corresponding to DN$_1$(n).

Outbound (DMS-to-AUTODIN) from DMS message flow

An organizational releaser in the DMS Secret domain must use DN$_1$(s) to send outbound (DMS-to-AUTODIN) Secret, Confidential, and Unclassified messages to MFI$_1$. The organizational releaser must use a Secret universal (Secret Domain FORTEZZA personality) to send S/C/U messages to MFI$_1$ because MFI$_1$ only has a Secret universal (Secret Domain FORTEZZA personality) to decrypt the message. MFI$_1$ then looks up DN$_1$(s)’s PLA for placement into the “From” line (Format Line 6) of the translated AUTODIN message. MFI$_1$ gets PLAs for the “To” and “Info” lines (Format Lines 7 and 8) from the MFI’s DDA field. MFI$_1$ completes the translation and forwards the message to AUTODIN.

An organizational releaser in the DMS Secret domain must send two Unclassified messages if it has recipients in both AUTODIN and in the DMS Unclassified domain. The releaser must use the Secret universal (Secret Domain FORTEZZA personality)/Secret DN$_1$(s) to send to AUTODIN and a SBU universal (Unclassified Domain FORTEZZA personality)/Unclassified DN$_1$ to send to DMS Unclassified domain recipients. The organizational releaser uses the Unclassified organizational entity name, DN$_1$(n), to send Unclassified messages via the DMS MTS and the Guard directly to its organizational Unclassified domain in-box, DN$_2$(n), or it can route the message via the PUA.

DN$_2$(n) releases its outbound (DMS-to-AUTODIN) Unclassified messages to MFI$_3$ using its SBU universal (Unclassified Domain FORTEZZA personality). MFI$_3$ looks up DN$_2$(n)’s PLA to place into the “From” line (Format Line 6) of the translated AUTODIN message. MFI$_3$ gets PLAs for the “To” and “Info” lines (Format Lines 7 and 8) from the MFI’s DDA field. MFI$_3$ then forwards the message to AUTODIN.

B.3.3 Transition Architecture SubType A(3):

Type A: For an organization that splits its messaging between Classified and Unclassified LANs. This transition architecture type is for use by an organization that receives and sends its Secret/Confidential (S/C) messages from its DMS Secret domain. It receives from AUTODIN its Unclassified (U) messages at its DMS Unclassified domain. Both the organization’s Secret and Unclassified domains send U messages to AUTODIN. The majority, about 75%, of the organizations transitioning fall into this category. If needed, DMS can further disseminate Unclassified message traffic that was delivered from

AUTODIN to the Unclassified domain via a Guard to a final destination in the DMS Secret domain.

- SubType A(3): For an organization that uses de-centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

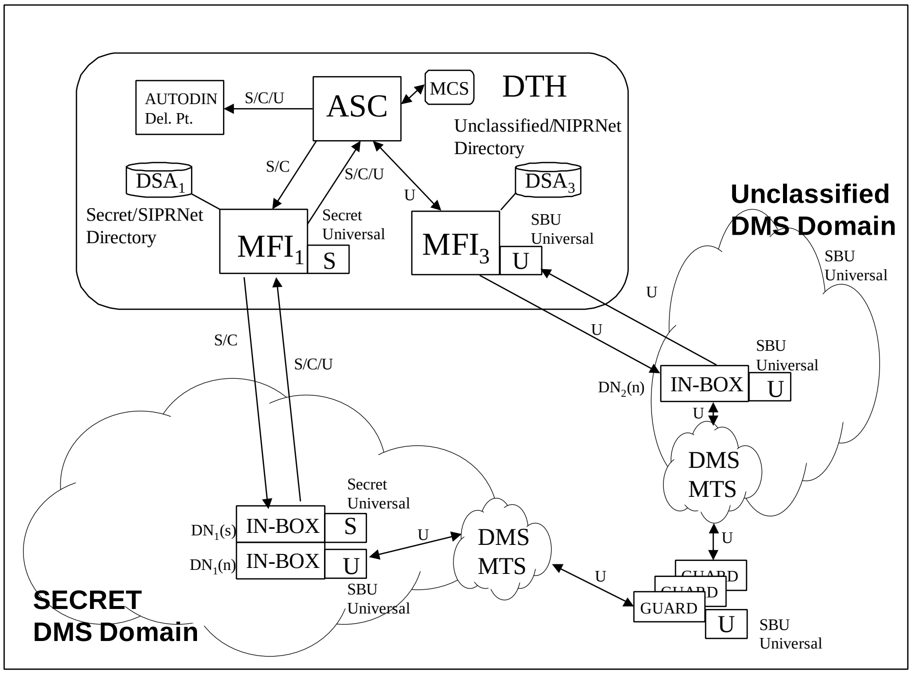


Figure B.3-3 Organizational Transition Architecture SubType A(3)

Inbound (AUTODIN-to-AUTODIN) to organization's AUTODIN delivery point

The organization elected to have dual delivery of messages and as such will receive a duplicate copy at its AUTODIN delivery point of all messages sent to its DMS mailboxes.

Inbound (AUTODIN-to-DMS) to DMS message flow

A Type A(3) organization receives its Secret and Confidential (S/C) messages from AUTODIN via MFI$_1$ to its Secret domain. MFI$_1$ uses its Secret universal (Secret Domain

FORTEZZA personality) to deliver S/C messages to the DMS Secret organizational role’s in-box corresponding to DN$_1$(s).

All Unclassified message traffic from AUTODIN is received via MFI$_3$ to the DMS Unclassified domain. MFI$_3$ uses its SBU universal (Unclassified Domain FORTEZZA personality) to deliver messages directly to the organizational role’s in-box corresponding to DN$_2$(n). The organizational role recipient can further disseminate Unclassified messages through the DMS MTS and the Guard to the organization’s Secret domain Unclassified in-box corresponding to DN$_1$(n).

Outbound (DMS-to-AUTODIN) from DMS message flow

An organizational releaser in the DMS Secret domain must use DN$_1$(s) to send outbound (DMS-to-AUTODIN) Secret, Confidential, and Unclassified messages to MFI$_1$. The organizational releaser must use a Secret universal (Secret Domain FORTEZZA personality) to send S/C/U messages to MFI$_1$ because MFI$_1$ only has a Secret universal (Secret Domain FORTEZZA personality) to decrypt the message. MFI$_1$ then looks up DN$_1$(s)’s PLA for placement into the “From” line (Format Line 6) of the translated AUTODIN message. MFI$_1$ gets PLAs for the “To” and “Info” lines (Format Lines 7 and 8) from the MFI’s DDA field. MFI$_1$ completes the translation and forwards the message to AUTODIN.

An organizational releaser in the DMS Secret domain must send two Unclassified messages if it has recipients in both AUTODIN and in the DMS Unclassified domain. The releaser must use the Secret universal (Secret Domain FORTEZZA personality)/Secret DN$_1$(s) to send to AUTODIN and a SBU universal (Unclassified Domain FORTEZZA personality)/Unclassified DN$_1$(n) to send to DMS Unclassified domain recipients. The organizational releaser uses the Unclassified organizational entity name, DN$_1$(n), to send Unclassified messages via the DMS MTS and the Guard directly to its organizational Unclassified domain in-box, DN$_2$(n).

DN$_2$(n) releases its outbound (DMS-to-AUTODIN) Unclassified messages to MFI$_3$ using its SBU universal (Unclassified Domain FORTEZZA personality). MFI$_3$ looks up DN$_2$(n)’s PLA to place into the “From” line (Format Line 6) of the translated AUTODIN message. MFI$_3$ gets PLAs for the “To” and “Info” lines (Format Lines 7 and 8) from the MFI’s DDA field. MFI$_3$ then forwards the message to AUTODIN.

B.3.4 Transition Architecture SubType A(4):

Type A: For an organization that splits its messaging between Classified and Unclassified LANs. This transition architecture type is for use by an organization that receives and sends its Secret/Confidential (S/C) messages from its DMS Secret domain. It receives from AUTODIN its Unclassified (U) messages at its DMS Unclassified domain. Both the organization’s Secret and Unclassified domains send U messages to AUTODIN. The majority, about 75%, of the organizations transitioning fall into this category. If needed, DMS can further disseminate Unclassified message traffic that was delivered from AUTODIN to the Unclassified domain via a Guard to a final destination in the DMS Secret domain.

- SubType A(4): For an organization that uses de-centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

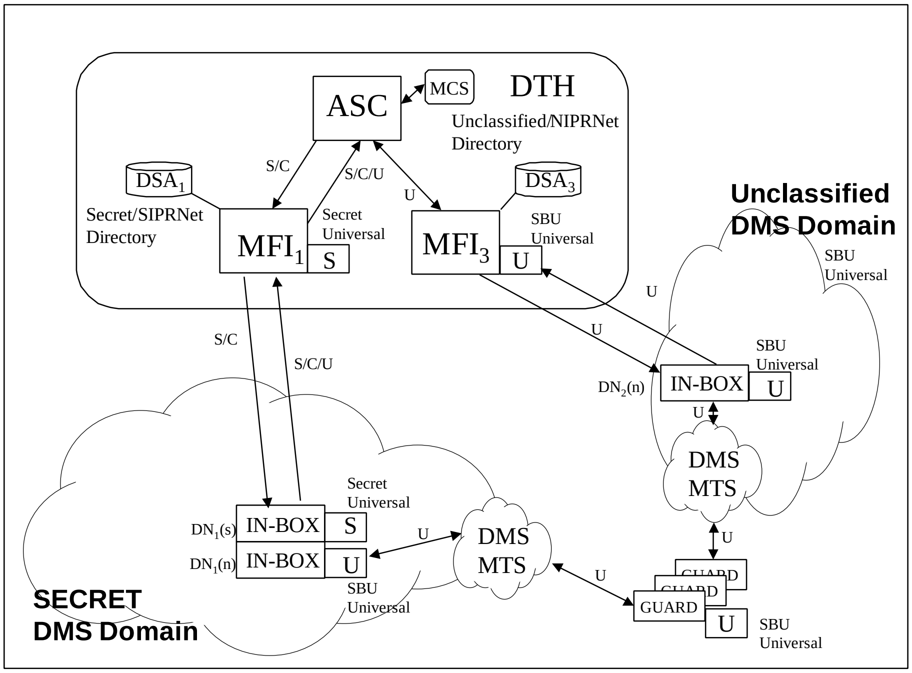


Figure B.3-4 Organizational Transition Architecture SubType A(4)

Inbound (AUTODIN-to-DMS) to DMS message flow

A Type A(4) organization receives its Secret and Confidential (S/C) messages from AUTODIN via MFI$_1$ to its Secret domain. MFI$_1$ uses its Secret universal (Secret Domain FORTEZZA personality) to deliver S/C messages directly to the DMS Secret organizational role’s in-box corresponding to DN$_1$(s).

All Unclassified message traffic from AUTODIN is received via MFI_3 to the DMS Unclassified domain. MFI_3 uses its SBU universal (Unclassified Domain FORTEZZA personality) to deliver messages directly to the organizational role's in-box corresponding to DN_2(n). The organizational role recipient can further disseminate Unclassified messages through the DMS MTS and the Guard to the organization's Secret domain Unclassified in-box corresponding to DN_1(n).

Outbound (DMS-to-AUTODIN) from DMS message flow

An organizational releaser in the DMS Secret domain must use DN_1(s) to send outbound (DMS-to-AUTODIN) Secret, Confidential, and Unclassified messages to MFI_1. The organizational releaser must use a Secret universal (Secret Domain FORTEZZA personality) to send S/C/U messages to MFI_1 because MFI_1 only has a Secret universal (Secret Domain FORTEZZA personality) to decrypt the message. MFI_1 then looks up DN_1(s)'s PLA for placement into the "From" line (Format Line 6) of the translated AUTODIN message. MFI_1 gets PLAs for the "To" and "Info" lines (Format Lines 7 and 8) from the MFI's DDA field. MFI_1 completes the translation and forwards the message to AUTODIN.

An organizational releaser in the DMS Secret domain must send two Unclassified messages if it has recipients in both AUTODIN and in the DMS Unclassified domain. The releaser must use the Secret universal (Secret Domain FORTEZZA personality)/Secret DN_1(s) to send to AUTODIN and a SBU universal (Unclassified Domain FORTEZZA personality)/Unclassified DN_1(n) to send to DMS Unclassified domain recipients. The organizational releaser uses the Unclassified organizational entity name, DN_1(n), to send Unclassified messages via the DMS MTS and the Guard directly to its organizational Unclassified domain in-box, DN_2(n).

