NEXOR

MILITARY MESSAGE HANDLING SYSTEMS (MMHS) - A REFERENCE ARCHITECTURE

MAY 2017

A NEXOR WHITE PAPER

© NEXOR 2017 ALL RIGHTS RESERVED

CONTENTS

3 INTRODUCTION

4 REFERENCE ARCHITECTURE

5 ARCHITECTURE DESCRIPTION

7 MMHS CLIENTS

9 MMHS MAILBOX

11 INFORMAL MESSAGING GATEWAY

12 NATO GATEWAY

13 TACTICAL GATEWAY

14 TACTICAL MMHS CLIENTS

15 SUMMARY

16 MMHS TERMINOLOGY AND DEFINITIONS

17 ABOUT NEXOR

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

INTRODUCTION

Military Message Handling Systems (MMHS) have become established as the de facto way of exchanging high grade electronic messages within a national military enclave, between military domains and within operational domains. The NATO and CCEB operational need to interconnect systems from different nations (and hence the systems of the suppliers used by those nations) has led to a much greater demand for interoperability.

This interoperability is enabled by a common set of technical standards and a common set of operational approaches between the communicating parties, which have been developed and implemented over many years.

As a result, the market place will no longer accept MMHS solutions that require large amounts of customisation and bespoke development within each implementation – the expectation is that the internal and inter-working issues have largely been resolved.

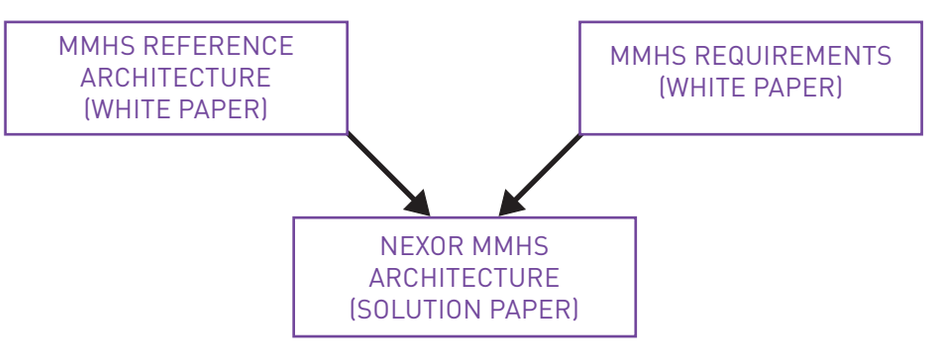
The interfaces are standard, so the expectation is that Commercial-off-the-Shelf (COTS) software should meet the external interoperability needs of any new solution, with modifications to the systems only required to interface to any pre-existing internal elements.

When designing an MMHS for a new environment, or to adapt an existing environment, the key choices become how to adapt or enhance what is already in place, or which standard commercial products meet the interface needs of MMHS interoperability.

The Nexor MMHS Reference Architecture has been created to simplify the scoping and design phases of an MMHS deployment project. It identifies the key components of a solution and defines their functionality – pulling together the common standards and common approaches used in the industry.

