NEXOR

MILITARY MESSAGE HANDLING SYSTEMS (MMHS) - ARCHITECTURE REQUIREMENTS

MAY 2017

A NEXOR WHITE PAPER

CONTENTS

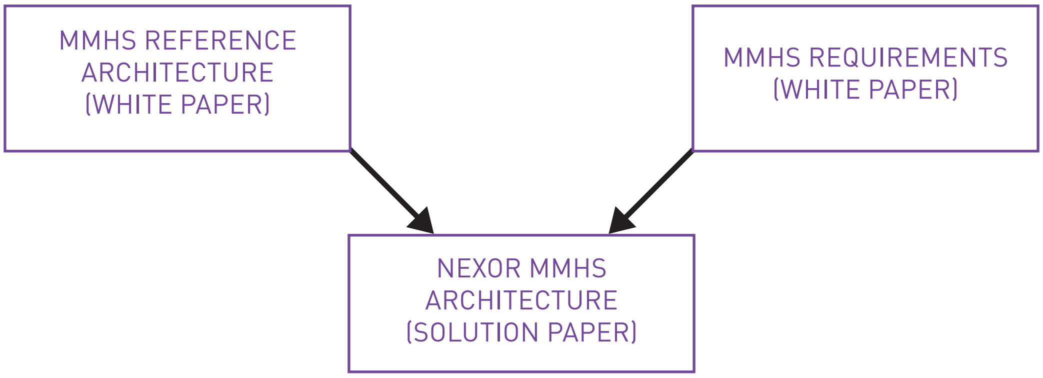
Version 1.0 published August 2008
Version 1.1 published February 2016
Version 1.2 published May 2017

INTRODUCTION

Military Message Handling Systems (MMHS) provide a means of exchanging high grade electronic messages within a national military enclave, between military domains and within operational domains.

Although each implementation of an MMHS may be different, there is usually a common set of requirements that must be met. These requirements cover areas such as security, availability, external connections, ease of use and the automating of various procedures.

This White Paper is one of a set of architectural documents describing the framework of an MMHS. This paper looks at the typical requirements of an MMHS. It should be read in conjunction with the MMHS Reference Architecture white paper and the Nexor MMHS Architecture solution paper.

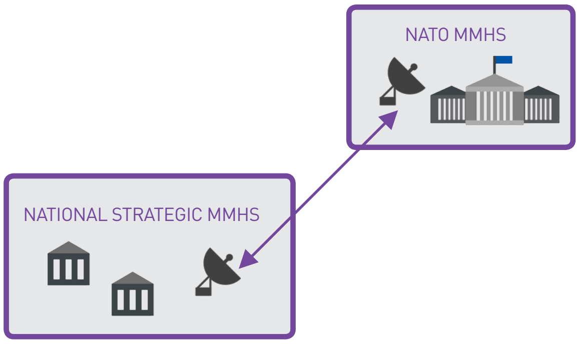

MMHS REFERENCE ARCHITECTURE (WHITE PAPER)
MMHS REQUIREMENTS (WHITE PAPER)
NEXOR MMHS ARCHITECTURE (SOLUTION PAPER)

TYPICAL REQUIREMENTS

This section describes a number of requirements that are common to national Military Message Handling Systems.

NATO INTEROPERABILITY

A major requirement of most national MMHS is that it can connect to other organisations, for example NATO.



For NATO interoperability, an MMHS must provide a STANAG 4406 Edition 2 interface. In practice, this means supporting the X.400 P1 transport carrying Cryptographic Message Syntax (CMS) signed X.400 P772 content.

To share addressing information between NATO and the MMHS, a directory is required that replicates with a NATO border directory. NATO currently specifies that an ACP133 compliant directory is required that can replicate using the X.500 DISP protocol.

To protect the internal national network, a high assurance guard may be required to prevent flow of nationally sensitive information out to NATO.

