

## **W h i t e   p a p e r**

Date: March 2006

### **Military Signals, Messaging or Email**

**A discussion on the merits of a single messaging infrastructure in a  
defence organisation**

**Copyright © Boldon James**

**The copyright in this document is vested in Boldon James. The contents of the document must not be reproduced (wholly or in part), used or disclosed without the prior written permission of Boldon James.**

## EXECUTIVE OVERVIEW

The evolution of military messaging systems can be characterised by a number of key features; notably, the requirement to grade messaging functionality according to operational requirement and the subsequent implementation of the operational grades within more than one infrastructure. This multiple messaging infrastructure has proved to be expensive whilst also exhibiting interoperability issues.

As such countries are no longer making a distinction in implementation between Messaging System grades (Traditional Comm Centre Architectures) and Email Systems (Outlook or Notes installed on every desk). Rather, Logical single integrated messaging networks are being deployed with implementations across the network supporting varying levels of grade and security domains with a “single desktop”.

This paper describes this latest trend in the implementation of Email and Messaging Systems in Defence and Military Organisations around the world.

A discussion on what is meant by High, Medium and Basic grade messaging and the associated security implications sets the scene. The latest trend, A Unified Approach to messaging grades is then examined, the benefits of which are numerous including greatly reduced total cost of ownership, homogenous training and administration and improved interoperability.

The paper also discusses how the definition of a Defence Messaging System is extending to cover not just the message flows within a Defence Organisation and individual armed services, but also to include all messaging under the control of that Defence Organisation. Specifically messages between the organisation and specific commercial organisations (suppliers to MoD).

The information in this document is based upon face to face interviews with end users and integrators in the USA, UK, Canada, New Zealand and various European nations. In addition we acknowledge research and output from the NATO MMHS (Military Message Handling System) Working Group.

## GRADED FUNCTIONALITY

The terms High, Medium and Basic Grade are often used to refer to the Functionality, Reliability and Integrity of the Messaging System (see [High Medium and Basic Grade](#) for formal NATO and UK MoD definitions).

### High Grade Messaging

A High Grade Service should be used where operational imperatives demand assured, secure and timely delivery (including Fire and Forget). This level of service should be used for (but not limited to) transactions between Organisations and where delivery is to the role responsible for acting upon that message on behalf of the Organisation. The High Grade Messaging Service is expected to maintain formal audit trails and trace facilities and historic message archives. Survivability in times of crisis is a characteristic of the High Grade Messaging Service.

Messages will usually be signed (and/or encrypted) either by an individual, a Role or an Organisation. Whilst Military message content will usually be initiated within a High Grade environment, non-Military messages (e.g. Intelligence) may equally demand High Grade service levels, possibly utilising message Precedence attribute. Messages may require backwards compatibility with legacy systems (e.g. ACP127).

The user community may expect to continue to make use of the general Office automation features (e.g. Calendar) even within a High Grade system, and may or may not be allowed to send/receive interpersonal messages and use Instant Messaging facilities.

### Medium Grade Messaging

Medium Grade services may tend to be more aligned with a commercial office environment, with interpersonal (as opposed to organisational) messages being the norm. These services are not expected to offer fully assured delivery (standard messaging Delivery Reports and Receipt Notifications might be available, but not "Fire and Forget") or formal audit; and they may not support highly available and survivable network infrastructures. Unlike High Grade Messaging, these grades of services are not intended for mission critical operations or life threatening situations but provide secure messaging services for strategic planning and the exchange of general interpersonal e-mail.

A Medium Grade Messaging Service is expected to provide confidentiality, authentication, integrity and non repudiation services based on digital signatures and user certificates. These facilities make the service suitable for transacting secure military business and e-commerce where there maybe legal implications associated with the delivery of a transaction.