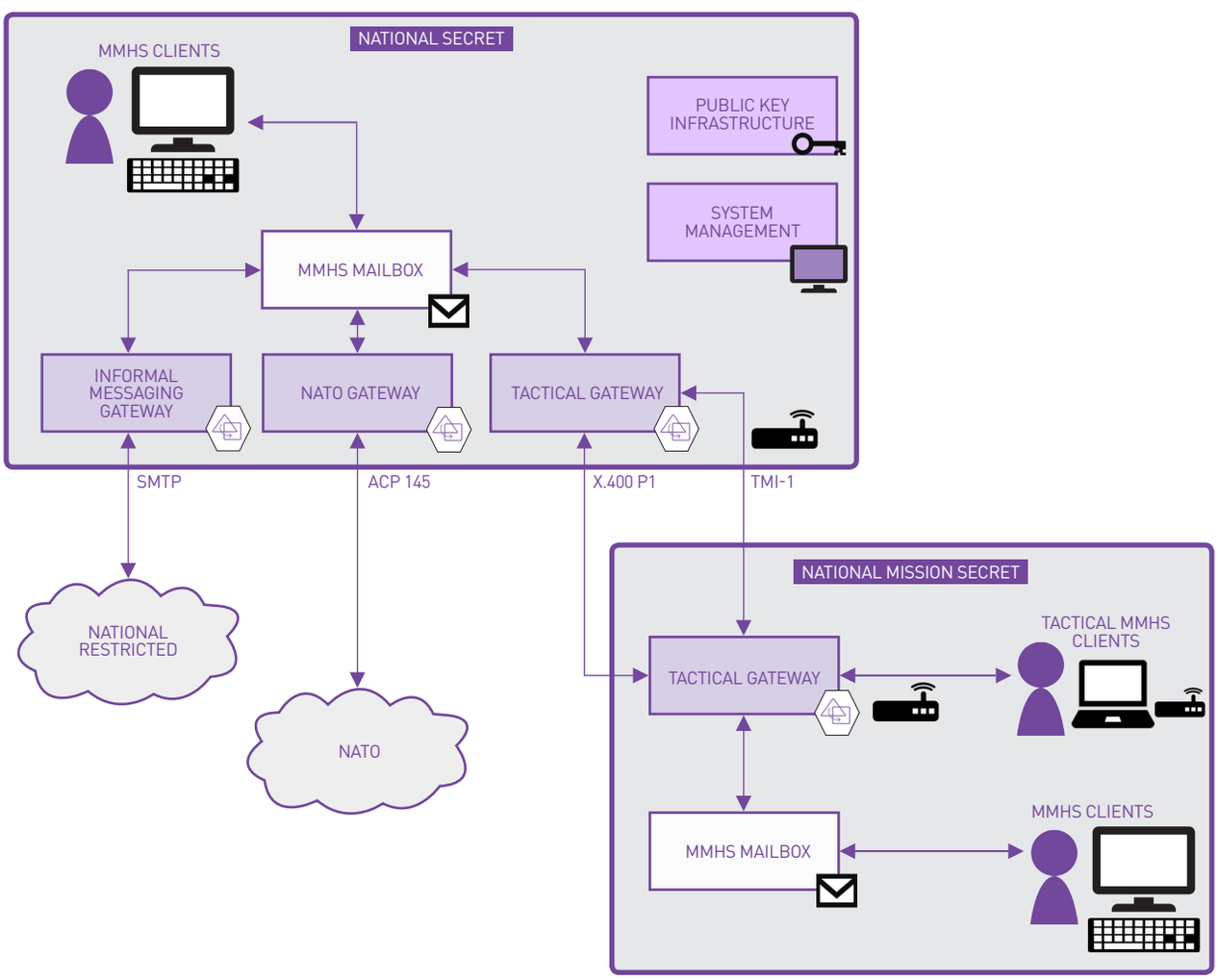
A key part of the Nexor MMHS Reference Architecture is that it is product independent; it defines the major system components and the interfaces between them. In the architecture there is no assumption and no specification of specific vendor components. This way, it allows the operation of a MMHS system to be specified and agreed before being mapped onto solution specifics.

This White Paper is the first in a set of architectural documents describing the framework of an MMHS and provides a high level view of the components, their functions and how they are interconnected.



REFERENCE ARCHITECTURE

The diagram below shows Nexor's reference architecture for Military Messaging Handling Systems (MMHS).



ARCHITECTURE DESCRIPTION

This section provides a brief introduction to each component of the MMHS Reference Architecture shown on page 4. Further details on the individual components can be found in the remainder of this paper.

MMHS CLIENTS

Users create, send and receive military messages formed in accordance with STANAG 4406 Edition 2 and ACP123. Addressing to organisations, roles and individual users is possible. Security can be applied to ensure confidentiality, integrity and non-repudiation, and that messages are correctly labelled. MMHS clients can be based around standard COTS office applications with additional plug-ins or web-based.

