

SPAWAR Systems Center, Charleston, National Capital Region: A Case Study in Implementing Secure Messaging in an Operational Environment

Background

In 2001, the Chief of Naval Operations directed the establishment of the Naval Network and Space Operations Command (NNSOC) to oversee the metamorphosis of Navy-wide information technology capabilities. NNSOC resulted from the merger of the former Naval Computer and Telecommunications Command and various other Navy activities with information technology roles, including the fledgling Navy Marine Corps Intranet Task Force. Headquartered within Naval District Washington, the primary mission of NNSOC was to oversee the metamorphosis of “Information Technology for the 21st Century” or IT-21 programs, an expansive initiative designed to upgrade, operate and evolve the information systems used throughout Navy tactical and strategic environments.

The establishment of NNSOC produced a cohesive framework to oversee network operations across the maturing fabric of commercial and military technologies, creating a single organization with responsibility for operations and management of myriad systems supporting Navy voice, video and data services.

The Defense Message System (DMS) is a secure X.400-based email system developed by the United States Government, in conjunction with industry partners, to provide for rapid, reliable and secure exchange of critical command and control information. Based on enhanced versions of commercial products, DMS replaced AUTODIN (Automated Digital Network) and a multitude of ancillary systems as the only official means of command and control messaging between the seat of government and the warfighter.

Challenges

Perhaps the most critical near-term objective for NNSOC was directing the evolution of its antiquated network of proprietary components and communications protocols that supported real-time exchange of command and control data between Navy commanders ashore and tactical war fighters worldwide. In its role as Defense Message System (DMS) Global Systems Manager for Navy, NNSOC faced multiple challenges in fielding DMS uniformly into all operational environments. The very nature of DMS’ “writer-to-reader” messaging entailed a fundamental change in relationships between NNSOC operational sites at the Atlantic and Pacific Naval Computer and Telecommunications Area Master Stations (NCTAMS LANT and NCTAMS PAC) and the DMS end-user. The Navy also had to address challenges not previously faced by other DoD and Government agencies, including limited bandwidth available to Navy tactical forces operating shipboard, the unique relationship between deployed shipboard tenants and their afloat host ships and a large number of “Address Lists” required by Navy message system users. Finally, NNSOC must ensure that the large financial commitments of embrace DMS universally were also consistent with long-term Navy objectives of the Navy Regional Enterprise Messaging Solution (NREMS).

1900 M St NW Suite 800, Washington, DC 20036
Main: (202) 355-7400

Fax: (202) 296-8215

SPAWAR Systems Center, Charleston, National Capital Region: A Case Study in Implementing Secure Messaging in an Operational Environment

Technical Solution

DKW played a critical role in Navy DMS evolution. Alongside our Navy partners, we spearheaded engineering, development and adoption of revolutionary new approaches to DMS integration based on “proxy” operations. DKW-engineered proxy solutions recognized the need to contract “writer-to-reader” messaging boundaries in order to centralize DMS operations ashore, while still maintaining the requisite DMS reliability, speed and security and while insulating the Navy war fighter from DMS complexities. The DKW development team integrated many new capabilities into the Defense Message Dissemination System (DMDS) product suite and played a fundamental role in defining operational requirements, technical interface parameters and integration of the ubiquitous SMTP/SMIME systems emerging throughout DoD under the Public Key Infrastructure (PKI) programs. The resulting DMS Proxy User Agent Policy (Interim Procedure 34), released by the Office of the Secretary of Defense to govern these interfaces, finally allowed Navy to design and implement a largely commercial-based solution that satisfied all messaging requirements integral to command and control messaging, but allowed tactical war fighters to participate seamlessly using only email and a web browser. The systems engineered and fielded by DKW are satisfying Navy-wide communications from both NCTAMS as well as providing DMS services to Navy shore activities. They will soon be the primary means of message delivery to all Navy ships, tactical squadrons and strategic activities.