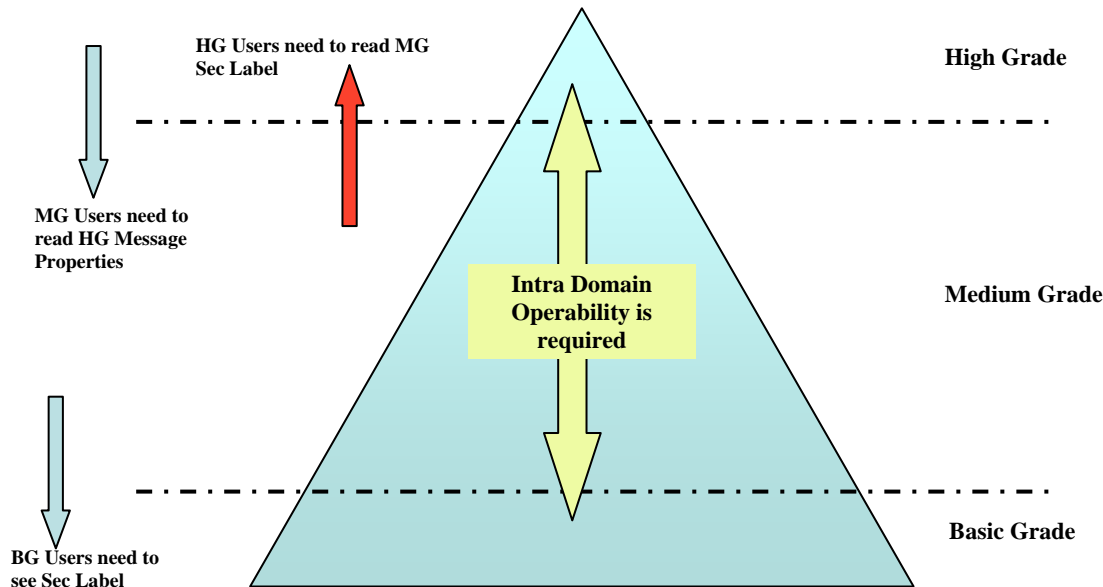
It is a matter for individual system design to define whether (for example) a High Grade Military message is meaningful within a Medium Grade environment. Thus a Medium Grade user may be provided with the ability to view a High Grade message that has been circulated to them, but they may not be allowed to initiate such messages.

### Basic Grade Messaging

Basic Grade has been identified as a separate service due to the simplicity and low cost of implementation, support and management. A Basic Grade system is intended to offer general e-mail and office automation with some basic security (e.g. a Protective Marking label) but without the complexity or requirement for a Public Key Infrastructure (PKI). Again a Basic Grade user may be given the ability to view a Medium Grade message (e.g. handle the fact that it is signed).

## A Single Messaging System

This split between grades of messaging can be represented in a pyramid (below) showing the user population divided horizontally by functionality. The diagram shows for example, a message originated from a medium grade environment may be addressed to a user within the Basic Grade environment.



A granular deployment of increasing, functionality, offering the right interface for the user whilst delivering a cost effective standards conformant solution.

Use of a pyramid illustrates the typical situation where there are relatively fewer High Grade users than Medium and/or Basic Grade users, and that the higher up the pyramid the more specialised the messaging system configuration and usage might be.

Further illustration of these three grades of Messaging Service is provided below giving an indication of their applicability to different defence operations and business needs. The descriptions are not intended to be definitive, but rather to be broad examples of typical qualities of such systems.

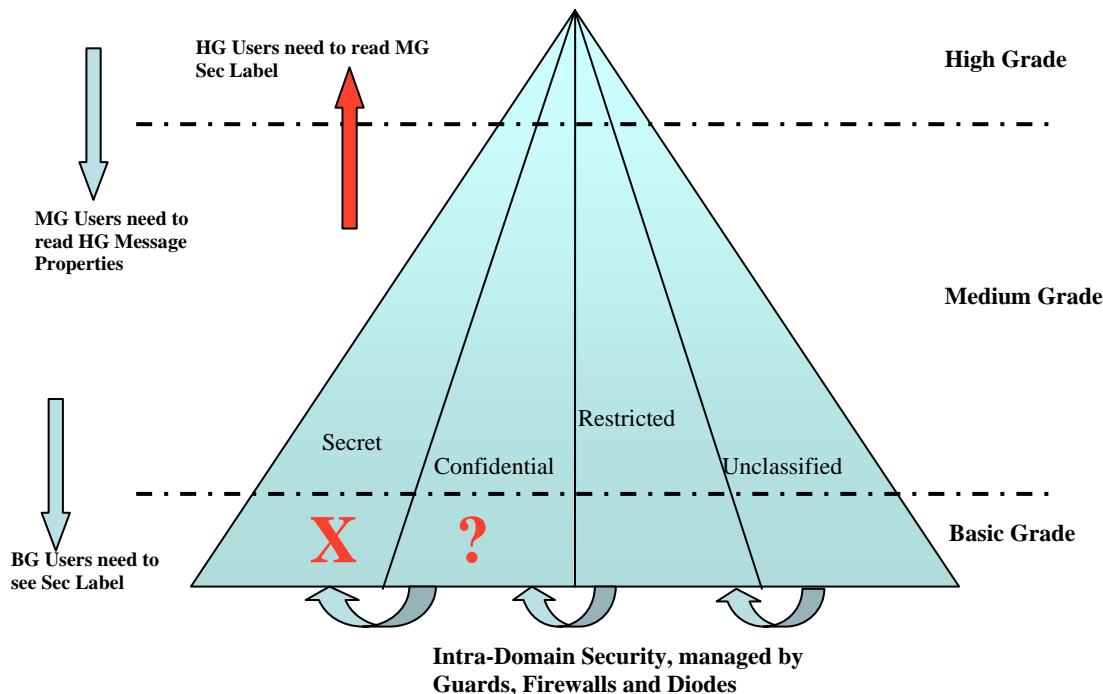
The type of transaction will generally determine the appropriate grade of service as well as the level of functionality and sophistication required of a system. A degree of flexibility must be provided to the user. For instance it would not be appropriate to pass mission critical orders using a Basic Grade system; however, if that were the only form of communication available in the field, then override mechanisms might be defined.