DN_2(n) releases its outbound (DMS-to-AUTODIN) Unclassified messages to MFI_3 using its SBU universal (Unclassified Domain FORTEZZA personality). MFI_3 looks up DN_2(n)'s PLA to place into the "From" line (Format Line 6) of the translated AUTODIN message. MFI_2 gets PLAs for the "To" and "Info" lines (Format Lines 7 and 8) from the MFI's DDA field. MFI_2 then forwards the message to AUTODIN.

B.3.5 Transition Architecture SubType B(1)a:

Type B: For an organization that communicates solely on a Classified LAN.

> SubType B(1): This transitional architecture type is for use by an organization that sends/receives S/C/U message traffic from/at its Secret domain. About 20% of the total number of DoD organizations transitioning populate this category.

- SubType B(1)a: For an organization that uses centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

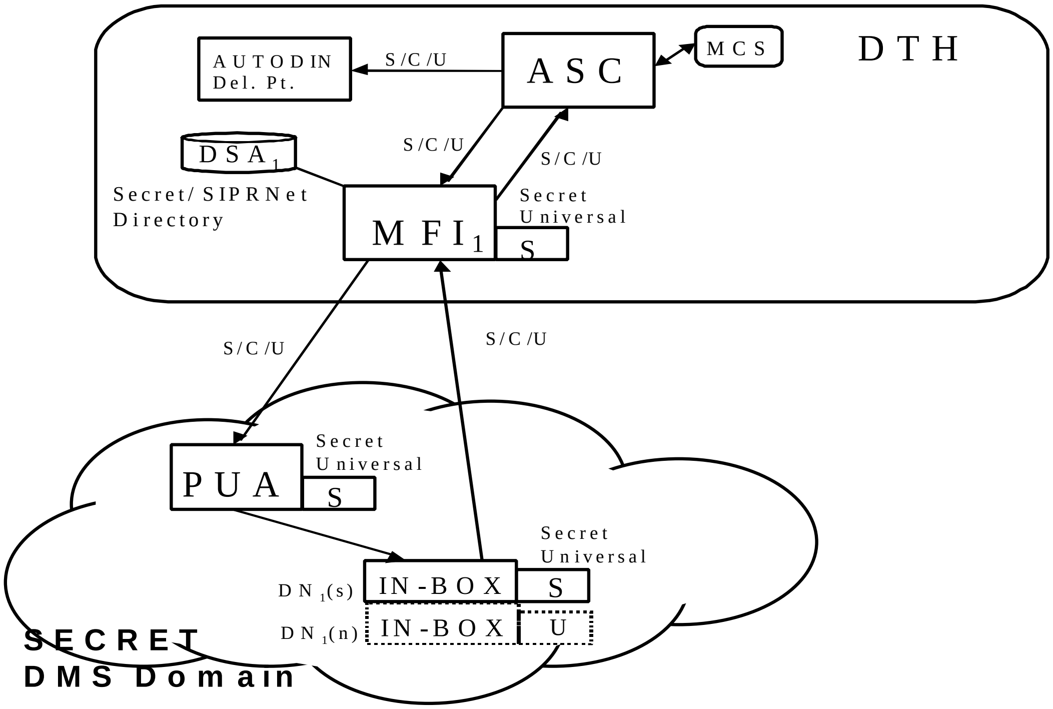


Figure B.3-5 Organizational Transition Architecture SubType B(1)a

Inbound (AUTODIN-to-DMS) to Organization's AUTODIN delivery point

This organization receives a copy of all levels of classified messages S/C/U at its AUTODIN delivery point until it is confident about delivery to its DMS in-box.

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type B(1)a organization receives its S/C/U messages from AUTODIN via MFI$_1$ to its Secret DMS domain. MFI$_1$ uses its Secret universal (Secret Domain FORTEZZA personality) to deliver the S/C/U messages to the organization's Secret centralized distribution point depicted by a PUA. Then, the PUA delivers to its Secret domain recipients using the Secret universal (Secret Domain FORTEZZA personality). The recipients are represented here as an organizational in-box corresponding to DN$_1$(s).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

The organizational releaser in the DMS Secret domain must use the Secret organizational DN (denoted by DN_1(s)) to originate a Secret, Confidential or Unclassified (S/C/U) message for a type B(1)a organization. All AUTODIN bound S/C/U message traffic is delivered to the MFI_1 using the Secret universal (Secret Domain FORTEZZA personality). The MFI_1 then forwards the traffic to AUTODIN.

An organizational releaser in the DMS Secret domain must send two Unclassified messages if it has recipients in both AUTODIN and in the DMS Unclassified domain. The releaser must use the Secret universal (Secret Domain FORTEZZA personality) / Secret DN1(s) to send to AUTODIN and a SBU universal (Unclassified Domain FORTEZZA personality) / Unclassified DN1(n) to send to the DMS Unclassified domain recipients.

B.3.6 Transition Architecture SubType B(1)b:

Type B: For an organization that communicates solely on a Classified LAN.

SubType B(1): This transitional architecture type is for use by an organization that sends/receives S/C/U message traffic from/at its Secret domain. About 20% of the total number of DoD organizations transitioning populate this category.

- SubType B(1)b: For an organization that uses centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

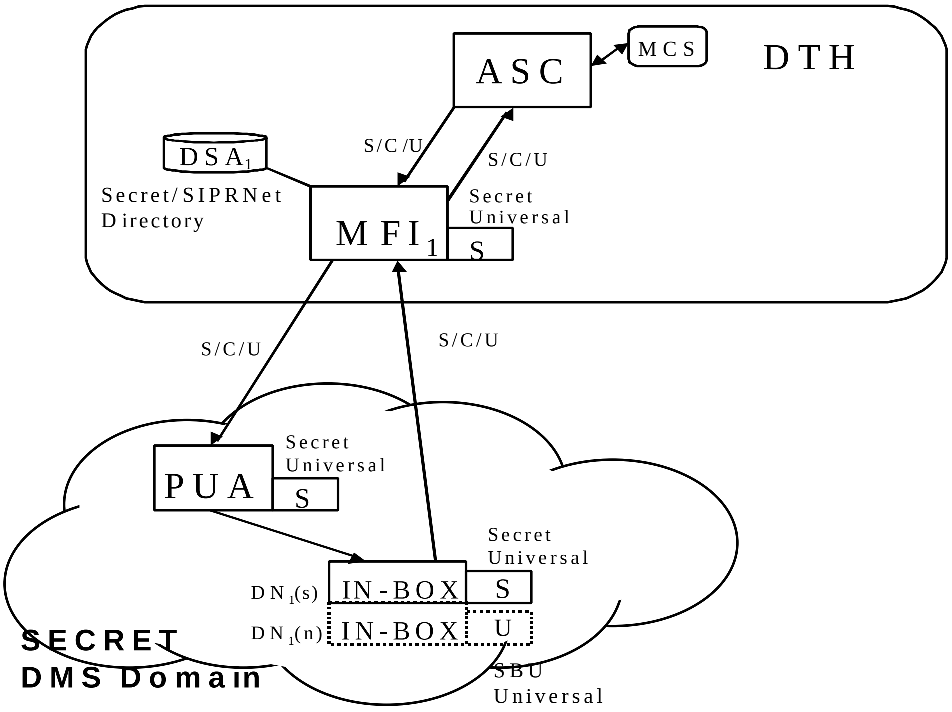


Figure B.3-6 Organizational Transition Architecture SubType B(1)b

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type B(1)b organization receives its S/C/U messages from AUTODIN via MFI$_1$ to its Secret DMS domain. MFI$_1$ uses its Secret universal (Secret Domain FORTEZZA personality) to deliver the S/C/U messages to the organization's Secret centralized distribution point depicted by a PUA. Then, the PUA delivers to its Secret domain recipients using the Secret universal (Secret Domain FORTEZZA personality). The recipients are represented here as an organizational in-box corresponding to DN$_1$(s).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

The organizational releaser in the DMS Secret domain must use the Secret organizational DN (denoted by DN$_1$(s)) to originate a Secret, Confidential or Unclassified (S/C/U) message for a type B(1)b organization. All AUTODIN bound S/C/U message traffic is delivered to the MFI$_1$ using the Secret universal (Secret Domain FORTEZZA personality). The MFI$_1$ then forwards the traffic to AUTODIN.

An organizational releaser in the DMS Secret domain must send two Unclassified messages if it has recipients in both AUTODIN and in the DMS Unclassified domain. The releaser must use the Secret universal (Secret Domain FORTEZZA personality) / Secret DN1(s) to send to AUTODIN and a SBU universal (Unclassified Domain FORTEZZA personality) / Unclassified DN1(n) to send to the DMS Unclassified domain recipients.

B.3.7 Transition Architecture SubType B(1)c:

Type B: For an organization that communicates solely on a Classified LAN.

SubType B(1): This transitional architecture type is for use by an organization that sends/receives S/C/U message traffic from/at its Secret domain. About 20% of the total number of DoD organizations transitioning populate this category.

- SubType B(1)c: For an organization that uses de-centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

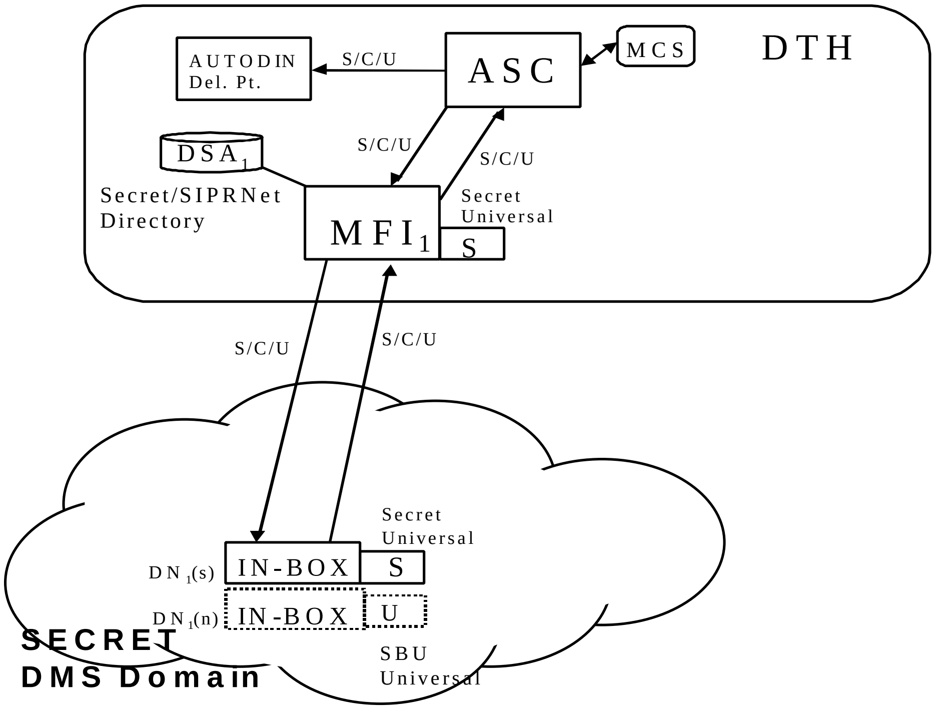


Figure B.3-7 Organizational Transition Architecture SubType B(1)c

Inbound (AUTODIN-to-DMS) to Organization's AUTODIN delivery point

This organization receives a copy of all levels of classified messages S/C/U at its AUTODIN delivery point until it is confident about delivery to its DMS in-box.

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type B(1)c organization receives its S/C/U messages from AUTODIN via MFI_1 to its Secret DMS domain. MFI_1 uses its Secret universal (Secret Domain FORTEZZA personality) to deliver the S/C/U messages to the organization's Secret in-box denoted by DN_1(s).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

The organizational releaser in the DMS Secret domain must use the Secret organizational DN (denoted by DN_1(s)) to originate a Secret, Confidential or Unclassified (S/C/U) message for a type B(1)c organization. All AUTODIN bound S/C/U message traffic is delivered to the MFI_1 using the Secret universal (Secret Domain FORTEZZA personality). The MFI_1 then forwards the traffic to AUTODIN.

An organizational releaser in the DMS Secret domain must send two Unclassified messages if it has recipients in both AUTODIN and in the DMS Unclassified domain. The releaser must use the Secret universal (Secret Domain FORTEZZA personality) / Secret DN1(s) to send to AUTODIN and a SBU universal (Unclassified Domain FORTEZZA personality) / Unclassified DN1(n) to send to the DMS Unclassified domain recipients.

B.3.8 Transition Architecture SubType B(1)d:

Type B: For an organization that communicates solely on a Classified LAN.

SubType B(1): This transitional architecture type is for use by an organization that sends/receives S/C/U message traffic from/at its Secret domain. About 20% of the total number of DoD organizations transitioning populate this category.