SECURITY

An MMHS should provide a high level of security in the system. This should include:

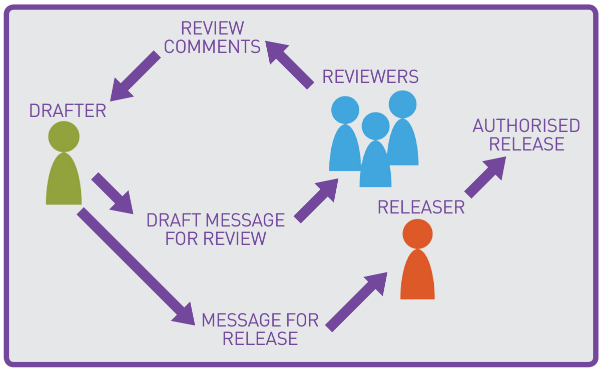
- **Confidentiality** – ensuring that messages cannot be read by those not intended to read them;
- **Integrity** – ensuring that messages cannot be modified without alerting the reader;
- **Non-repudiation of origin** – ensuring that the originator of the message cannot deny having sent it;
- **Non-repudiation of receipt** – ensuring that the reader of the message cannot deny having opened it;
- **Strong Authentication** – ensuring that access to components in the system is by users who are who they claim to be;
- **Access Controls** – ensuring that access to messages or components in the system is only allowed for users that are authorised to do so;
- **Data leakage prevention** – ensuring that only data that should flow between domains is allowed;
- **Availability** – ensuring that the MMHS is highly available by providing reliability of all components, maintainability of the system and survivability of the system following attacks.

EASE OF USE

An MMHS should be easy to use and to administer. Extending standard COTS software to add MMHS specific functionality is one way of ensuring that there are familiar user interfaces and a reduced cost in training users and administrators.

RELEASE WORKFLOW

An MMHS needs to provide a draft and release mechanism to ensure that users who do not have the correct authorisation to release a message have their messages automatically (and transparently) sent to a release authority. Draft messages may have a number of reviewers who will comment on the message prior to it being sent to the release authority for authorised release.



TYPICAL REQUIREMENTS CONT.

ROLE-BASED MESSAGING

An MMHS will be required to support mailboxes for roles and possibly also for individuals. A role mailbox may be configured to allow multiple individuals to access it. MMHS Clients must be able to send messages to and from Role addresses and may have to encrypt messages to allow only role members to access them.

ORGANISATIONAL-BASED MESSAGING

An MMHS may be required to support mailboxes for organisations. An organisational mailbox may have a number of users who access it, or may make use of message profiling. In this case, an automatic distribution agent called a "Profiler" re-distributes messages addressed to an organisation to the relevant roles within that organisation based on various criteria in the message.

A profiler will typically be required to re-distribute messages based on message text, subject, Subject Indicator Codes (SICs) and originator.

FIRE AND FORGET

For high grade messaging, a MMHS must ensure that a message can be sent and that the system will ensure that it is actioned in a timely manner. Specific functionality can be provided to complement an MMHS Mailbox by performing the following functions automatically:

- Monitoring the connection status of the user;
- Alerting the user on a different email address if the user is not connected when new mail of a configured precedence arrives;
- Redirecting messages that are not read within a configured time to a user who can action the message.

ADDRESS LIST EXPANSION

For military messages that are addressed to a distribution list, the system must expand the list to the correct roles. Where the messages are signed and or encrypted, a specialised component is required to verify the signature and redistribute the message to the recipients.

ARCHIVING

All MMHS messages must be kept for a specified period of time in a central, searchable location. Archiving can help to provide for the legal accountability requirement of an MMHS as well as help with messages that require some form of manual intervention.

X.400 CONNECTION

Messages entering and leaving the mailbox component are processed to meet the strict speed of service requirements of military messages. In practice, this means:

- Making multiple simultaneous connections to remote Message Transfer Agents (MTAs);
- Each connection supporting multiple back-up MTAs to ensure the successful transfer of messages in the event of a primary MTA failure;
- Handling messages in precedence order, including the pre-emption of lower precedence messages to get a high precedence message transferred.

These requirements are often met using a dedicated X.400 connector attached to the mailbox component.

DIRECTORY SERVICES

Information about the MMHS users has to be stored in a directory. The information must be replicated throughout the MMHS and must be made available to all components of the MMHS. Access to the directory is usually via LDAPv3.