## SECURITY

Security is a key aspect of Defence systems, with all messages being bound by the defined Security Policy. Whilst the overall Policy and associated labels may be quite complex, the single Protected Marking value is often used to describe boundaries and limit User capabilities.

If we now add Security to the pyramid shown above we obtain a picture representing the user population, divided horizontally by functionality and vertically by Security Classification. The diagram

below gives a representation of the message<sup>1</sup> population of a logically single integrated messaging network.



The pyramid is essentially a grid with every cell indicating a possible combination of functionality and security, but presented as a pyramid it??

For example, a message originated from a medium grade environment may be addressed to a user within the Basic Grade environment. If this is a valid operation (permitted by the security policy) then the receiving environment must allow such a message to be viewed, or some transformation must occur en-route.

The pyramid is not proscriptive; rather it presents a single messaging system which in reality may be several discrete systems with air gaps and/or boundary gateways between them. Whenever a message moves from one cell to another it is likely that there will be issues systems designers have to consider.

The pyramid also implies the need to consider the total message traffic on a unified basis, with unified Directory services. The message traffic may include inter-personal, formal and military messaging content; a mixture of transports (typically SMTP and X.400); with different operational requirements applying. It is vital that messaging software provides the basic features AND necessary flexibility if it is to enable systems designers to deliver effective and usable solutions.

Each system may have its own particular definition of (for example):

- The functionality available within a single Grade – indeed there may only be a single Grade within the system.
- The Security Classifications actually available.

<sup>1</sup> A person may have access to multiple user identities, each with different functional and/or security capabilities. An identity may be cleared to receive High Grade messages, but not allowed to initiate them. Thus a complete view is made up of all the possible message types overlaid with the individual user and identity capabilities.

- Whether a specific combination of Grade and Security is valid (for example there may be no Basic Grade/Top Secret messages).
- Allowed message flows e.g. Restricted might be allowed to enter a Top Secret domain, but not vice-versa.
- Individual user capabilities (functional and clearance) will overlay the underlying system features.

Whilst the pyramid indicates that there may be a need to limit a user's ability to send or receive messages with particular content and/or security label there will typically be further limitations such as an individual identity may draft a Secret message, but may not be allowed to release such a message, whilst exceptional circumstances may demand an operational ability to override this rule!

Any individual message has a specific combination of functional and security attributes; selected by the originator, and possibly constrained by the originating environment. The message is addressed to one or more recipients within the same or a different domain with either or both of the recipients and/or target domain having different functional and/or security capabilities.

The pyramid does not imply any particular system topology. For example, a Medium Grade Messaging system may support all the Security levels, or it may be split into two (Top Secret and Secret / Restricted and Unclassified).

In many ways none of the above is new, these sorts of requirements have always existed, but their solution has often forced physical separation of systems, or has meant that all traffic within a system was processed to specifications required by the highest grade information being carried. Alternatively different software is installed incurring major system administration overheads, and it has been difficult to allow users to receive messages of a particular type (e.g. Signed) without also allowing them to originate messages of that type.

The trend is towards a single message box that can present the whole range of messages that users may have to handle, with software providing the separation (e.g. different forms and roles/mailboxes) necessary to enable the user to compartmentalise their activities.

## **A UNIFIED APPROACH TO H/M/B GRADE**

It is interesting to note that the grade definitions above are mostly concerned with level of service and security issues; they refer to message content and format within a grade only as a means of illustration.

This fosters the approach that the messaging system should be considered as a single entity which in itself triggers a subtle change in thought processes that can have far reaching benefits.