- SubType B(1)d: For an organization that uses de-centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

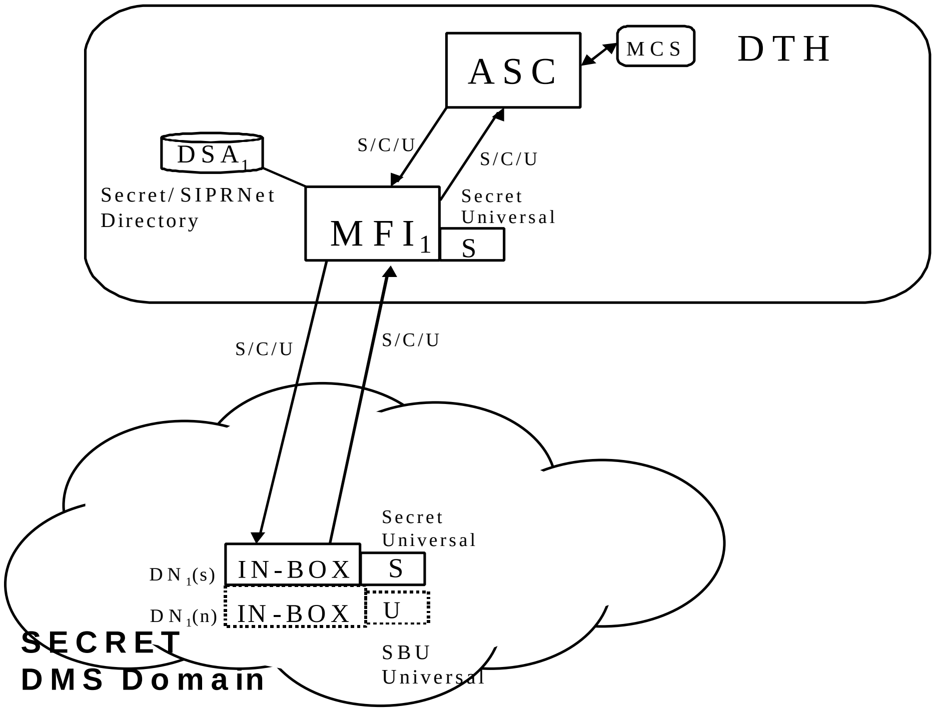


Figure B.3-8 Organizational Transition Architecture SubType B(1)d

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type B(1)d organization receives its S/C/U messages from AUTODIN via MFI$_1$ to its Secret DMS domain. MFI$_1$ uses its Secret universal (Secret Domain FORTEZZA personality) to deliver the S/C/U messages to the organization's Secret in-box denoted by DN$_1$(s).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

The organizational releaser must use the Secret organizational DN (denoted by DN$_1$(s)) to originate a Secret, Confidential or Unclassified (S/C/U) message for a type B(1)d organization. All AUTODIN bound S/C/U message traffic is delivered to the MFI$_1$ using the Secret universal (Secret Domain FORTEZZA personality). The MFI$_1$ then forwards the traffic to AUTODIN.

An organizational releaser in the DMS Secret domain must send two Unclassified messages if it has recipients in both AUTODIN and in the DMS Unclassified domain. The releaser must use the Secret universal (Secret Domain FORTEZZA personality) / Secret DN1(s) to send to AUTODIN and a SBU universal (Unclassified Domain

FORTEZZA personality) / Unclassified DN1(n) to send to the DMS Unclassified domain recipients.

B.3.9 Transition Architecture SubType B(2)a:

Type B: For an organization that communicates solely on a Classified LAN.

SubType B2: This transitional architecture type is for use by an organization that sends/receives S/C message traffic ONLY at its Secret domain. Less than 5% of the total number of DoD organizations transitioning populate this category.

- SubType B(2)a: For an organization that uses centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

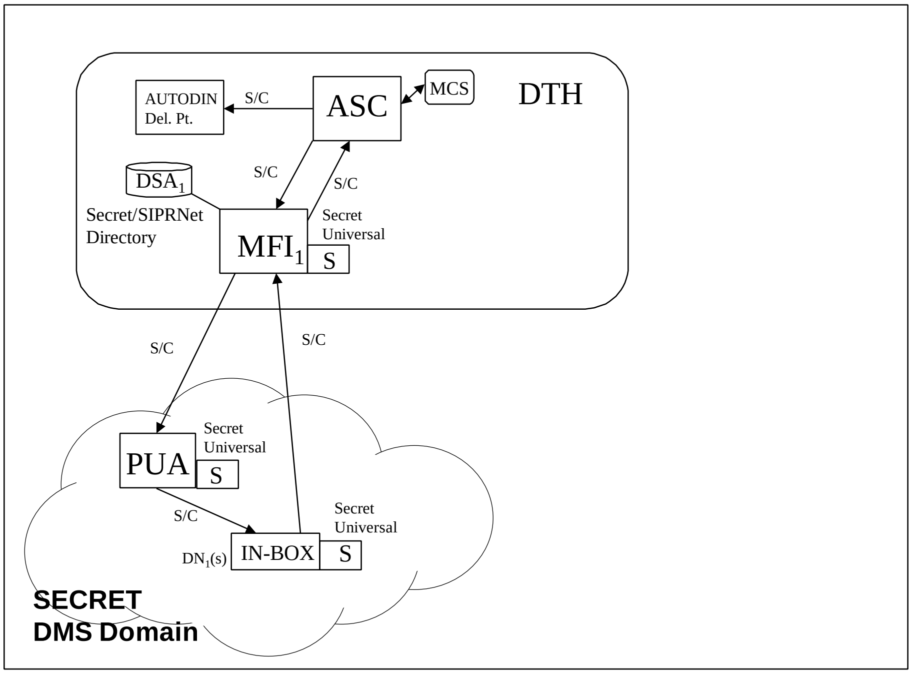


Figure B.3-9 Organizational Transition Architecture SubType B(2)a

Inbound (AUTODIN-to-DMS) to Organization's AUTODIN delivery point

This organization receives a copy of all its Secret and Confidential (S/C) messages at its AUTODIN delivery point until it is confident about delivery to its DMS in-box.

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type B(2)a organization receives its S/C messages from AUTODIN via MFI_1 to its Secret DMS domain. MFI_1 uses its Secret universal (Secret Domain FORTEZZA personality) to deliver the S/C messages to the organization's Secret central distribution point denoted by a PUA. Then, the PUA delivers to its Secret domain recipients using the Secret universal (Secret Domain FORTEZZA personality). The recipients are represented here as an organizational in-box corresponding to DN_1(s).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

The organizational releaser in the DMS Secret domain must use the Secret organizational DN (denoted by DN_1(s)) to originate a Secret or Confidential (S/C) message for a type B(2)a organization. All AUTODIN bound S/C message traffic is delivered to the MFI_1 using the Secret universal (Secret Domain FORTEZZA personality). The MFI_1 then forwards the traffic to AUTODIN.

B.3.10 Transition Architecture SubType B(2)b:

Type B: For an organization that communicates solely on a Classified LAN.

> SubType B2: This transitional architecture type is for use by an organization that sends/receives S/C message traffic ONLY at its Secret domain. Less than 5% of the total number of DoD organizations transitioning populate this category.

- SubType B(2)b: For an organization that uses centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

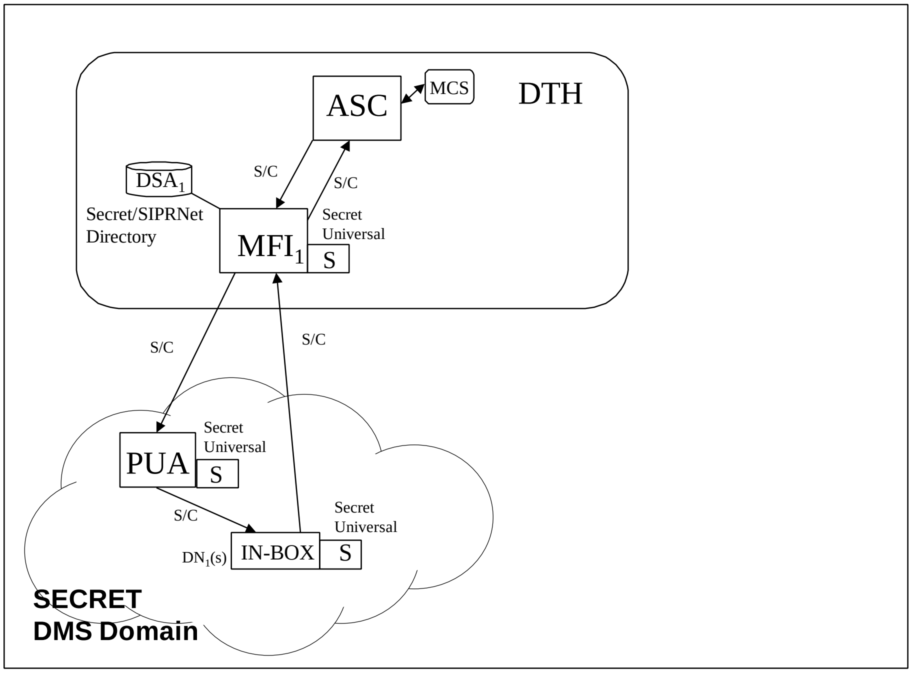


Figure B.3-10 Organizational Transition Architecture SubType B(2)b

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type B(2)b organization receives its S/C messages from AUTODIN via MFI$_1$ to its Secret DMS domain. MFI$_1$ uses its Secret universal (Secret Domain FORTEZZA personality) to deliver the S/C messages to the organization's Secret central distribution point denoted by a PUA. Then, the PUA delivers to its Secret domain recipients using the Secret universal (Secret Domain FORTEZZA personality). The recipients are represented here as an organizational inbox corresponding to DN$_1$ (s).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

The organizational releaser in the DMS Secret domain must use the Secret organizational DN (denoted by DN$_1$(s)) to originate a Secret or Confidential (S/C) message for a type B(2)b organization. All AUTODIN bound S/C message traffic is delivered to the MFI$_1$

using the Secret universal (Secret Domain FORTEZZA personality). The MFI$_1$ then forwards the traffic to AUTODIN.

B.3.11 Transition Architecture SubType B(2)c:

Type B: For an organization that communicates solely on a Classified LAN.

> SubType B2: This transitional architecture type is for use by an organization that sends/receives S/C message traffic ONLY at its Secret domain. Less than 5% of the total number of DoD organizations transitioning populate this category.

- SubType B(2)c: For an organization that uses de-centralized DMS message distribution and dual deliver of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

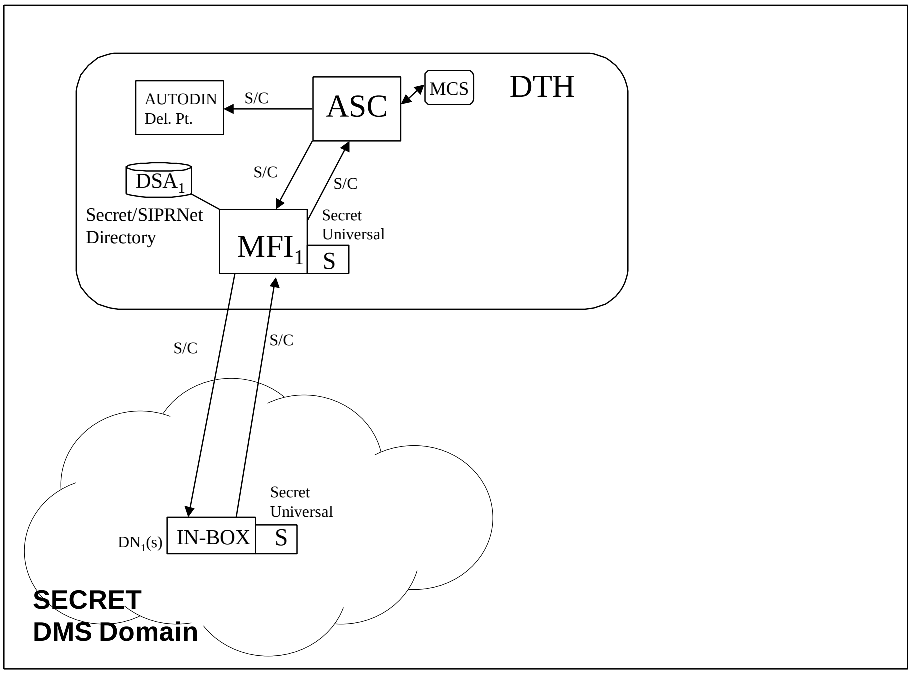


Figure B.3-11 Organizational Transition Architecture SubType B(2)c

Inbound (AUTODIN-to-DMS) to Organization's AUTODIN delivery point

This organization receives a copy of all its Secret and Confidential (S/C) at its AUTODIN delivery point until it is confident about delivery to its DMS in-box.