MMHS MAILBOX

Sent and received messages are stored in the MMHS mailbox for retrieval by an MMHS Client. MMHS services provided for an MMHS mailbox include:

- Automatic redistribution of messages addressed to an organisation to specific roles (profiling);
- Expansion of messages sent to distribution lists (mail list expansion);
- Monitoring of mailboxes to ensure messages are acted on in a timely manner (fire and forget);
- X.400 connection to other components in the system;
- Automatic archiving of messages.

The MMHS mailbox can be based on standard COTS groupware applications or other proprietary database software.

INFORMAL MESSAGING GATEWAY

Messages can be sent to individual users' mailboxes in the informal email domain located in a security domain below the MMHS domain. MMHS security will be verified and removed and messages converted to standard SMTP format for transfer to the informal email system. Incoming messages can be passed straight through to the MMHS Mailbox.

NATO GATEWAY

Messages can be sent to NATO or to other nations via NATO. MMHS security on the message will be verified and removed and a national signature applied to the message (ACP145). Messages will be scanned to ensure that no nationally sensitive data is sent out of the gateway. Incoming messages will have any signature verified and removed before passing the message into the MMHS.

A directory is available to be able to share specific addresses and distribution lists with NATO and other nations.

TACTICAL GATEWAY

Messages can be sent from the fixed / strategic MMHS to the deployed MMHS. Where bandwidth is low or unreliable, messages can be sent over STANAG 4406 Annex E protocol to a deployed headquarters. Where bandwidth is good, messages can be sent over standard X.400 P1 protocol. A single gateway could communicate with multiple deployed locations.

TACTICAL MMHS CLIENTS

Where users require MMHS at a level below Battalion, tactical MMHS Clients provide a single user workstation capable of sending and receiving military messages in a low / unreliable bandwidth environment. As with the fixed MMHS clients, the user agent can be based on standard COTS office software with additional plug-ins or web-based.

ARCHITECTURE DESCRIPTION CONT.

Where an MMHS is required in a **fixed strategic** infrastructure, the following components may be required:

- MMHS Clients;
- MMHS Mailbox;
- Informal Messaging Gateway;
- NATO Gateway;
- Tactical Gateway.

Where an MMHS is required in a **tactical deployed** infrastructure, the following **additional** components may also be required:

- Tactical MMHS Clients.

Although not covered in any detail in this paper, these two components will also be necessary in an MMHS:

SYSTEM MANAGEMENT

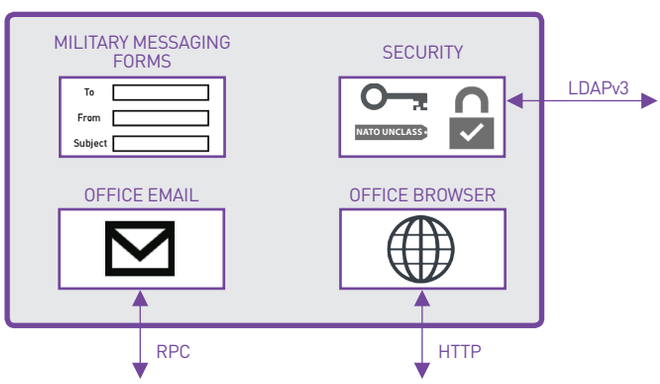
Configuration and monitoring of the MMHS components can be performed from a central location using system tools and the management interfaces supplied with the MMHS specific products.

PUBLIC KEY INFRASTRUCTURE (PKI)

For securing the MMHS, a PKI is required. The PKI will provide a Certificate Authority and a Registration Authority to enable generation and management of certificates and certificate revocation lists. It will also define the method for storing the public keys in a directory and the private keys using hardware or software tokens.

MMHS CLIENTS

MMHS clients enable users to send military messages using dedicated forms to represent the military messaging elements of service. Forms extend standard email messages to include all of the fields required to generate a valid military message.



