Isode’s High Grade Messaging Solution

High Grade Messaging (HGM) is used in the UK to describe formal military organizational messaging. NATO refers to this as Military Messaging, which is the term generally used in Isode literature.

This whitepaper looks at Isode’s HGM (Military Messaging) solution, covering end user Web and Mobile clients, messaging servers, interoperability with various military messaging protocols, security, management, and tactical deployment including use of HF Radio. It gives a summary of all the components provided by Isode, with references to product descriptions and more detailed whitepapers.

Isode provides a number of client, server and management products to support HGM (Military Messaging). A site will generally be supported by a number of Isode servers, described in more detail below. The primary Isode end user interface to HGM is the Harrier Web interface, which gives flexible user access to the HGM service. Access to the HGM servers uses open standard protocols, so that other clients may be used. In particular mobile access is supported using Harrier on Android, which provides optimized network performance and user interface suitable for mobile use.
Although a HGM system may be deployed as a single set of servers at one site, a more common architecture involves systems operating at multiple sites with links to partners and tactical units, as shown above. For this type of system, a distributed approach is essential, using communication between HGM servers over a number of different protocols commonly used for military messaging such as MMHS over SMTP, STANAG 4406, ACP145 and ACP127. Isode server & gateway products support all of these protocols. In the event of other protocols being defined to support HGM, Isode could cleanly add them to provide interoperability.

**Isode's Gateway and Server Products**

The Isode HGM gateway, based on Isode's M-Switch MTA, may be deployed as part of the core HGM service or as a separate function. The gateway provides access to core military messaging protocols, in particular:

- **ACP127**: The original text based organizational messaging protocol family.
- **STANAG 4406 and ACP145**: The current NATO standards for military messaging.
- **MMHS over SMTP**: SMTP with RFC 6477 extensions to support military messaging.

**ACP127**

ACP127 "Communication Instructions – Tape Relay Procedures:" is the best known of a number of text messaging protocols used for HGM (Military Messaging). Related protocols in common military use include ACP126, ACP128 and JANAP 128. Although NATO planned to replace ACP127 with STANAG 4406, ACP127 continues to be widely used. Some nations are shifting from STANAG 4406 back to ACP127.

Isode provides support for ACP127 and related protocols in M-Switch, enabling connectivity to ACP127 systems over TCP or Serial Line. ACP127 relay is supported, but the most important capability is flexible gatewaying to STANAG 4406 and MMHS over SMTP, which enables Harrier Web to be used as a client for ACP127 services, with full ACP127 capability provided to the user in a modern Web interface. Further information on M-Switch ACP127 gateway capability is provided in [M-Switch ACP127 Gateway to STANAG 4406 and MMHS over SMTP].

**STANAG 4406 and ACP145**

STANAG 4406 is the NATO standard for military messaging, based on the X.400 family of messaging protocols. STANAG 4406 is widely used. Isode provides two server products for STANAG 4406:

- [M-Switch](#) provides full message switching support for STANAG 4406, and in particular **MIXER** conversion between STANAG 4406 and SMTP with RFC 6477. This enables deployment of full STANAG 4406 communication and integration with Harrier Web.
- **M-Store X.400** provides a full STANAG 4406 mailbox service, enabling access from STANAG 4406 clients using the X.400 P7 protocol.

Further information on STANAG 4406 and Isode STANAG 4406 components is provided on the [STANAG 4406 Military Messaging](#) page.

ACP145 defines a profile of STANAG 4406 and deployment approach for international military messaging gateways. It is being used and adopted by a number of NATO and allied countries, including some that are moving away from internal use of STANAG 4406. M-Switch provides full ACP145 support, and can be used to interconnect ACP145 with a variety of national protocols. Further information on ACP145 is provided in [ACP145: Isode Support of International MMHS Gateways](#).

**MMHS over SMTP**

HGM (Military Messaging) provides formal organizational communication, which should be viewed as a distinct service from informal (person to person) email. This can be confusing, as two of the approaches discussed in this paper to provide HGM are based on standard email protocols. As can be seen from the Harrier screenshots in the next section, the detailed elements of HGM are different to informal email. The associated processes are also different.

Harrier (described below) makes use of standard internet messaging protocol for server access; SMTP (Simple Mail Transfer Protocol) for message submission and IMAP (Internet Mail Access Protocol) for message access. These base standards are extended in a number of ways, particularly with [RFC 6477](#) "Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail". This approach and details on the extensions is given in the Isode whitepaper [Military Messaging (MMHS) over SMTP](#).