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type B(2)c organization receives its S/C messages from AUTODIN via MFI_1 to its Secret DMS domain. MFI_1 uses its Secret universal (Secret Domain FORTEZZA personality) to deliver the S/C messages to the organization's Secret in-box denoted by DN_1(s).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

The organizational releaser in the DMS Secret domain must use the Secret organizational DN (denoted by DN_1(s)) to originate a Secret or Confidential (S/C) message for a type B(2)c organization. All AUTODIN bound S/C message traffic is delivered to the MFI_1 using the Secret universal (Secret Domain FORTEZZA personality). The MFI_1 then forwards the traffic to AUTODIN.

B.3.12 Transition Architecture SubType B(2)d:

Type B: For an organization that communicates solely on a Classified LAN.

SubType B2: This transitional architecture type is for use by an organization that sends/receives S/C message traffic ONLY at its Secret domain. Less than 5% of the total number of DoD organizations transitioning populate this category.

- SubType B(2)d: For an organization that uses de-centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

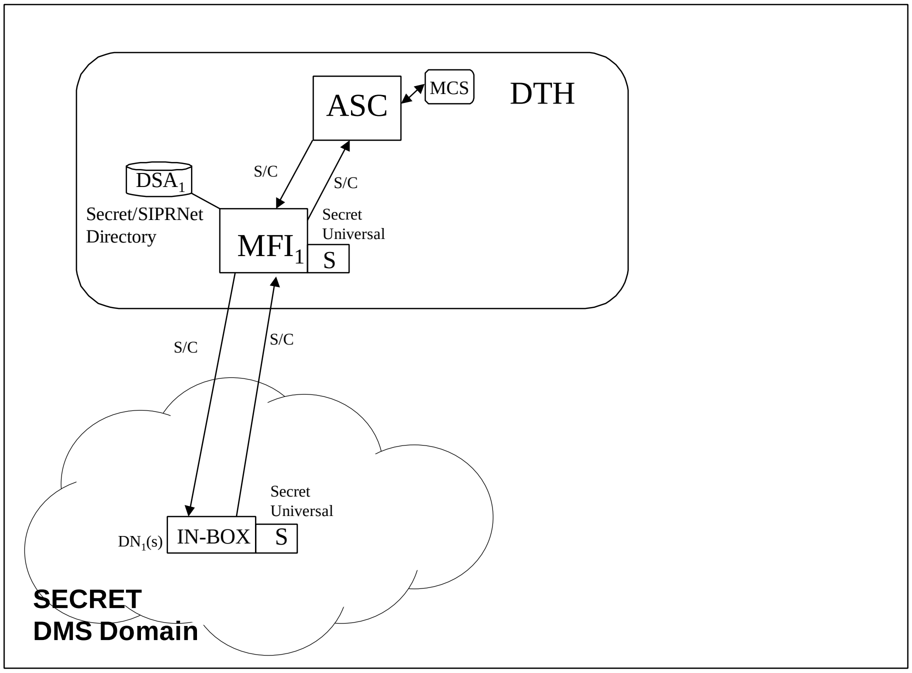


Figure B.3-12 Organizational Transition Architecture SubType B(2)d

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type B(2)d organization receives its S/C messages from AUTODIN via MFI$_1$ to its Secret DMS domain. MFI$_1$ uses its Secret universal (Secret Domain FORTEZZA personality) to deliver the S/C messages to the organization's Secret in-box denoted by DN$_1$(s).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

The organizational releaser must use the Secret organizational DN (denoted by DN$_1$(s)) to originate a Secret or Confidential (S/C) message for a type B(2)d organization. All AUTODIN bound S/C message traffic is delivered to the MFI$_1$ using the Secret universal (Secret Domain FORTEZZA personality). The MFI$_1$ then forwards the traffic to AUTODIN.

B.3.13 Transition Architecture SubType C(1):

Type C: For an organization that communicates solely on an Unclassified LAN. It sends/receives unclassified message traffic ONLY. This type comprises about 5% of the total number of DoD organizations transitioning to DMS.

- SubType C(1): For an organization that uses centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

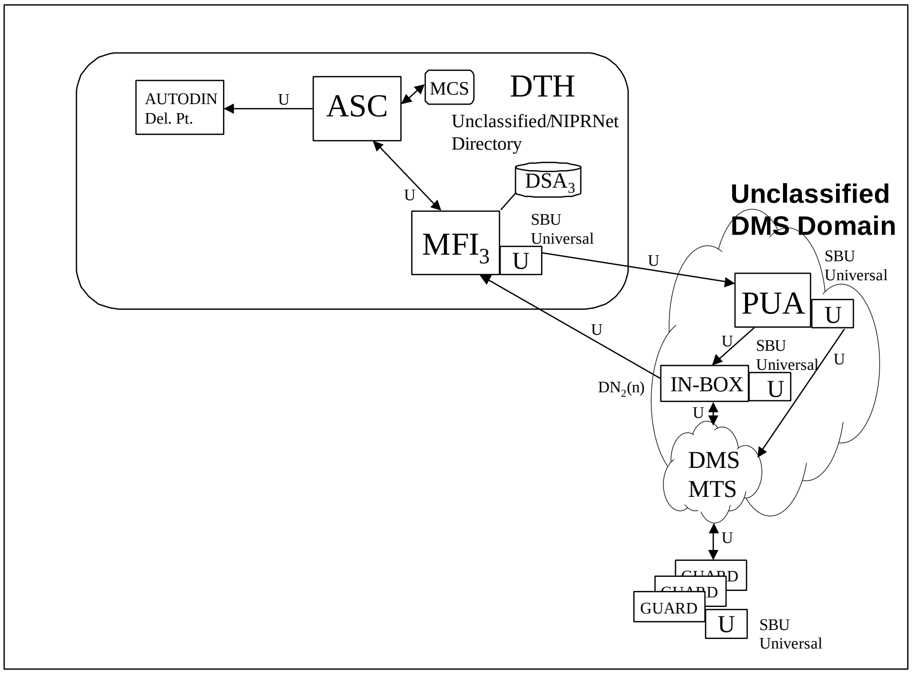


Figure B.3-13 Organizational Transition Architecture SubType C(1)

Inbound (AUTODIN-to-DMS) to Organization's AUTODIN delivery point

This organization receives a copy of all its Unclassified (U) messages at its AUTODIN delivery point until it is confident about delivery to its DMS in-box.

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type C(1) organization receives its U messages from AUTODIN via MFI_3 to its Unclassified DMS domain. MFI_3 uses its SBU universal (Unclassified Domain FORTEZZA personality) to deliver the U messages to the organization's Unclassified central distribution point denoted by a PUA. Then, the PUA delivers to its Unclassified domain recipients using the SBU universal (Unclassified Domain FORTEZZA personality). The recipients are represented here as an organizational in-box corresponding to $DN_2(n)$.

Outbound (DMS-to-AUTODIN) to DMS Message Flow

A DMS organizational Type C(1) releaser may address an Unclassified (U) message to both AUTODIN and DMS recipients in the same message because both require the same SBU universal (Unclassified Domain FORTEZZA personality). The message routes through the DMS MTS to the DMS recipients and through the local MFI, MFI_3, to the AUTODIN recipients.

The organizational releaser in the DMS Unclassified domain must use the SBU universal (Unclassified Domain FORTEZZA personality) and Unclassified organizational DN (denoted by $DN_2(n)$) to originate an Unclassified message for a type C(1) organization. All AUTODIN bound U message traffic is delivered to the MFI_3 using the SBU universal (Unclassified Domain FORTEZZA personality). The MFI_3 then forwards the traffic to AUTODIN.

B.3.14 Transition Architecture SubType C(2):

Type C: For an organization that communicates solely on an Unclassified LAN. It sends/receives unclassified message traffic ONLY. This type comprises about 5% of the total number of DoD organizations transitioning to DMS.

- SubType C(2): For an organization that uses centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

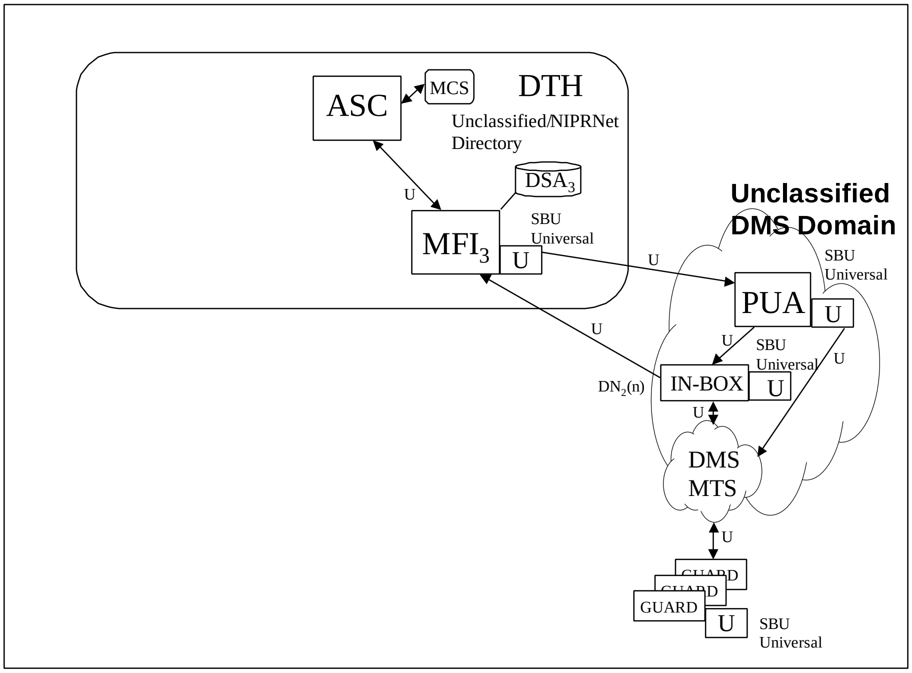


Figure B.3-14 Organizational Transition Architecture SubType C(2)

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type C(2) organization receives its U messages from AUTODIN via MFI_1 to its Unclassified DMS domain. MFI_3 uses its SBU universal (Unclassified Domain FORTEZZA personality) to deliver the U messages to the organization’s Unclassified central distribution point denoted by a PUA. Then, the PUA delivers to its Unclassified domain recipients using the SBU universal (Unclassified Domain FORTEZZA personality). The recipients are represented here as an organizational in-box corresponding to $DN_2(n)$.

Outbound (DMS-to-AUTODIN) to DMS Message Flow

A DMS organizational Type C(2) releaser may address an Unclassified (U) message to both AUTODIN and DMS recipients in the same message because both require the same SBU universal (Unclassified Domain FORTEZZA personality). The message routes through the DMS MTS to the DMS recipients and through the local MFI, MFI_3, to the AUTODIN recipients.

The organizational releaser in the DMS Unclassified domain must use the SBU universal (Unclassified Domain FORTEZZA personality) and Unclassified organizational DN (denoted by $DN_2(n)$) to originate an Unclassified message for a type C(2) organization. All AUTODIN bound U message traffic is delivered to the MFI_3 using the SBU universal (Unclassified Domain FORTEZZA personality). The MFI_3 then forwards the traffic to AUTODIN.

B.3.15 Transition Architecture SubType C(3):

Type C: For an organization that communicates solely on an Unclassified LAN. It sends/receives unclassified message traffic ONLY. This type comprises about 5% of the total number of DoD organizations transitioning to DMS.

- SubType C(3): For an organization that uses de-centralized DMS message distribution and dual delivery of messages during transition to both an AUTODIN delivery point and a DMS mailbox.