For example, where H/M/B Grade systems are considered in isolation there is a tendency to design the software solution to each in response to the stated requirements which may lead to different software deployed in each system with consequent administrative and support costs, especially when system and functional boundaries are subsequently reassessed.

Considering the requirements of all grades of messaging as part of a single unified message system causes designers to start from the position that they want a single (desktop) solution which is then configured at user logon to meet the specific requirements of the individual users and domains. This ensures that administration, support and training can be homogenous and cost effective.

Whilst each grade of system is likely to have specific security policy requirements the overall design should allow for appropriate Security Enforcing Functionality at the clients, servers and Gateways. The architectures may be similar across the grades even if the specific checks are different.

Thus a check at send time that a recipient is cleared to receive some content may consist of a simple comparison of a FLOT (First Line of Text) label value in Basic Grade against Directory held information, but a full ESS Label check by accredited software in a Medium Grade environment at time of send, at delivery and at time of access.

If a unified approach is to work, then there is of course a whole range of practical challenges such as:

- A single overall security policy.
- Definitions of the classes of user to be supported and the specific capabilities of each class and how these relate to the required security domains.
- Directory contents and access to information such as Public Certificates.
- Message formats (e.g. X.400, SMTP, and ACP145) and any Gateways that might be required.
- Migration from, and inter-working with, existing systems, including external allied systems.
- Ensuring that the flexibility provided by this unified approach does not just lead to choices not being made and systems end up with too many options.

## An Example

The following presents a summary description of possible system functionality.

**High Grade messages** use standard Outlook with extensions and can contain Military (P772) content that is Signed and optionally encrypted. Messages are encoded as PCT. A NATO Policy is in use for labelling of messages. Recipient clearance and capability is checked before sending.

**Medium Grade messages** use standard Outlook with extensions, but do NOT contain Military attributes. Messages will be signed, but encryption is not available. Messages are sent as S/MIME (with ESS labels). As in High Grade a NATO Security Policy is used for Labelling. Recipient clearance and capability is checked before sending.

**Basic Grade messages** use standard Outlook. They cannot be signed or encrypted and can have no security label. Messages are encoded as MIME.

A **High Grade user** can send and receive High Grade Messages and medium grade messages (by selecting Military or standard message forms).

A **Medium Grade user** can send and receive Medium Grade and Basic Grade messages (distinguished by the existence of a label or not). A medium grade user can also view a High Grade message (note that if the message was encrypted then the user must have a suitable private key to decrypt). If a high grade message is received, it cannot be forwarded other than by downgrading it to a Medium Grade message (i.e. all Military elements of service are lost). (See also \* below)

A **Basic Grade user** can send and receive Basic Grade messages and can view (signed) Medium Grade messages.

- \* The system might be further structured so that there are two security domains where one domain contains a mixture of High Grade and Medium Grade users (but no Basic Grade) and the other has only Medium and Basic Grade (no High Grade), and High Grade message were

not allowed to flow outside the higher domain. In this case the Medium Grade users within the 'lesser' domain would not require the ability to view high grade messages with a consequent reduction in costs.

The above functionality can be delivered using a single desktop solution. Specific users gain access to specific features according to their and the local system configured capabilities.

The above assumes that individual identities will only receive messages for which they are cleared – i.e. that the relevant user access controls are in place.

## INTERNATIONAL TRENDS

Major systems around the world (e.g. UK DII, US DMS and others) are already evolving systems to use the "Single Desktop / Multiple Role" approach with H/M/B Grade messaging capabilities and with users able to send and receive a variety of message contents (MIME, S/MIME, PCT).

These systems are directed not only at the traditional operational defence messaging requirements and the latest standards (e.g. STANAG Ed2, JSP457 ACP145), but the meaning of a defence system is also expanding to cover day to day interactions between defence organisations and defence contractors which is bringing fresh design requirements.

Another trend is to provide more capability through WEB interfaces. For example, Outlook Web Access can be extended to allow Military Content messages to be handled, which in turn may make it feasible to handle messages on lightweight devices such as palm pilots.

## Future Challenges

The messaging systems described earlier in this document cover the organisational message flows, but information flows at the 'sharp end' may use 'convenient' mechanisms such as 'COTS Instant Messaging'. Such mechanisms are used because they meet an operational need even though they are deficient in a number of aspects normally essential to in theatre messaging. Can the necessary features be added without compromising the very qualities that make such mechanisms useful? For example:

- Security - Can confidentiality be assured if necessary?
- Integrity - Can a conversation be guaranteed as unchanged between send and read?
- Non Repudiation - Are the Writers and Readers really who they purport to be?
- Classification - Can we add a security label to a conversation and monitor the system to ensure that individuals who fail the clearance check cannot join the conversation?
- Archive - Can we record the content of the conversation as well as details of participants, times and dates?
- Persistence - Can we review the history of a conversation?