SECURITY

The MMHS client will ensure that messages are consistently labelled and that services such as confidentiality, integrity, and non-repudiation are offered using digital signatures and encryption. An MMHS client may also perform access controls to ensure messages are only sent and received to users that have the relevant security clearance.

DRAFT AND RELEASE

An MMHS client can 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. Messages will be released by the release authority or returned to the drafter with comments.

FORMATTED MESSAGES

For organisations that require formatted messages such as AdatP-3 and USMTF, a body editor is typically integrated into the client. This editor provides the means of generating valid formatted messages, which are then attached as bodyparts to the military message.

MESSAGE CHECKING

The MMHS client is responsible for ensuring that the messages in the MMHS do not contravene the messaging policies of the organisation. This means ensuring that messages meet the security policies, do not introduce viruses into the system and can meet the speed of service requirements by enforcing limits on message sizes and attachments.

MMHS CLIENTS CONT.

ADDRESSING

The MMHS client should be able to access a directory to allow the user to retrieve addresses and other information used during the composition and submission of messages.

Since the information from the directory is fundamental to be able to secure the messages and correctly address them, the MMHS client should have a number of features to ensure that this information is always available including local caching of entries downloaded from the directory and access to multiple backup directories.

MESSAGE DELIVERY

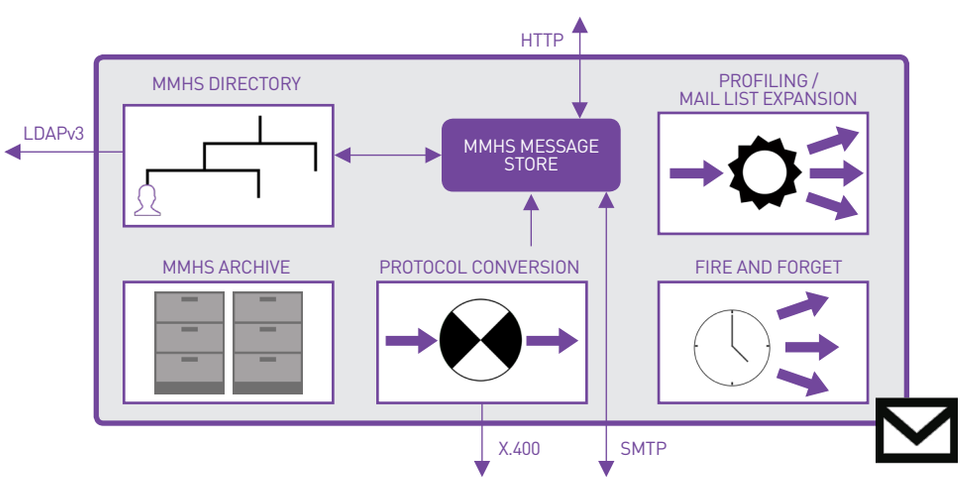
When new messages arrive at the MMHS client, a visible and audible alert will be given to the user. Alerts will be configurable based on various criteria in the message.

An MMHS client will include tools such as automatic filing of messages into folders and sorting of messages using various criteria in the message e.g. precedence, classification. The MMHS client will be responsible for generating notifications when a message has been read or if it is deleted without reading.

MMHS MAILBOX

The MMHS Mailbox provides the local organisation with an MMHS capability. The core of the MMHS Mailbox may be a standard COTS groupware application or a database product.

The MMHS mailbox will hold messages on behalf of the MMHS users and may include message stores for individual, role, and organisational messages. The MMHS mailbox will provide an indication of the outcome of message processing using message tracking logs and reports for message delivery or non-delivery.



MESSAGE PROFILING

Messages that are addressed to an organisation, rather than an individual or role will be handled by a Profiling User Agent. This will redistribute incoming messages to one or more role mailboxes based on the message contents. The message profiling needs to take account of messages that may be signed and/or encrypted. Message profiling will typically be based on Subject Indicator Code (SIC), message text and message subject.

MAIL LIST EXPANSION

Messages that are addressed to a distribution list will be handled by a Mail List Expansion Agent.