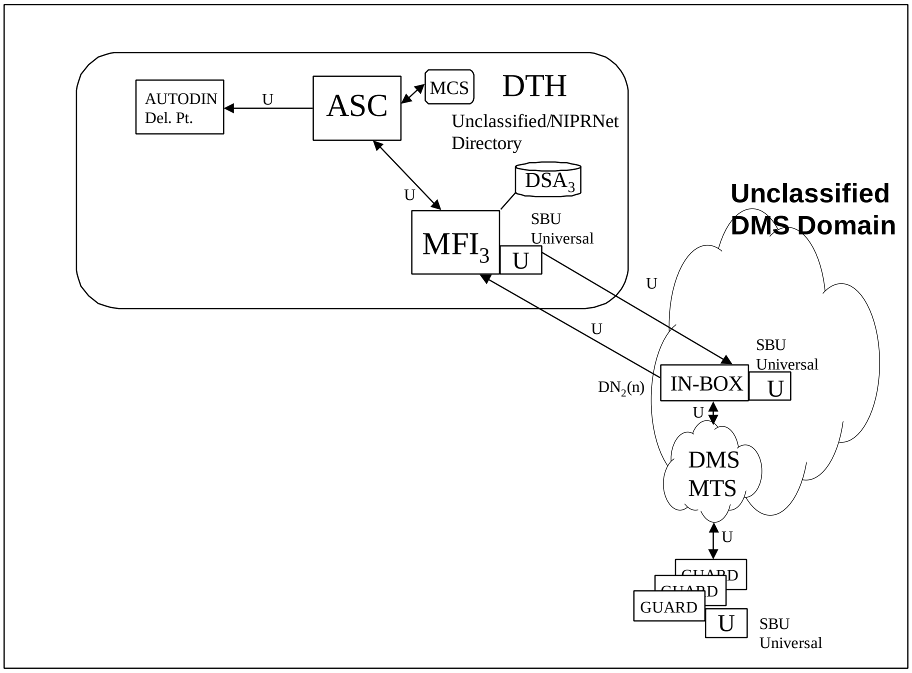


Figure B.3-15 Organizational Transition Architecture SubType C(3)

Inbound (AUTODIN-to-DMS) to Organization's AUTODIN delivery point

This organization receives a copy of all its Unclassified (U) messages at its AUTODIN delivery point until it is confident about delivery to its DMS in-box.

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type C(3) organization receives its U messages from AUTODIN via MFI_3 to its Unclassified DMS domain. MFI_3 uses its SBU universal (Unclassified Domain FORTEZZA personality) to deliver the U messages to the organization's Unclassified in-box denoted by DN_2(n).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

A DMS organizational Type C(3) releaser may address an Unclassified (U) message to both AUTODIN and DMS recipients in the same message because both require the same SBU universal (Unclassified Domain FORTEZZA personality). The message routes through the DMS MTS to the DMS recipients and through the local MFI, MFI $_3$, to the AUTODIN recipients.

The organizational releaser must use the SBU universal (Unclassified Domain FORTEZZA personality) and Unclassified organizational DN (denoted by DN_2(n)) to originate an Unclassified message for a type C(3) organization. All AUTODIN bound U message traffic is delivered to the MFI_3 using the SBU universal (Unclassified Domain FORTEZZA personality). The MFI_3 then forwards the traffic to AUTODIN.

B.3.16 Transition Architecture SubType C(4):

Type C: For an organization that communicates solely on an Unclassified LAN. It sends/receives unclassified message traffic ONLY. This type comprises about 5% of the total number of DoD organizations transitioning to DMS.

- SubType C(4): For an organization that uses de-centralized DMS message distribution and single delivery of messages to a DMS mailbox during transition.

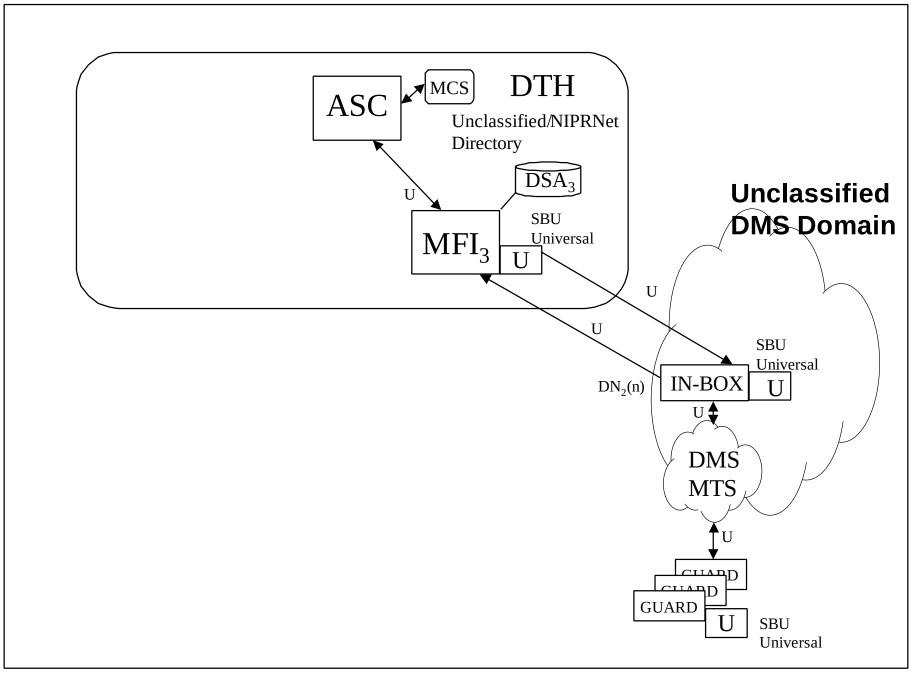


Figure B.3-16 Organizational Transition Architecture SubType C(4)

Inbound (AUTODIN-to-DMS) to DMS Message Flow

A Type C(4) organization receives its U messages from AUTODIN via MFI$_3$ to its Unclassified DMS domain. MFI$_3$ uses its SBU universal (Unclassified Domain FORTEZZA personality) to deliver the U messages to the organization's Unclassified in-box denoted by DN$_2$(n).

Outbound (DMS-to-AUTODIN) to DMS Message Flow

A DMS organizational Type C(4) releaser may address an Unclassified (U) message to both AUTODIN and DMS recipients in the same message because both require the same SBU universal (Unclassified Domain FORTEZZA personality). The message routes through the DMS MTS to the DMS recipients and through the local MFI, MFI $_3$, to the AUTODIN recipients.

The organizational releaser must use the SBU universal (Unclassified Domain FORTEZZA personality) and Unclassified organizational DN (denoted by DN$_2$(n)) to originate an Unclassified message for a type C(4) organization. All AUTODIN bound U message traffic is delivered to the MFI_3 using the SBU universal (Unclassified Domain FORTEZZA personality). The MFI_3 then forwards the traffic to AUTODIN.

B.4 Example AUTODIN Transition Strategy Selection

B.4.1 Transition Planning Overview

This section provides an overview of the transition planning process. The information provided in this section is designed to amplify the transition planning steps discussed in Section 4 and the transition architecture planning guidance outlined in Section B.2.1. The following messaging scenario and operational examples are provided to improve the reader's understanding of the transition planning process and provide a frame of reference for selecting transition implementation options.

Transition Scenario: The 918th Signal Battalion is planning to transition from AUTODIN to DMS. The unit is comprised of a commander, a primary staff, and three subordinate signal companies. The parent unit and its subordinate units are all located at Fort Smith, Maryland. AUTODIN messages are addressed and delivered to elements of the 918th Signal Battalion and three subordinate Signal Companies using four PLAs assigned to one RI.

Reception of messages from AUTODIN. The 918th Signal Battalion and its subordinate units receive their Unclassified organizational messages via an unclassified LAN. Secret and Confidential messages are received and hand delivered via courier in combination with over-the-counter messaging services provided by the base communications center.

Release of messages to AUTODIN. All outgoing AUTODIN messages (Unclassified, Confidential, and Secret) are released by designated release authorities within the 918th Signal Battalion. Each released message (hard and magnetic copy) is transported to the Fort Smith communications center via courier for over-the-counter entry into AUTODIN.

The 918th Signal Battalion is a subordinate unit to the 492nd Signal Brigade. The 492nd Brigade Headquarters has begun its DMS transitioning. The 918th and its sister battalions are all scheduled to transition to DMS.

B.4.2 Review Current Operations

The initial step in transition planning involves identifying current operational concepts, procedures and policies. Factors to be considered include the following:

1. Current organizational message drafter and releaser policies and procedures.

2. Existing procedures and policies that dictate how messages are received and distributed within the organization.

3. Existing procedures and policies for storing and accounting for received organizational messaging traffic.

Notional Assessment of 918th Signal Battalion Messaging

The following notional assessment for the 918th Signal Battalion outlines the information that should be considered during this transition planning step.

The Commander, Administrative Officer, Executive Officer, and Operations Officer are the only organizational message release authorities for the entire battalion. Their signatures are on file at the base communications center.

AUTODIN messages are addressed and delivered to elements of the 918th Signal Battalion and three subordinate Signal Companies using RI **"RUATHNF"** and the following PLA assignments:

- COMMANDER 918TH SIGNAL BN FORT SMITH MD
- COMMANDER 533RD SIGNAL CO FORT SMITH MD
- COMMANDER 352ND SIGNAL CO FORT SMITH MD
- COMMANDER 253RD SIGNAL CO FORT SMITH MD

Unclassified organizational messages are received and distributed to appropriate destinations within the battalion via an unclassified LAN. The battalion's Administrative Officer oversees pick-up and distribution of classified messages and ensures that message couriers are properly indoctrinated and identified to the base communications center. A battalion courier makes periodic (and on-call) visits to the base communications center to pick-up incoming, and deliver outgoing, organizational messages. The classified messages are loggedinto a ledger by date time group, message originator, message recipient, classification, and subject fields. If a recipient is not readily identifiable, the Administrative Officer makes the distribution decision. Classified messages, other than those addressed directly to the Commander, are stored by the message recipient. Messages addressed to the Commander are stored by the battalion Security Officer.

All outgoing Unclassified organizational messages are delivered to the battalion Administrative Officer via e-mail for release and further transfer to the base communications center. Classified messages are delivered to the Administrative Officer in hardcopy form for release and further transfer to the base communications center.

B.4.3 Identifying Messaging Objectives

The second step of the transition planning process is to identify the messaging objectives of the transitioning unit. This step includes determining which elements of the organization are scheduled to transition to DMS and the organization's strategy for accomplishing the transition. Using the above scenario, the following notional messaging objectives and transition strategy are presented to illustrate key transition initiatives that could be associated with this planning step.

Notional Messaging Objectives for 918th Signal Battalion

Based on the above scenario it could be assumed that all elements of the 918th Signal Battalion will transition to DMS using the Type A Transitional Messaging Architecture described in paragraph B.2.1 and the "hard-cutover" transition approach outlined in paragraph B.1.2.2. Since the unit is currently supported by four PLAs, assumptions are that DMS equivalents to these legacy PLAs will be established and that one or more DMS organizational user accounts will be established to support DMS messaging operations.

B.4.4 Identify DMS Concepts

An analysis of the DMS product capabilities and the organization's future operational concepts is the third step in the DMS transition planning process. This step is closely linked to the analysis of current operating procedures. The major objective of this step in the transition planning process is to link the organization's current policies, procedures, and operational concepts with capabilities that are supported by DMS products. Key items to be considered are:

- Number of anticipated DMS organizational users and the types and quantities of DMS products required.
- Implementation approach for distributing and handling DMS organizational messages
- Naming and addressing conventions needed to support organizational messaging requirements between AUTODIN and DMS communities.
- Policies and procedures for handling classified and unclassified messaging (including changes in distribution determination and message release associated with the introduction of DMS technology).
- Access to NIPRNET and SIPRNET connectivity.

Notional Assessment of 918th Signal Battalion Future Messaging Concepts

The following assessment outlines a possible approach for meeting requirements identified in the 918th Signal Battalion notional scenario:

An analysis of 918th Signal Battalion's notional messaging scenario indicates that an organizational DN should be established for each of the unit's legacy PLAs. Since the unit adopted the "hard-cutover, the existing legacy PLAs should be associated with the unit's new DMS DNs. Based on the unit's internal messaging policies, the resulting DN to PLA mapping for the unit could include office codes for the battalion commander and staff elements and a one-to-one DN-PLA mapping for each of the subordinate unit commanders. Figure B.4-1 below outlines this notional addressing scheme for the 918th Signal Battalion (note this is one of several optional DMS PLA/Office Code solutions that DMS supports for Release 2.1).