Our design successfully achieved all required delivery assurances, confidentiality and non-repudiation of DMS organizational messages by proxy, and obviating the need for X.400 transports, X.500 directory services and X.509 certificate management at the DMS subscriber location. The NCTAMS DMS Proxy components in our solution function across any available TCP/IP network; however, to achieve delivery assurance and eliminate the need for message encryption, our topology design capitalized on the network path between the NCTAMS DMS Proxy host sites and the recipients on the OCONUS Navy Enterprise Network (ONE-NET), the Navy/Marine Corps Intranet (NMCI) and the Integrated Shipboard Networking Systems (ISNS).

The NCTAMS DMS Proxy exchanges GENSER organizational messages classified up to and including SECRET between the host sites and subscribing organizations, operating on separate Unclassified (NIPRNet) and SECRET-high (SIPRNet) DMS enclaves. The NCTAMS DMS Proxy exchanges messages bi-directionally using DMDS Interchange Format messages to preserve message-unique content in plaintext email, including the recipient information, precedence and other elements of service. A key aspect of our solution is the parallel components, interfaces and message flows between the NCTAMS DMS Proxy host site and the subscriber on the Unclassified and SECRET enclaves. This seamless transition between identical deployments facilitates centralized administration of DMS components, while enabling decentralized administration of user profiles.

The system, designed to operate as a DMS 3.1 Remote Groupware Server (RGWS) using the existing resources of the servicing DSP minimized costs of the new infrastructure. Incoming messages received from outside organizations at the RGWS are decrypted at the NCTAMS DMS Proxy host site and relayed as a PKI/SMIME email to the subscribers. Outgoing messages originated by subscribers are prepared using one either: DMDS Proxy Message Releaser (ProxyMR) Forms for Microsoft Exchange or DMDS Web Proxy Draft/Review/Release Forms or Common Operating Environment Message Processor (CMP). Once the subscriber releases a message, it is relayed to the NCTAMS DMS Proxy host site as PKI/SMIME email and converted to a DMS message and delivered to DMS recipients. In addition to the manufacturer’s guidance and Software Users Manuals, our team developed SOPs that define specific operational and administrative functions at the NCTAMS DMS Proxy host site.

1900 M St NW Suite 800, Washington, DC 20036

Main: (202) 355-7400

Fax: (202) 296-8215

SPAWAR Systems Center, Charleston, National Capital Region: A Case Study in Implementing Secure Messaging in an Operational Environment

Benefits

DKW has supported the creation and operation of the NNOC at the Washington Navy Yard via:

- DMS architecture planning
- Preliminary fielding and functional evaluation of DMS products and topologies in a closed community
- Supporting DMS infrastructure design
- Serving as the primary designer and integrator for the NCTAMS DMS Proxy host site, which functions as the gateway for incoming and outgoing Unclassified and Secret messages
- Seamless bi-directional messaging using DMDS Interchange Format to preserve content, recipient information and other elements of service in plaintext email
- Continuing support of programs, such as Message Conversion System (MCS) and Plain Language Address Distribution System (PLADS), which allows users to cross the bridge between legacy and DMS
- Collecting data and statistics for NNOC, such as traffic metrics and problem analysis
- Ongoing operational support and maintenance

Results

- DKW has installed, configured, tested, and deployed a robust DMS Proxy architecture for the NNOC at the Washington Navy Yard
- DKW facilitated the migration of users from legacy to DMS
- Communications services to fleet units, shore activities, and joint forces are transmitted through a secure, highly reliable messaging system
- DKW planned and executed the transition of over 60,000 users from a Version 1 X.509 Certificate infrastructure to a Version 3 X.509 Certificate infrastructure without loss of service
- Supported closure of legacy system, realizing a cost savings of over \$30M

For information contact Dustin Defee at (202) 355-7406 or ddefee@dkwcommunications.com.

DKW Communications, Inc. provides information technology, software engineering, and business process services and solutions to a range of government customers in intelligence, law enforcement, security, and diplomacy.

1900 M St NW Suite 800, Washington, DC 20036
Main: (202) 355-7400

Fax: (202) 296-8215