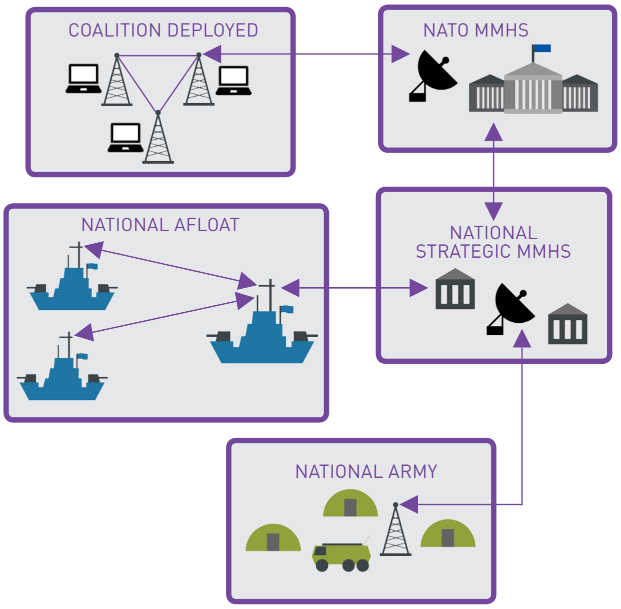
Replication of the directory may be using proprietary methods internally, but at the border to NATO, X.500 DISP replication is specified.

TYPICAL REQUIREMENTS CONT.

REACHBACK CAPABILITY FOR DEPLOYED FORCES

An MMHS that is deployed either on board a ship or in an army field headquarters will require a capability to communicate back to the fixed national MMHS.

This communication may be over low or unreliable bandwidth. There may also be a requirement for communication with coalition forces via the national strategic system and NATO.



DEPLOYED MMHS AT LOWER ECHELONS

Where a MMHS has to reach further into the deployed space down to levels below the headquarters, there will be a requirement for individual users to communicate over low or unreliable bandwidths back to a deployed headquarters.

INTERWORKING WITH CURRENT INFORMAL MESSAGING SYSTEM

Users in the MMHS may require the ability to send interpersonal messages to and from an existing informal messaging system. This may include providing separation between the network running the MMHS and the network running an informal messaging system.

SUMMARY

The MMHS Requirements White Paper simplifies the early stages of a MMHS project by focusing on identifying the typical functionality that a MMHS must provide. It aims to de-mystify MMHS terminology and allow end users to determine which functionality is mandatory versus desirable, thereby enabling the production of a clear specification that is both product and supplier independent.

As such, it is a beneficial tool for the end user community, particularly if a MMHS is a new or unfamiliar subject. Systems Integrators will also find it useful to enable objective engagement with both customers and product suppliers.

Used in conjunction with Nexor's MMHS Reference Architecture, this document aids understanding of how required functionality is provided by the various architectural and interoperability components. This broadens and deepens the MMHS baseline.

For Nexor, using generic MMHS requirements as a start point for discussion engenders a consultative rather than product-oriented approach by ensuring that key functionality is discussed and its importance identified before mapping any products or solutions. This contributes to reducing solution costs and risk.

GLOSSARY

ACP	Allied Communications Procedure
COTS	Commercial Off The Shelf
MMHS	Military Message Handling System
NATO	North Atlantic Treaty Organisation
P1	X.400 transport protocol defined in ITU X.411
P772	Military Messaging Content Protocol defined in STANAG 4406
STANAG	Standard NATO Agreement
X.400	Set of messaging standards defined by ITU
ITU	International Telegraphic Union

ABOUT NEXOR

Nexor has a rich history of deploying MMHS solutions that support mission critical systems. With our heritage in research we continue to innovate and apply this approach to creating solutions to meet our customers' specific requirements.

For over twenty-five years our **military messaging** solutions have been delivered to defence organisations around the globe. In doing so we have developed long-term relationships with key system integrators and military organisations, such as NATO and the European Defence Agency.

Our innovative MMHS solutions have created competitive advantage for our customers and on several occasions we have created a solution that proves to be a technological first.

Underlying our creativity is a value set that encompasses our commitment to customer service, communication and continuous improvement. We believe in 'doing things properly' and that's why our customers have such high levels of confidence in our MMHS solutions.

CONTACT DETAILS

Nexor Limited, 8 The Triangle, Enterprise Way
ng2 Business Park, Nottingham, NG2 1AE, UK

+44 (0)115 952 0500
info@nexor.com
www.nexor.com