## CONCLUSIONS

Designing and deploying a single messaging infrastructure reduces costs and increases operational benefits by:

- Allowing equipment sharing – the same kit can be used by different individuals who will be presented only with the functionality defined by their profile
- Common training since user interfaces and operational processes can be common - with extension modules for the needs of higher grade users and administrators.

- Common Software can be rolled out with central configuration of users and systems to apply the necessary constraints.
- Subject to security policy a user may log on anywhere as the relevant software will be available.
- The same station can be used by one individual to act in a number of Roles.
- Interoperability between different levels within the system

Clearly this approach does bring challenges such as the need for a common infrastructure (e.g. Directory services and Security Policy), but it should be recognised that it is more cost effective to address issues at system design time rather than at system integration time (or later!).

## High Medium and Basic Grade Definitions

NATO Definitions are taken from Stanag4406 Annex F. UK Definitions are taken from UK MoD Policy: Defence Messaging Jan-05)

High Grade	Nato	<b>A High Grade Messaging Service</b> is the mechanism for exchanging critical information and official correspondence throughout Defence Organisations and with its partners, in a manner optimised to meet stringent requirements for <b>assurance of delivery, survivability, reliability, ease of use, security, integrity, non repudiation and archiving</b> commensurate with a general purpose service.
	UK MoD	<b>High Grade Messaging</b> will provide a <b>resilient service</b> for use in command and control environments where <b>guaranteed delivery and non-repudiation of origin and receipt are required</b> . The primary purpose of HGM is to support operational tasks and Crisis Management situations. It will replace the existing Formal Messaging Service and be interoperable with the MGM service.
Medium Grade	NATO	<b>A Medium Grade Service</b> is the mechanism for exchanging important information between individuals throughout Defence and its partners, in a manner optimised to meet <b>assurance of delivery and security</b> . It is differentiated from High Grade by its emphasis on the <b>originator accepting responsibility for ensuring delivery</b> having been achieved.
	UK MoD	<b>Medium Grade Messaging</b> will provide a general purpose service, designed to provide for routine unstructured information exchange processes. These are messages containing non time-sensitive operational and operational support information. Some users will be provided with the capability to <b>send and receive</b> messages (including organisational messages) <b>to or from the HGM service</b> .
Basic Grade	NATO	<b>The Basic Grade Service</b> is the electronic mechanism for exchanging routine information between persons throughout Defence and its partners, in a manner optimised to deliver a basic capability in the cheapest way consistent with <b>basic requirements for security</b> .
	UK MoD	<b>Basic Grade Messaging</b> is for exchanging routine information between individuals throughout Defence and its partners, under the control of MOD. It is characterised as 'fire and hope' as there are no guarantees of message delivery. It should <b>not be used for official correspondence, without appropriate procedures in place to confirm the message has been received</b> .

## **About Boldon James**

We are a successful organisation focused on providing messaging and connectivity software solutions tailored to key vertical markets including, Defence, Aviation and Government. In the UK our high grade consultants extend this offering by assisting organisations to manage IT and operational risks through a portfolio of services.

The utilization of commercial off-the-shelf (COTS) software at the core of our messaging and directory solutions enables us to provide products which meet the requirements of high grade formal messaging environments such as Defence, Intelligence and Aviation as well as other environments in Government and Commerce.

The Consultancy Services division is focused on the creation of Security Policy, BS7799 implementation (through to certification if required), Risk Assessment, Training and Awareness campaigns, Business Continuity and Penetration Testing. These services are tailored for Central and Local Government, the NHS, Utilities, Police Services and large Corporations and led by consultants who are CESG Listed Advisor Scheme members (CLAS) and CHECK accredited team leaders.

Our robust data communications software provides core functionality in many OSI networks around the world as well as including support for the majority of users of ICL VME (Fujitsu Services) Mainframe Computers both in the UK and around the world.

Boldon James is proud of its reputation which is built on the competence of our staff, many of whom can be categorised as world class performers in their field. Our staff hold an impressive array of relevant professional qualifications and accreditations. We believe that customer service is the key to success.

**For further information please visit: <http://www.boldonjames.com>**