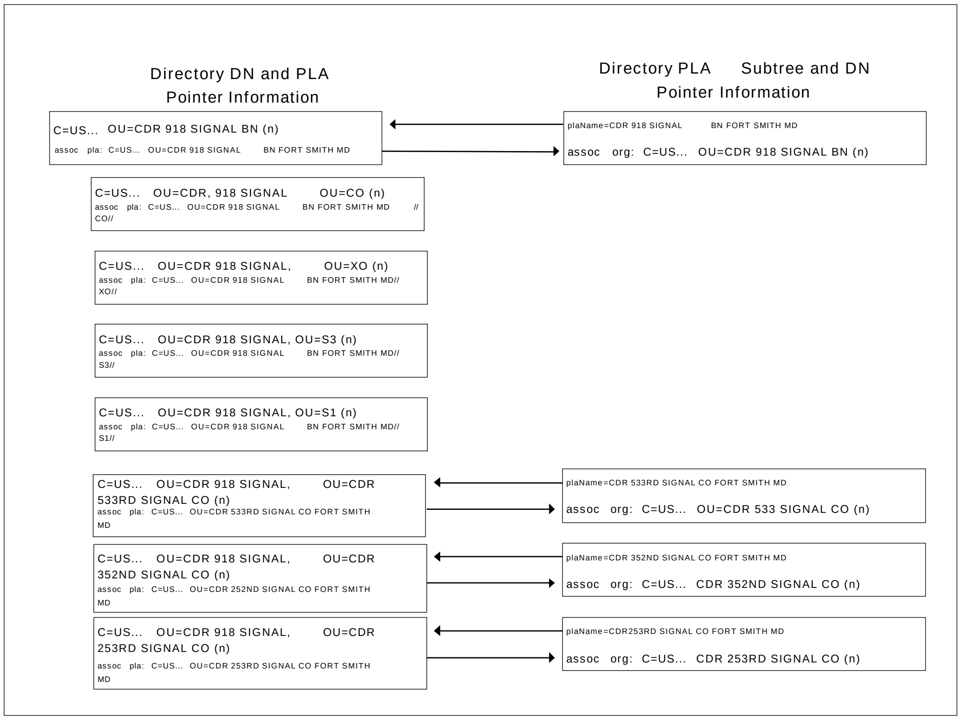

Directory DN and PLA
Pointer Information
Directory PLA Subtree and DN
Pointer Information
C=US... OU=CDR 918 SIGNAL BN (n)
assoc pla: C=US... OU=CDR 918 SIGNAL BN FORT SMITH MD
plaName=CDR 918 SIGNAL BN FORT SMITH MD
assoc org: C=US... OU=CDR 918 SIGNAL BN (n)
C=US... OU=CDR, 918 SIGNAL OU=CO (n)
assoc pla: C=US... OU=CDR 918 SIGNAL BN FORT SMITH MD // CO//
C=US... OU=CDR 918 SIGNAL, OU=XO (n)
assoc pla: C=US... OU=CDR 918 SIGNAL BN FORT SMITH MD// XO//
C=US... OU=CDR 918 SIGNAL, OU=S3 (n)
assoc pla: C=US... OU=CDR 918 SIGNAL BN FORT SMITH MD// S3//
C=US... OU=CDR 918 SIGNAL, OU=S1 (n)
assoc pla: C=US... OU=CDR 918 SIGNAL BN FORT SMITH MD// S1//
C=US... OU=CDR 918 SIGNAL, OU=CDR 533RD SIGNAL CO (n)
assoc pla: C=US... OU=CDR 533RD SIGNAL CO FORT SMITH MD
plaName=CDR 533RD SIGNAL CO FORT SMITH MD
assoc org: C=US... OU=CDR 533 SIGNAL CO (n)
C=US... OU=CDR 918 SIGNAL, OU=CDR 352ND SIGNAL CO (n)
assoc pla: C=US... OU=CDR 252ND SIGNAL CO FORT SMITH MD
plaName=CDR 352ND SIGNAL CO FORT SMITH MD
assoc org: C=US... CDR 352ND SIGNAL CO (n)
C=US... OU=CDR 918 SIGNAL, OU=CDR 253RD SIGNAL CO (n)
assoc pla: C=US... OU=CDR 253RD SIGNAL CO FORT SMITH MD
plaName=CDR253RD SIGNAL CO FORT SMITH MD
assoc org: C=US... CDR 253RD SIGNAL CO (n)

Figure B.4-1 Notional DMS Addressing Scheme

Based on previously identified operational policies and procedures, the recommended DMS operational policies and procedures should include the following:

- Unclassified messages should be delivered to the intended recipient. Under this policy, the organization's recipients should continue to receive and store incoming unclassified organization traffic. Messages that are not addressed to specific organizational recipients (i.e. not addressed to the office codes or subordinate unit PLAs should be routed to the battalion Administrative Officer for distribution. *(Note: Using a PUA to handle this function could support this concept.)*

- The classified message handling policy would be dependent upon the availability of SIPRNET connectivity for the unit's organizational messaging users. If the majority of the users have access to secure LANs that are connected to the SIPRNET, the policy should be direct delivery to the message recipient. Messages that are not addressed to specific organizational recipients should be delivered to the security officer. In the event that SIPRNET connectivity is not available to all recipients, the policy could be to deliver all classified message traffic to a single point within the unit, for example the battalion security officer (since he/she is likely to have the required security clearances). If the option to have the classified traffic delivered to the designated officer is implemented, policies similar to those described in the notional scenario should be adopted.

B.4.5 Selecting DMS Transitional Architecture

The final transition planning step involves selecting the appropriate DMS transition architecture. There are three general transitional architecture alternatives to choose from:

- Split the organization onto NIPRNET and SIPRNET operating environments to support both "secret and below" and "unclassified" messaging. (Type A)

- Implement DMS totally in a SIPRNET environment to support "secret and below" messaging requirements. (Type B)

- Transition the organization totally onto a NIPRNET operating environment to support "unclassified only" messaging requirements. (Type C)

Based on limited SIPRNET connectivity and the high ratio of unclassified to classified message traffic, the Type A Transitional Messaging Architecture as described in paragraph will be used by most organizations.

Notional 918th Signal Battalion Architecture

Based on the notional review of the above transition planning steps, the recommended transition architecture for the 918th Signal Battalion is Type A. (See Section B.2.1.) As a result of the identified transition strategy, operational concepts, and internal policies of the unit, a possible transition solution is to:

- Since SIPRNET connectivity and secure operating environments will be available, the three companies will install S/C DMS client platforms within their respective operating environments. This corresponds to Subtype A(4) (See Section B.3.4.) Alternatively, a single organizational messaging account on the SIPRNET could be established for the security officer to receive all of the battalion's incoming classified message traffic.

- Establish individual organizational accounts on the NIPRNET for the battalion commander, the three company commanders, and each of the battalion's principle staff officers.

- Establish a default organizational account that could be assigned to either the admin officer or a PUA to handle non-recipient specific incoming messages.

- Establish alternate delivery accounts/agreements with the brigade headquarters or other organizations at Fort Smith to ensure alternate delivery of high precedence messages (unclassified and classified) during system outages and/or periods of non-availability.

APPENDIX C

UPGRADING DMS

Note

This appendix reproduces exactly Defense Information Systems Agency, *Defense Message System (DMS) Interim Procedure 4-V01: System Upgrade Procedures*, DSA DOC 01-046, December 12, 1998. This material is reproduced for reference purposes.

Defense Message System (DMS)

Interim Procedure 4-V01

System Upgrade Procedures

Prepared for

DISA D3121

DMS Global Systems Manager

11440 Isaac Newton Sq

Reston VA 20190

by

Data Systems Analysts, Inc.

10400 Eaton Place

Suite 500

Fairfax, VA 22030

Table of Contents

1 Purpose

This document provides the operational transition procedures for upgrading the global DMS system (both infrastructure and ACC/LCC enclaves) with new product releases. These procedures replace the Operational Procedures for DMS Releases, Version 1.0 (DMS Document Control Number 0331-01, 29 June 98).

2 Scope

The policies and procedures described apply to DMS Release 2.0 and all future DMS releases. They are applicable to the RSMs, the S/a Program Management Offices (PMO)[8] and their ASM/LSMs. This document provides the operational procedures necessary to execute the Implementation Strategy and Plan for DMS Releases (ISP) prepared by the DMS integration contractor.

3 Overview

3.1 DMS Product Release

[8] The S/a DMS Program Management Office is responsible for these procedures as long as the office is active. If the PMO is deactivated the S/a DMS sustaining command takes responsibility.

DMS implements and deploys system capabilities through a series of coordinated software product releases. Each release of DMS provides new capabilities and/or enhancements to established products as part of an integrated system. Release levels also correspond to achievement of significant program capabilities.

3.1.1

A major software release can be expected approximately every six months. This maintains momentum and permits infusion of new technology on a routine basis. The DMS integration contractor uses the DMS Configuration Control Board (CCB) approved capabilities matrix to work with product providers to develop an integrated product plan for each release.

3.1.2

The DMS Product Plan document explains the DMS product development and release process in more detail. The DMS Product Plan is available for download from the on-line library from the DMS Controlled Access Web Page (http://www.disa.mil/D2/dms/invited/index2.html).

3.2 DMS Implementation Strategy and Plan for DMS Release (ISP)

The ISP is prepared by the DMS integration contractor at the direction of the DISA DMS Program Manager (PM). It defines the strategy, procedures and schedule for the implementation of a new DMS product release. The ISP will be published and released concurrent with JITC integration testing and prior to Beta Site testing [9]. The ISP is available on the DISA DMS Controlled Access WEB page in the On-line Library. All personnel involved in the implementation of DMS Product Releases should become familiar with the ISP. The ISP provides detailed information on all aspects of the release and its implementation that is of concern to all staff levels. The information and procedures in the following paragraphs serve as guidelines for executing the information in the ISP.

3.3 Operational Impact

In the operational environment there are too many sites to complete the transition to a new product release instantly. However, DMS product releases are to the extent possible, developed to be backward compatible with the previous release, facilitating interoperability and coexistence of two releases for a designated period of time. The Transition Strategy section in the ISP addresses the capability of the release for backward compatibility and provides a transition plan that minimizes impacts to the operational environment. The ISP also includes a chapter that identifies the risks associated with the upgrade and the mitigation strategy to alleviate these risks. The GSM will assess the operational impact of the release and, if necessary, provide supplemental procedures to compliment the transition strategy in the ISP. S/a PMOs and ASM/LSMs should also

[9] Beta site testing is testing of a new DMS Product Release at selected operational sites. The purpose of this testing is to assess the release in the operational environment before releasing it for global installation.

determine the operational impact of the product release on their DMS ACC/LCC operations and plan accordingly.

4 Transition Procedures

The GSM, in conjunction with the DISA DMS Program Manager,[10] will authorize release of a new DMS product when the product has satisfactorily completed testing and meets established criteria. The ISP identifies the strategy to transition the DMS network (infrastructure and ACC/LCC sites) to the new product release version.

4.1 Transition Schedule

The ISP identifies the order of upgrade. The order of upgrade identifies the sequence in which infrastructure (ROSC, Regional Node, DMS Transition Hub), Beta test, and ACC/LCC sites will be upgraded. In line with the order of upgrade the ISP provides the schedule that sites will upgrade. The GSM will assess the operational impact of the schedule. If necessary the GSM will provide additional scheduling instructions to the ROSCs and the S/a PMOs. S/a PMOs should review the ISP schedule for local planning purposes. If there are any conflicts the S/a PMO will notify the GSM to resolve the conflict. The "official" schedule is provided by the GSM.

[10] The GSM and DISA DMS Program Manager will jointly authorize a new release as long as the DMS Program Manager position is active.

4.2 GSM Authorization to Install

The GSM will send out a notification authorizing sites to install the new product release. ASM/LSMs should not install the new product release until the authorization has been received from the GSM. The GSM notification will normally be sent directly to the RSMs, S/a PMOs and Beta site LSMs. The S/a PMOs will notify their ASM/LSMs accordingly.

4.3 Software Distribution

The new product release will be distributed to sites in a phased approach according to the order and schedule for the upgrade. The software will be shipped to commissioned sites by the DMS integration contractor complete with installation instructions and documentation. The list of documentation for the new release is identified in the ISP. Software will be distributed to the various E&I activities (contractor and S/a E&I) for staging and configuring and to sites in the process of installation at the time of transition. The ISP contains a table with the list of sites to receive the software and their address. This list should be reviewed closely and any discrepancies identified to the respective S/a PMO. The S/a PMO will contact the DMS integration contractor Trouble Desk to resolve the discrepancy.

4.3.1

Software will normally be received by the sites in advance of the upgrade schedule however, it should not be installed until the GSM authorization described in paragraph 9.5.4.2 is received.

4.3.2

Sites that do not receive their software should contact their respective S/a PMO. The S/a PMO will notify the DMS integration contractor trouble desk to resolve the problem.

4.4 Upgrade Status Ticket

Each RSM, Beta and site ASM/LSM will open a DMS Upgrade Status Ticket when they begin the upgrade process. The DMS Upgrade Status Ticket is a trouble ticket prepared to track and report the status of the upgrade process to the servicing ROSC. The Beta and site ASM/LSMs will submit the Upgrade Status Ticket 72 hours prior to beginning the upgrade. The Upgrade Status Ticket will identify the start of the upgrade process and the proposed schedule for executing each step in the process.