The above diagram shows how Harrier uses IMAP to access Isode's M-Box server, which stores delivered messages, and SMTP to submit messages to M-Switch which transfers messages to other servers and delivers messages to M-Box. M-Switch and M-Box are the core servers in Isode's HGM solution; other Isode servers used for HGM are discussed later.
Isode's Harrier Client for Mobile & Web

IMAP and SMTP provide secure open standards access to the Isode HGM servers, which gives flexible access and choice of HGM client. Isode's own client, Harrier, is available as a Web client and as a native Android mobile client.
Harrier on Android

Capabilities provided and shown in the screenshots above include Action and Information recipients (with associated six level precedence), Security Labels, SICs (Subject Information Codes), Message Type, Message Instructuions & Handling Instructions, DTG (Date Time Group) & Filing Time, ZEN recipients (recipients not handled directly), Reply-by & Expiry times and Exempted Recipients.

Harrier on Android gives the UI benefits of a native client, which are particularly beneficial on smaller devices (e.g., phones). By directly using IMAP and SMTP from the client to server, excellent network performance is provided, which can be important when operating over degraded networks. The LEMONADE profile of IMAP and SMTP is used to get best performance, which is described further in [LEMONADE Profile: The Key Standard for Mobile Messaging].

Further information on Harrier Web is provided in the whitepaper [Harrier: Military Messaging for Web and Android].

**Constrained Bandwidth**

Modern commercial email systems will usually operate over very fast reliable networks. With HGM, there is an additional requirement to operate over very slow and degraded networks.

**Messaging Protocols for Constrained Links**

NATO defines an approach for use of STANAG 4406 over constrained networks, which is required for operation over links of slower than 20 kbps. This family of protocols is supported in M-Switch and described in [Military Messaging over HF Radio and Satellite using STANAG 4406 Annex E].
The key protocol supporting this communication is ACP142: "P_Mul – A Protocol for Reliable Multicast Messaging in Constrained Bandwidth and Delayed Acknowledgement (EMCON) Environments". ACP142 defines a multicast communication that operates efficiently over a wide range of networks. M-Switch supports a mapping of SMTP onto ACP142, so the MMHS over SMTP can be provided over constrained networks without the need to convert to STANAG 4406.

**HF Radio & STANAG 5066**

HF Radio is a critical communications technology for HGM (Military Messaging) as it gives an alternate option to Satcom for Beyond Line of Sight (BLOS) communications. It is clearly important when Satcom is not available or there are operational reasons to not use Satcom. HF Radio has performance and operational characteristics that need special protocols. Messaging communication over HF Radio will generally use STANAG 5066 to interface with the modem layer.

Isode uses STANAG 5066 in a number of applications and will support STANAG 5066 link protocols in its planned Icon 5066 product. This is described in the whitepaper [Icon 5066 & Isode's Strategy for Modem Independent Application Deployment over HF Radio].

There are a number of options for sending messages over STANAG 5066. Isode supports a number of standard options and some additional approaches to support STANAG 4406, SMTP and ACP127 communication over HF. These are described in [Messaging Protocols for HF Radio] and [M-Switch ACP127 Gateway to STANAG 4406 and MMHS over SMTP].

**BRASS**

HGM (Military Messaging) makes use of broadcast HF radio to communicate messages to multiple ships using an approach referred to as BRASS (Broadcast and Ship to Shore). This broadcasts messages over multiple HF channels so that ships can receive HGM communication. This will work for ships in EMCON (radio silence) as they can just listen to the broadcasts. For ships not in EMCON, ship to shore channels allow messages to flow in the reverse direction and also to ensure that all broadcast messages are received.

BRASS currently works using ACP127 protocols, in some cases running directly over the modems without STANAG 5066. M-Switch supports these legacy protocols and associated management. Newer protocols, in particular ACP142, are supported to enable migration of BRASS services to newer technologies. This is described in the whitepaper [Isode's Solution for BRASS (Broadcast and Ship to Shore)].

**Reliability, Archiving and Tracking**

HGM (Military Messaging) is used for mission critical communication and messages are often sent over poor quality links. It is critical to ensure reliability. All messages going through M-Switch will be archived in an HGM configuration and accessible by operators with appropriate privileges. This basic capability ensures that operators can deal sensibly with any message loss or retransmission requirements.
Reliability is ensured by use of end to end acknowledgements. Delivery Reports record arrival of messages at the destination. Read Receipts record that message has been read and responsibility taken. M-Switch records details of messages as they are transferred and then records details of both types of acknowledgement as they come back. The acknowledgements are correlated with the original messages, which enables M-Switch management to determine if any acknowledgements are missing or delayed. The operator is alerted to this, enabling appropriate action to be taken. This system also enables audit of successful message transfer, so that service providers can report on quality of service against Service Level Agreements. This is described in more detail in [Using Message Acknowledgements for Tracking, Correlation and Fire & Forget].