This will redistribute incoming messages to one or more mailboxes based on the members of the distribution list which will typically be stored in the MMHS directory. Mail list expansion needs to take account of messages that may be signed and/or encrypted.

MMHS MAILBOX CONT.

FIRE AND FORGET

To get assured delivery of messages, a fire and forget component will typically be part of the MMHS mailbox. When a message is delivered, the mailbox can be monitored to ensure that it has been opened within a given time. If it has not, the message can then be redirected to a guaranteed action point.

X.400 CONNECTIVITY

When messages are sent between organisations, they will usually be sent using X.400 P1 protocol. This provides some advantages over SMTP (which is used by most commercial email systems). The main advantages for MMHS are in a reliable transfer service, efficiency and precedence-based transfer of messages.

ARCHIVING

The MMHS mailbox component also provides archiving of messages. This can be achieved using additional archive mailboxes and addressing to specific archive recipients or by integrating an existing archiving or document management solution.

Archiving needs to take account of messages that may be signed and/or encrypted. Encrypted messages retrieved after a long period of time may also mean that decryption keys have expired.

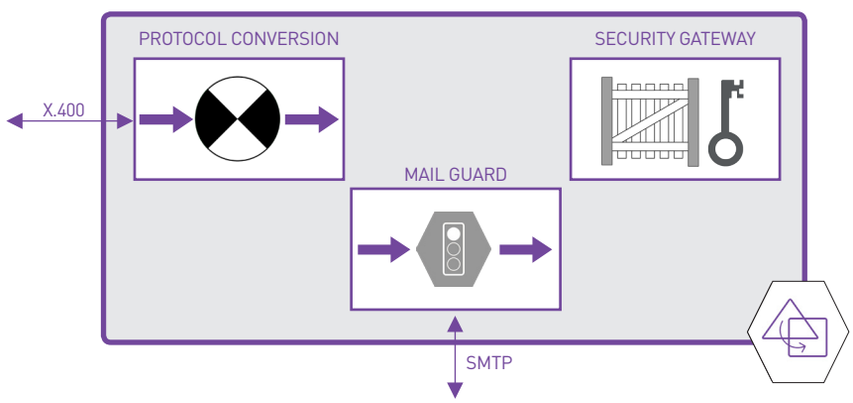
DIRECTORY

The MMHS mailbox component also provides a directory to store user, role, organisational and system wide information. This will include email addresses, PKI information and distribution lists.

The directory may be provided by the operating system infrastructure e.g. Microsoft Active Directory, or could be an LDAP enabled ACP133 X.500 directory. Directory information will be replicated around the MMHS to ensure that each component has access to up-to-date information.

INFORMAL MESSAGING GATEWAY

The MMHS will be used for formal military messaging, but it may require a connection to an existing informal messaging system. This component will be provided by an Informal Messaging Gateway.



PROTOCOL CONVERSION

The MMHS will be generating messages that have military content and may be being sent over an X.400 P1 transport. Typically, an informal messaging system will support the SMTP protocol and will not be able to handle military messaging elements of service such as Primary Precedence.

Protocol conversion allows mapping between the different transport protocols and potentially downgrading the military content to something that can be understood in the informal messaging environment. The MIXER standard (RFC 2156) defines how to map between SMTP and X.400.

SECURITY GATEWAY

A security gateway ensures that MMHS specific security (signature and encryption) is validated and removed prior to transfer of messages out of the MMHS to a system that cannot process them. The security gateway can also add security to messages entering the MMHS from the informal messaging system if required.

MAIL GUARD

Typically, the informal messaging system will run on a network that is classified lower than the MMHS network. A Mail Guard will ensure that only messages that conform to the defined security policy are allowed to leave the MMHS network and pass on the informal messaging network. The security policy may involve checking security labels; message text and attachments; as well as originator and recipient addresses.

NATO GATEWAY

The NATO Gateway component provides a connection between the national MMHS and NATO or via NATO to other national MMHS.