4.4.1

If the upgrade testing requirements involve backbone testing with the ROSC the projected backbone testing schedule will be included in the status ticket. If the backbone testing schedule is in conflict with other ROSC activities the ROSC can work with the site to reschedule backbone testing.

4.4.2

The ASM/LSM will update the trouble ticket periodically as the upgrade progresses. The updates will identify the start and completion of each step in the process.

4.4.3

When the upgrade process requires taking site components connected to the backbone offline, the ASM/LSM will notify the RSM with the time the component is removed from service and then with the time the component is returned to service. This procedure ensures that the RSM is aware of the status of site components connected to the backbone.

4.4.4

The RSM will close the Upgrade Status Ticket when the site notifies them that verification test procedures described in chapter 4 were executed successfully.

4.4.5

The DMS Upgrade Status Ticket will not be used for problems encountered during the upgrade. When a problem is encountered a separate trouble ticket will be opened for each problem and processed according to established procedures; the trouble ticket must clearly indicate the product release designation (e.g., 2.0). A separate trouble ticket is required to effectively track each problem as it is escalated from the site to the RSM and to the DMS integration contractor.

4.5 Site Specific Upgrade Procedures

4.5.1 ROSC, Regional Node and DTH Upgrade Procedures

The RSM will monitor DMS Upgrades at Regional Nodes and DMS Transition Hubs. The RSM will coordinate the upgrade schedule and implementation with the personnel performing the upgrade (i.e. System Administrator, E&I or other). The RSM will open a DMS Upgrade Status Ticket when a Regional Node or DTH begins.

4.5.1.1

The DMS integration contractor will provide the RSMs technical support to assist in the transition at the RSMs, Regional Nodes and the DTHs to include the following:

- On-call installation support
- On-call troubleshooting
- Testing assistance to ensure proper operation of infrastructure components

The ROSC should contact the DMS integration contractor trouble support desk for this support.

4.5.1.2

The ROSC will ensure verification test procedures described in chapter 4 are performed. When the upgrade process is completed, including successful verification testing, the ROSC will close the Upgrade Status Ticket.

4.5.2 Beta Test Site Upgrade Procedures

The Beta sites will receive the DMS release approximately two weeks after the release has been delivered to JITC for integration testing. Beta sites are required to execute a series of test procedures against the release to verify correct operation. They are also required to provide a weekly status report on their test progress and issues. The test and weekly status report procedures can be found in the Transition Strategy chapter of the ISP under Beta Sites.

4.5.2.1

The Beta site may upgrade to the new release when they have received authorization from the GSM. The Beta site will initiate the upgrade process by preparing a DMS Upgrade Status Ticket. The Beta site will upgrade components according to the order of upgrade recommended in the ISP.

4.5.2.2

When Beta test sites require technical support, they will prepare a trouble ticket that clearly states the problem is with the Beta software. A separate trouble ticket is required for each individual problem identified. The trouble ticket will then be escalated to their servicing ROSC. The ROSC will briefly review the trouble ticket and if they are not able to resolve it rapidly, they will escalate the trouble ticket to the DMS integration contractor technical support desk for resolution.

4.5.2.3

The Beta site will conduct the verification test procedures described in chapter 4. When the entire site system upgrade is complete the Beta site will close the DMS Upgrade Status Ticket and forward it to the ROSC notifying them of completion of the site upgrade.

4.5.3 ACC/LCC Upgrade Procedures

ACC/LCCs will implement DMS System upgrades when authorization is received from the GSM through the S/a PMO.

4.5.3.1

The ACC/LCC will initiate the upgrade process by preparing a DMS Upgrade Status Ticket. The site will upgrade components according to the order of upgrade recommended in the ISP.

4.5.3.2

The ACC/LCC sites will utilize the standard process for receiving technical support through escalating Trouble Tickets to their servicing ROSC. If the ROSC is not able to resolve the issue, they will escalate to the DMS integration contractor trouble desk for resolution. Any phone calls directly from an ACC/LCC to the DMS integration contractor trouble desk will be directed back to the appropriate ROSC for their action. The DMS integration contractor and the ROSCs will work closely together to identify any systemic issues/trends and communicate these to sites.

4.5.3.3

The ACC/LCC will perform the verification test procedures described in chapter 4. When the entire site upgrade is complete and tested the site will close the DMS Upgrade Ticket and forward it to the ROSC notifying them of completion of the site upgrade.

4.6 DMS System Upgrade Reporting

The ROSCs will report the status of the DMS Upgrade progress in their AOR through the ROSC DMS Daily Status Report. This includes the status of Regional Nodes, DTHs, Beta Sites and ACC/LCCs.

4.7 DMS Upgrade Completion

The DMS System Upgrade will be completed when all the operational sites upgrades have been declared complete through the upgrade status ticket and reporting process described above. Closure of the Upgrade Status Ticket according to these procedures serves as certification of the site upgrade. Sites will not be required to be recommissioned as the result of an upgrade to a new DMS product release.

5 Release Installation Verification Testing

The ISP provides a detailed description of the testing process for each DMS product release. Starting with release 2.0 the process is divided into three phases:

1. DMS Product Testing
2. DMS Integration Testing
3. Verification Testing

While DMS Product and Integration testing are critical to the deployment decision, Verification Testing is key to determining whether or not the new release has been installed successfully. The following provides a brief summary of the three phases.

5.1 Phase I, DMS Product Test

The DMS Product Test (DPT) is performed jointly by the DMS integration contractor and the Joint Interoperability Test Command (JITC). The test is conducted in the DMS integration contractor integration and test lab. The focus of testing is on new builds received from the product vendors. The tests performed verify a particular product will correctly install, can be configured and all required functions are working. The next step in DPT is a system level test performed to verify interoperability of the entire suite of release products.

5.2 Phase II, DMS Integration Test

The integration test is performed by JITC over a wide area network (WAN) to assess the product release performance in a WAN environment rather than a lab environment. The integration test is divided into three phases.

5.3 Integration Test Phase 1

Integration Test Phase 1 will be conducted by experienced JITC testers at three sites. This testing will ensure the system is correctly configured and that experienced personnel can successfully execute the new test scenarios. These testers also have the experience to verify the interfaces to the AUTODIN system, verify correct functioning of the Network Time Protocol (NTP) and Directory System, perform load testing, and verify fault tolerant features such as alternate routing.

5.4 Integration Test Phase 2

Experience has shown that ordinary users will see and use the system differently than experienced testers do and consequently, will find problems that escape the testing process, regardless of the amount of previous testing. There simply is no substitute for “real users”. JITC will address this issue by having users who are not professional testers send and receive messages during Integration Test Phase 2.

5.5 Integration Test Phase 3

In Integration Test Phase 3, JITC will complete their evaluation of the system. In this phase all components, including the endpoints, will be upgraded to the new release level. Experienced testers will perform this evaluation in a lab environment.

5.6 Verification Test Procedures

Verification testing consists of a series of tests designed to verify that the primary DMS functions are working correctly together as a system after installation of a new product release at a site. Verification testing will be performed by each infrastructure and ACC/LCC site after completing upgrade procedures, to certify that their DMS configuration is performing properly. The test procedures are provided in the ISP. These procedures are generic and have not been tailored to any particular site. Each site should only perform the tests that apply to their particular enclave. Successful execution of the verification tests is required to close the DMS Upgrade Status Ticket and declare the site upgrade

APPENDIX D

DMS SECURITY SERVICES

Note

This appendix reproduces exactly Section 2.5 from Defense Information Systems Agency, *DMS Organizational Messaging Concept of Operations,* DMS Release 2.1 Products, October 24, 1999. This material is reproduced for reference purposes.

1.1 Security Services

DMS security is provided by a combination of Public Key Infrastructure, FORTEZZA services, and Defense Information Infrastructure (DII) defense in depth.

1.1.1 DII Layered Security

DMS security is reliant on the overall DII security posture. Elements of the DII-based defense in depth include: use of protected DOD wide area networks such as the SIPRNET and NIPRNET, use of multiple security domains with physical separation between the domains, host computer protection through use of properly configured secure operating systems, protection of enclave boundaries with firewalls and guards, use of secure protocols for identification, authentication and privacy (e.g., digital signature and encryption), LAN and host enclave monitoring, and Information Warfare (IW) situation awareness. In accordance with MROC Change 2, the National Security Agency (NSA) is responsible for providing flexible, secure products capable of providing a range of digital signature and encryption options, appropriate message security classification labels and markings, and authentication, access management and access control mechanisms. Use of approved NSA cryptography appropriate to the classification and sensitivity of the message is also specified, when required. Note that in addition to using physical separation between security domains DMS will also provide cryptographic separation between these security domains.

Securable operating systems are a key component of DMS security. Beginning with DMS Release 1.1 procedures for securing the operating systems have been developed using DII Common Operating Environment (COE) Security Technical Implementation Guidelines (STIGs). Several IW organizations including DISA’s INFOSEC division and the Air Force Information Warfare Center (AFIWC) have been consulted to provide a plan for incremental and iterative security posture improvement.

1.1.2 Public Key Infrastructure

A public key infrastructure is a set of data structures, personnel, policies, procedures, internal accountability, and management practices that enable the generation and distribution of certificates. This includes a Directory Service in which certificates for users are stored, and a trusted methodology for the issuance of certificates is available.

DMS uses a concept called public key cryptography. With DMS certification, each user is assigned a one key pair for message encryption/decryption and one key pair for signature encryption/decryption. In these pairs, one key is called the *public key* and the other called the *private key*. Each person's public keys are published while the private keys are kept secret. The private key can decrypt that data - and only that data - encrypted with the corresponding public key, and vice-versa. So, while a user can encrypt a message using public information, the message can be decrypted only with the private key which is in the sole possession of the intended recipient. Thus, public-key cryptography can be used not only for confidentiality (*encryption*), but also for authentication (*digital signatures*).

In DMS, every user's public key is kept in the DMS directory so that it is widely available for anyone who wishes to send that user a message. A user's private key is kept on the user's FORTEZZA card, where its use is protected by a log-in process (the entry of a PIN).

A message originator looks up the intended recipients in the DMS directory, and retrieves the intended recipient's address and public key for message encryption. The originator's signature is encrypted with the originator's private key. The message recipient then uses his/her private key(s) to decrypt the message and read it, and the originator's public key to decrypt the digital signature and ensure authenticity as well as integrity.

To support the public key mechanisms an authentication hierarchy is required. The DMS key management concept is based on the multi-level hierarchy recommended in X.509. Each level of the hierarchy derives its authority (certificate) from the next higher level. The initial DMS certificate authentication hierarchy consists of three levels. See Figure 2-2.

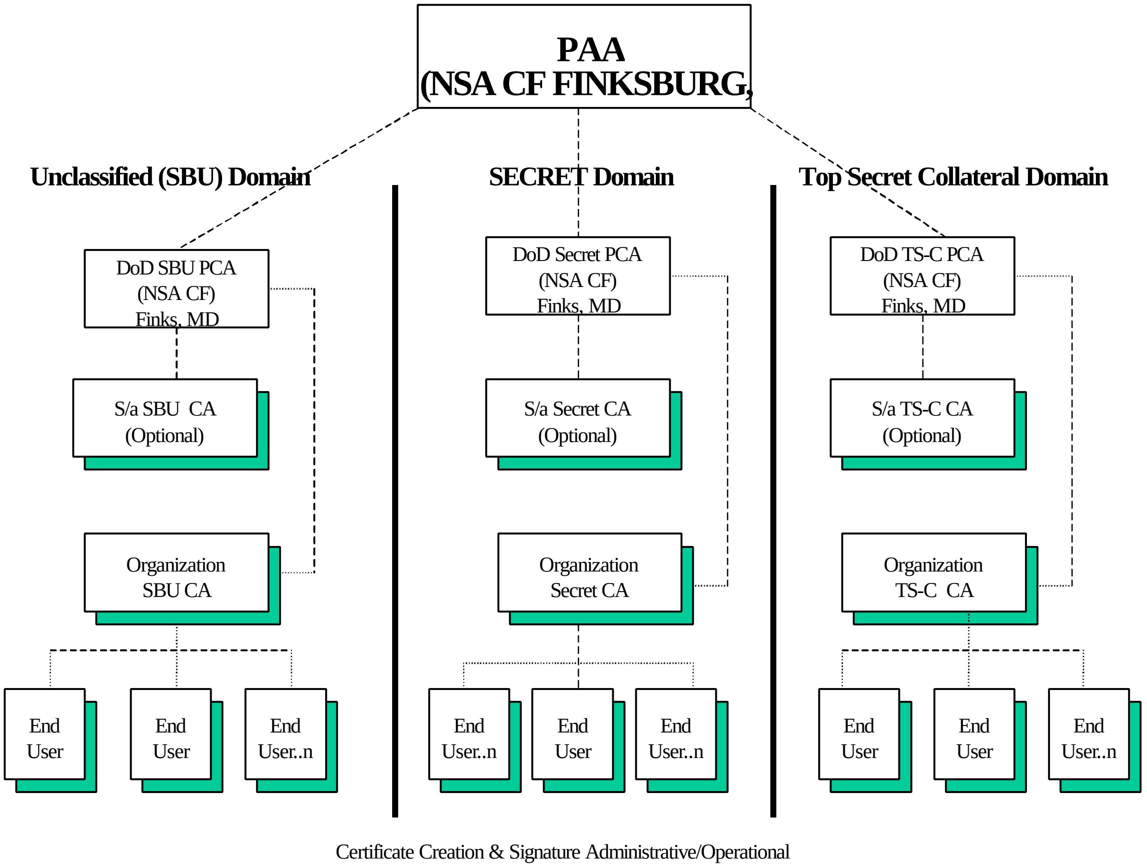


Figure 2-2 DMS Certificate Hierarchy

- Policy Approving Authorities (PAA) are the topmost and most trusted point in the hierarchy. PAAs are responsible for implementing a consistent global security policy. They establish and maintain subordinate Policy Creation Authority components by issuing their certificates. All certificates within a domain are derived from the appropriate PAA so the PAA's certificate serves as the source of authenticity for all certificates created within its domain. The PAA's certificates are self-signed (the DNs for the subject and issuer in the PAA certificate are identical).