Security

Security is crucial for HGM (Military Messaging) and many features of Isode’s product set address security requirements. There are a number of general security capabilities, including:

- Connections generally provide an option to use TLS (Transport Layer Security) to provide data confidentiality and integrity for links.

- Operator access to HGM components uses appropriation authentication and authorization. Message Security and Security Labels are looked at in more detail.

Signing & Encryption

Messages can be signed and encrypted for SMTP (using S/MIME) and STANAG 4406. It is highly desirable to use the end to end security provided by these technologies, and not to simply rely on link security. Harrier Web will support S/MIME security.

It is important to provide server side support for this security for two reasons:

- Message encryption and digital signature is protocol specific. So in multi-protocol environments, which are likely for HGM, there is a need to strip and then re-apply message security as part of the protocol conversion.

- At national and organizations, messages must be decrypted to perform validation of message content. It is often necessary to use different digital signatures, as PKI is typically not integrated and trusted across such boundaries.

M-Switch provides capability to verify message signatures and to sign and encrypt messages. This enables effective use of message security in a cross domain multi-protocol environment.

Security Labels

Use of Security Labels to protectively mark messages and other information is a crucial part of military security. The concept of security labels is straightforward and display and selection of Security Labels in Harrier, as illustrated above, is simple. The underlying technologies associated with deploying interoperable Security Labels are complex. Isode’s approach to this is to abstract the complex functionality into a separate Security Label Server product used as a back end to Harrier and described in the whitepaper.
Easy Security Label Support for Email Clients. This approach enables clean and flexible security label support in Harrier.

Message server support is also needed for security labels. M-Switch ensures that security labels are correctly represented in the necessary protocols. It can also use Security Labels to provide access control and map security labels between different protocols and different security domains. Details are given in Security Label Capabilities in M-Switch.

Directory & Capability Checking

Directory is a key part of an HGM (Military Messaging) solution and Isode includes M-Vault military directory as an element of the HGM solution. M-Vault's capabilities are described in more detail on the Military Directory page and Isode’s directory products are summarized on the Directory Servers & Management Tools page. Directory is an important element of HGM to ensure high quality service. In particular the following capabilities use directory:

- Address Lookup. The model is that all potential message recipients have entries in the directory. The client will be able to look up these addresses using search. This is convenient for the message originator and also helps to ensure that messages are only sent with valid recipient addresses.

- Boundary Checking. When a message goes across a site boundary or cross domain, it can make sense to ensure all addresses are valid. ACP145 requires this and M-Switch supports boundary address checks.

- Encryption. Messages are encrypted using the public key of the message recipient. A message sender can use the directory to retrieve recipient certificates, to enable message encryption to any recipient.

- Security Label checking. Isode’s Security Label Server checks Security Labels against recipient Security Clearance held in the directory. This enables Harrier to present only valid Security Labels for the message recipients. M-Switch can also enforce the same checks on message submission.

- Capability Checking. It is vital to ensure that messages can be received by intended recipient. Some recipients with modern clients such as Harrier can receive messages of large size, any character set and any attachment. An ACP127 recipient might be limited to small messages using ITA2 character set and without attachments. Recipient capabilities can be stored in the directory, which enables Harrier to constrain messages to match recipient capability.

Message Correction and Vetting

When errors occur in an informal email system, "delivery report" errors are generated and sent back to the message sender. This enables the message sender to address the problem. The model of HGM (Military Messaging) is "fire and forget", which means that the sender should never need to deal with message problems.

In order to achieve "fire and forget", messages which cannot be delivered are sent to an operator for correction. M-Switch provides a Web Interface for correction, which enables the operator to take appropriate action. This includes:
Isode

- Changing the recipient address for mis-addressed messages.
- Modifying SICs (Subject Indicator Codes) if they are missing or invalid.
- Removing message attachments (if messages are too large).

A related capability, with a similar M-Switch Web interface is message vetting. This allows operator approval of messages before they are sent. This vetting is often an essential part of HGM message workflow.

**Operational Management**

![ACP127 config in MConsole](image)

Providing a complex mission critical service such as HGM needs sophisticated configuration and operational control. Isode provides this using MConsole, a single management GUI with multiple views to address configuration and operational concerns. MConsole can be used as a diagnosis tool, or for continuous operational monitoring of HGM services.

**Conclusions**

This paper has described Isode’s HGM (Military Messaging) solution, showing how it provides easy to use Web and Mobile front ends in the Harrier products, and a set of server products providing the range of secure multi-protocol capabilities needed in a full HGM solution for operation over fast networks, constrained networks and HF Radio.
The majority of the products and features here are available from Isode now (Harrier as a Beta release). BRASS, Message Correction & Vetting and Capability Checking will be available in future releases. If you are interested in preview access to these capabilities, please contact us.