PROTOCOL CONVERSION

A NATO Gateway may require protocol conversion to map between the messaging protocols used internally within the MMHS and that required by a NATO interface. (X.400 P1 as defined in STANAG 4406 Edition 2 with a signed P772 content).

Security Gateway

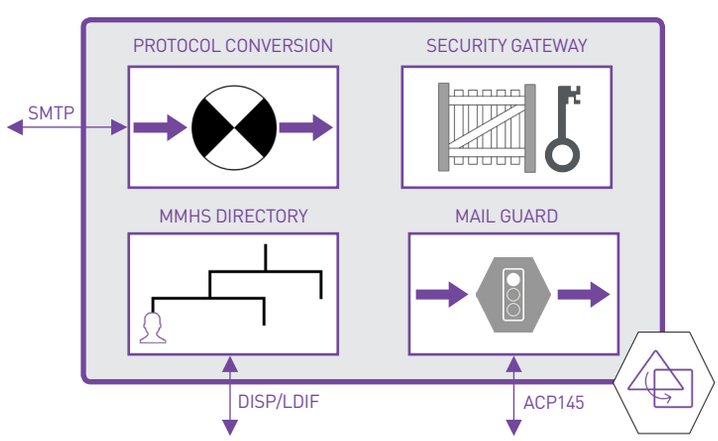
A security gateway ensures that the internal MMHS specific security is validated and removed prior to transfer of messages to NATO. The security gateway will then apply a national signature to the message based on the ACP145 standard. Incoming messages from NATO will have any signature validated and removed prior to messages entering the MMHS.

Mail Guard

A Mail Guard will ensure that only messages that conform to the defined security policy are allowed to leave the national MMHS network. The security policy may involve checking security labels, message text and attachments, and originator and recipient addresses.

MMHS Directory

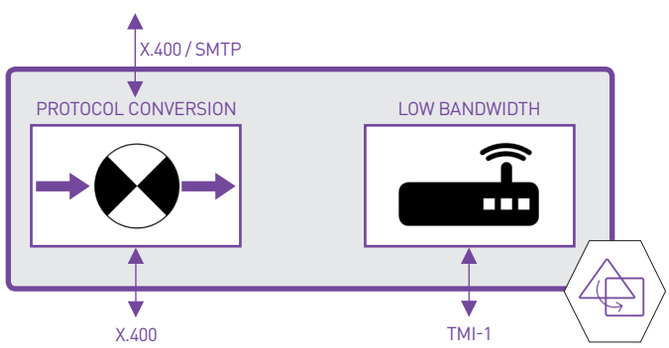
The MMHS directory shares a subset of the national MMHS directory data with NATO and other nations to enable MMHS interworking. This may include a subset of email addresses and distribution lists.



TACTICAL GATEWAY

Where the fixed infrastructure has to communicate with a deployed infrastructure, A Tactical Gateway is required. Communications between the two infrastructures may be high quality, large bandwidth, or low and unreliable bandwidth or a mixture of both.

A standard (STANAG 4406 Ed.2 Annex E TMI-1) has been defined by NATO for transferring military messages over a low or unreliable bandwidth (e.g. < 19Kbps). Where the bandwidth is not an issue, the Tactical Gateway may also be required to transfer data using standard X.400 or SMTP.



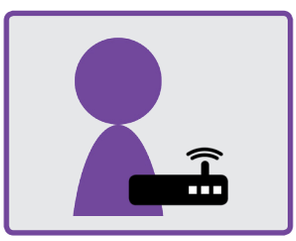
PROTOCOL CONVERSION

A Tactical Gateway may require protocol conversion between the internal MMHS messaging protocol and X.400 in order to use the STANAG 4406 Annex E TMI-1 which is an X.400 based protocol.