- Policy Creation Authorities (PCAs) authenticate the subordinate levels within their domains. Responsibilities include issuing and signing Certificate Authority certificates and programming identities onto FORTEZZA cards. PCAs have been established for the DoD, Civil, and Intelligence communities.

- Certification Authorities (CAs) authenticate users within their domains. They are the focal point for key, certificate and privilege management for end users. CAs initialize and manage FORTEZZA cards for end users. They also maintain a list of revoked certificates and report compromised keys to the PCA.

- Registration Authorities (RA) are appointed by Service and Agencies to establish registration policies and manage directory information. The RA may delegate specific levels of directory implementation management to Sub Registration Authorities (SRAs). Each SRA may delegate data gathering and local user identification responsibilities to Organizational Registration Authorities (ORAs) at the post, camp, and station level. SRAs and ORAs assist the CA/RA with the registration process by collecting and authenticating end user information. ORAs also distribute FORTEZZA cards to users and act as points of contact for user cards, keys and certificates. SRAs are responsible for obtaining unique DNs for the user. They also register DNs with the directory. ORA and SRA roles may be combined in some organizations. Registration Authorities do not sign certificates.

The PAA, PCAs, and CAs use CAWs and ADUAs to perform their functions.

Note that cryptographic separation takes place at the PCA level where different KEA universals are unique to each security domain. DSS universals for signatures are common across all security levels under the PAA. From a user perspective, this means a user can have multiple certificates, or personalities, on a single FORTEZZA card, each personality providing the information necessary for the user to interoperate with other users within a single DMS security domain.

1.1.3 FORTEZZA Services

FORTEZZA-based services for DMS products include confidentiality, integrity, identification and authentication, and non-repudiation. These are dependent on the Public Key Infrastructure (PKI).

1.1.3.1 Confidentiality

Confidentiality ensures privacy of data and is accomplished through encryption. The FORTEZZA card provides an encryption engine using the Skipjack algorithm to encrypt a message such that only the designated recipient can decrypt it.   DMS established high assurance confidentiality services through the use of the Skipjack algorithm and sufficient key lengths. Skipjack is a symmetric encryption algorithm that uses a shared Secret key. The key is exchanged among authorized recipients by encrypting it with the KEA and the private key of the originator and the public key parts of the recipients. The recipient’s public key information is obtained from the certificate maintained in the directory. The originator’s private keys are stored on the FORTEZZA card. Security for DMS is based on ACP 120 and DoD’s Message Security

Protocol (MSP). It provides interoperability across all of the DMS products. Through Release 2.2, DMS will use MSP 3.0 which accommodates X.509 Version 1 certificates. MSP 3.0 provides classification level access controls. DMS 3.0 introduces X.509 version 3 certificates with ACP 120/MSP 4.0. Version 3 certificates will provide message level access controls to include compartment, code word and caveat capability in addition to classification level controls. Other mechanisms for confidentiality are being examined for future implementations. Software FORTEZZA implementations are under development and reportedly provides less assurance. In this case, the same algorithm and key length is used but the keys are stored in software on your computer hard drive or on smart cards instead of the FORTEZZA cards.

1.1.3.2 Integrity and Authentication

Data integrity is the protection of messages against unauthorized modification. In DMS, writer-to-reader integrity is a means by which a message reader can be sure that the received message is the same as the source message. This is achieved by a verification process called "hashing", which is run on the unencrypted message. This process produces a checksum called a "hash value". It is this value which, when encrypted by the originator's private key, is transmitted with the message as a digital signature. The recipient client's MSP decrypts the message and recomputes the hash value. The message hash value is then decrypted with the originator's public key and the two hash values are compared. Any changes to the message during transmission will result in a failure of this comparison.

DMS security policy requires organizational messages be signed. Recipients of an organizational message can verify the validity of the digital signature and be assured both that the message was received exactly as transmitted and that it was actually sent by the purported originator. The fact that the hash value can be decrypted with the originator's public key (from the X.500 Directory) proves that it was encrypted with the originator's private key, available only on the originator's FORTEZZA card. This constitutes a valid digital signature and provides proof of origin that an originator cannot deny (see Para. 2.4.3.4 below). Note that MSP allows a message to be signed without being encrypted. Both signing and encryption are functions of MSP; neither service is available in the P772 environment. The same signing process applied to a receipt notification provides proof of receipt that also cannot be denied.

The MSP process at the DMS client is transparent to the user. The message originator needs only to select an option to sign the message, while the MSP at the recipient's client verifies the signature and hash value and will not allow the message to be opened unless these are valid.

1.1.3.3 Identification and Access Control

DMS provides enhanced Identification and Access Control by using the PIN associated with the FORTEZZA card. Once the user had been authenticated to the card, the user will select an identity, organizational or individual, from that user's set on the FORTEZZA card. This combination of events, what the user *has* (the card), what the user *knows* (the PIN), and specific privileges for accessing DMS services (Organization Messaging Flag, Domain specific KEA and DSS) ensure that only authorized personnel may utilize the card and access authorized DMS services.

1.1.3.4 Non-repudiation

This “proof of participation” EoS is useful when a message recipient wishes to know without question that the purported message originator is the actual originator or when the originator wishes to know without question that a message recipient received and opened the message. It also protects against users denying participation in message exchange when in fact they participate. Non-repudiation takes two forms: non-repudiation with proof of origin and non-repudiation with proof of delivery. Digital signatures are used to provide either form of non-repudiation. Proof of origin non-repudiation is fulfilled by having the originator digitally sign the message. Proof of delivery non-repudiation is provided by having the recipient return a digitally signed receipt.

1.1.4 FORTEZZA CMI Roles

Personnel must be assigned to perform the following roles in support of the FORTEZZA management structure:

a. ISSO – The Information Systems Security Officer (ISSO) must be appointed and trained to perform the following duties:

- Assign security privileges and access controls of users.
- Assign initial account login passwords to all new accounts.
- Perform archive and delete functions of the CAW audit log and the CAW security event. Review audit log at least once per week.
- Ensure that the CA is acting in accordance with all requirements of this document.
- Act as the root password holder if access to the root account is needed.
- Act as the second party in multi-party control (MPC) operations, when needed.
- Provide support to the CA if password lockout occurs.
- Perform or assist the Security Officer in performing security investigations in response to CMI-related security incidents (e.g.; lost or compromised cards and/or PINs).

b. **CA** - Certification Authorities are appointed in writing by the site commander and operate CAWs full-time to register FORTEZZA card users and issue their certificates. Specifically, CAs:

- Generate and publish X.509 certificates and CRLs.
- Program, securely distribute, inventory, and replace FORTEZZA cards.
- Perform administrative management of card user information databases, PINs and key storage.
- Perform back-ups of the CAW database each duty day.
- Access the directory each duty day for new CKL.
- Perform inventories of programmed and unprogrammed FORTEZZA cards (with the aid of RAs).
- Assist the ISSO and/or Security Officer with investigations into CMI-related security incidents.

c. **SA -** The System Administrator is a local person who performs the following CAW related duties on a part-time basis:

- Perform initial secure start-ups and all shut downs of the workstation.
- Setup of any new accounts not set up by the CAW installation team.
- Make any necessary changes to the initial network configuration.
- Create an emergency boot floppy to recover from catastrophic system loss.
- Perform weekly system backup and archive functions.
- With ISSO, change the host name and/or internet protocol (IP) address, if required.
- Perform proper system shutdown as required.

d. **RA -** A Registration Authority is appointed in writing by the site commander and assists a CA part-or full-time with registering FORTEZZA card users, by gathering registration information and forwarding it to the CA. RAs can gather data and request, but not **sign**, user certificates.

1.1.5 Operational Security Procedures for FORTEZZA Card Utilization

The section provides guidance on the minimum security related policies and procedures that should be implemented for the FORTEZZA for Classified (FFC) card user/owner. This includes security education, physical storage and safeguards, access controls, and emergency destruction procedures. The Defense Services and Agencies (S/A) should use these guidelines (and other Operational Security procedures for the FORTEZZA card) to develop operational policies for their areas of responsibility within the DMS. The local Designated Approving Authority (DAA) can further promulgate these S/A policies and establish local policy and procedures for the use of FORTEZZA within their area of authority. Refer to Attachment 2 for a detailed overview on policy and guidance discussions.

APPENDIX E

REFERENCES

REFERENCES

General Reference Documents:

1. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, " Revised Defense Message System Transition Plan," Memorandum for Director of Information Systems for Command, Control, Communications, and Computers, Director, Space Information Warfare Command and Control (N6), Director C4I USMC, Director, Headquarters Communications and Information (AF/SC), and Director, Defense Information Systems Agency, Washington, DC, December 28, 1999.

2. Space and Naval Warfare Systems Command, Systems Center Charleston, *DMS Fielding Conference: Brief for Washington LCC,* Charleston, South Carolina, June 17, 1998.

3. United States Coast Guard, *Defense Message System (DMS) Primer: A Coast Guard Introduction to DMS,* Telecommunication and Information Systems Command, Alexandria, Virginia, September 1997.

Program Management Office (PMO) Documents:

1. Defense Information Systems Agency, *Defense Message System (DMS) Interim Procedure 4-V01: System Upgrade Procedures,* DSA DOC 01-046, Arlington, Virginia, December 12, 1998.

2. Defense Information Systems Agency, *Defense Message System Product Plan*, Version 3.03, Arlington, Virginia, August 20, 1999.

3. Defense Information Systems Agency, *Defense Message System Overview*, Arlington, Virginia, February 16, 1998.

4. Defense Information Systems Agency, DISA Defense Message System (DMS) Web site [www.disa.mil/D2/dms/components.html], Arlington, Virginia, October 8, 1999.

5. Defense Information Systems Agency, *DMS Organizational Messaging Concept of Operations*, DMS Release 2.1 Products, Arlington, Virginia, April 30, 1999 (Update).

6. Defense Information Systems Agency, *DMS Organizational Messaging Concept of Operations,* DMS Release 2.1 Products, Arlington, Virginia, October 24, 1999 (Update).

7. Defense Information Systems Agency, *DMS Organizational Messaging Concept of Operations,* Attachment 2, "Operational Procedures for FORTEZZA Card Utilization," DMS Release 2.1 Products, Arlington, Virginia, October 24, 1999 (Update).

Editorials and Issues:

1. Murray, Bill, and Gregory Slabodkin, "DoD Figures AUTODIN Must Run Until 2004," *Government Computer News,* June 15, 1998.

2. Verton, Daniel, "AF Users Say DMS is Not Light or Lean Enough," *Federal Computer Week*, June 14, 1999.

3. Verton, Daniel, "DMS Gaps Force DoD to Keep AUTODIN," *Federal Computer Week,* May 18, 1998.

APPENDIX F

COPYRIGHT NOTE

Note

Inclusion of Web graphics in this document is supported by the following article: Tad Crawford and Laura Mankin, “The Digital Millennium Copyright Act,” *The Editorial Eye: Focusing on Publications Standards and Practices,*Vol. 22, No. 2, Alexandria, Virginia: EEI Press, February 1999.