LOW BANDWIDTH

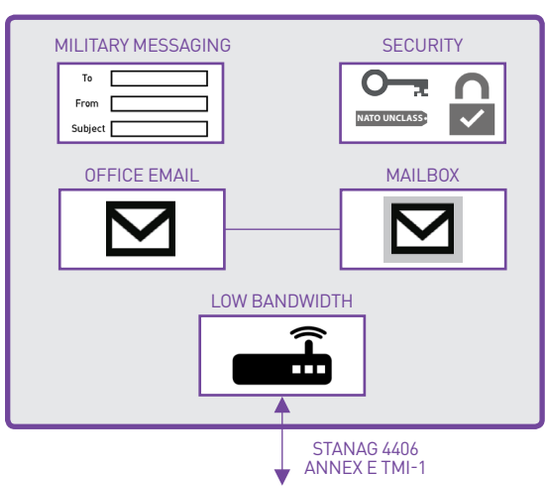
A low bandwidth component which conforms to STANAG 4406 Annex E TMI-1 will ensure that messages are compressed according to the standard and can be sent using multicast or unicast. The Tactical Gateway may be required to handle Emissions Control (EMCON) conditions where either end of the gateway may be unable to transmit data and can only receive.

TACTICAL MMHS CLIENTS



Where an MMHS is deployed to land forces in a brigade or battalion headquarters or to naval forces on a ship, a local area network will include MMHS Clients and MMHS Mailboxes as detailed earlier.

This will provide a local MMHS capability. Where an MMHS capability is required at levels lower than the headquarters (e.g. down to Company level), a single user mobile platform that can handle MMHS is required. The mobile platform must be capable of working offline and also connecting back to deployed headquarters or even back to the fixed infrastructure.



MMHS CLIENT

The Tactical MMHS Client contains a fully functional MMHS Client as used in the fixed infrastructure. The client must be capable of working offline, and so make use of caching and local address books for addressing and PKI information.

MAILBOX

The Tactical MMHS Client includes a fully functional mailbox to be able to store and retrieve messages even whilst communications are not available between the client and headquarters.

LOW BANDWIDTH

In order to communicate with headquarters over low bandwidth, a component is required that can implement STANAG 4406 Annex E TMI-1. This will ensure that messages are compressed handle multicast or unicast, and can run in EMCON conditions.

SUMMARY

The MMHS Reference Architecture simplifies the early stages of an MMHS project by focusing on introducing MMHS terminology and identifying the key system components and interfaces in an entirely product and supplier independent way. It introduces relevant common standards and approaches to ensure that a robust baseline is achieved.

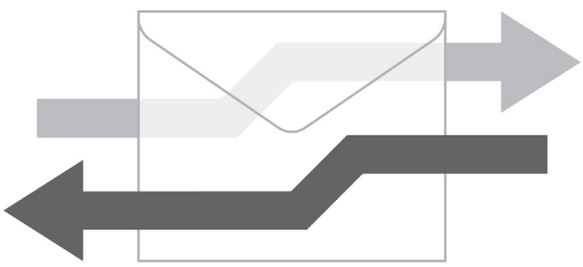
As such, it is a beneficial tool for the end user community, particularly if MMHS is a new or unfamiliar subject. Systems Integrators will also find it useful to enable objective engagement with both customers and product suppliers.

Used in conjunction with Nexor's MMHS Requirements White Paper, this document aids understanding of which architectural and interoperability components provide which functionality. This broadens and deepens the MMHS baseline.

For Nexor, the MMHS Reference Architecture engenders a consultative rather than product-oriented approach by ensuring that key architecture and interoperability needs are clarified before mapping any products or solutions. This contributes to reducing implementation risks and bespoke costs.

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

GLOSSARY

ACP	Allied Communications Procedure
Adat-P3	Automatic Data Processing Publication 3
COTS	Commercial Off The Shelf
EMCON	Emissions Control
ITU	International Telegraphic Union
Kbps	Kilobits per second
MIXER	Mime Internet X.400 Enhanced Relay
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
RFC	Request For Comments
SMTP	Simple Mail Transfer Protocol
STANAG	Standard NATO Agreement
TMI-1	Tactical Messaging Interfaces 1
USMTF	United States Message Text Format
X.400	Set of messaging standards defined by ITU