| | | | |
|---|---|---|---|
| **JSP 602 Instruction** | 1016 | **Applicability** | Applications, Infrastructure, Network/Communications, Security |
| **Configuration Identity** | Version: 01.02<br>Amended: 2009-03-02<br>Reviewed: 2005-06-21 | **Epoch Applicability** | 2005 - 2009 |

# JSP 602: 1016 - Messaging Services

## Outline

*Description:* This policy leaflet covers two specific and distinct policy areas, Message Text Formats and Messaging Protocols and Standards. The Message Text Formats section covers the structure and format of military and business formatted messages; the standards for these are independent of the transfer/delivery mechanism. The Messaging Protocols and Standards section covers the mechanisms used for transferring and delivering messages.

*Reasons for Implementation:* Messaging is one of the principal means of achieving information exchange within the MOD and between MOD and other organisations. Standardisation of the MTFs is essential to achieving a common understanding of message contents. Standardisation of the messaging protocols is essential to message delivery and the provision of the different grades of messaging service that are necessary to meet the MOD's needs.

*Issues:* Message Text Formats, in particular Military MTFs, are applicable across all GII domains. Due to bandwidth limitations in the Tactical domain, data compression needs to be considered particularly where MTFs are encoded using XML (see JSP602: 1031 XML Policy).

Also, because Messaging services extend to all GII domains they will utilise bearer systems with a wide range of bandwidth capabilities. There is a significant risk of overloading low bandwidth bearers with messages and large attachments.

Instant Messaging protocols (such as XMPP) are not covered by this policy. Other highly interactive forms of communication (e.g. whiteboarding) are covered under JSP602: 1005 – Collaboration Services.

*Guidance:* MOD currently requires five types of messaging: Very High Grade, High Grade, Medium Grade, Basic Grade and Public Service (for definitions see 'MOD Policy for Defence Messaging' - DGINFO/DCBMJ6/J6 Pol/Defence Messaging). The first three types will typically be implemented using Formal Messaging Standards; the other two will typically be implemented using interpersonal messaging standards.

This policy is consistent with the NC3TA with the following exceptions:

- OS-OTG (formerly known as OTHT-Gold) is not mandated within the NC3TA.

This policy is consistent with the e-GIF with the following caveats:

- For Interpersonal Messaging, the e-GIF does not specify the use of IMAP;
- The e-GIF does not address Formal (X.400 based) Messaging.

## Policy

The following table covers the policy relating to Message Text Formats.

**Strategic**

**1016.01: Interoperability with NATO**

**1016.01.01** All systems and/or projects required to interoperate with NATO systems using character oriented messages shall use the following message text formats:

> **1016.01.01.01** FORMETS/ADatP-3 baseline 12.2 - as defined within APP-11 NATO Message Catalogue
>
> *Comment:* FORMETS is intended to be used for all formatted character-oriented messages within the NATO Command, Control and Information System (NCCIS). FORMETS consists of five parts. Part I defines the rules for designing standard message text formats. In FORMETS, messages consist of a number of sets, which are built from a number of fields. Parts II-IV provide catalogues of message text formats, set formats and field formats, respectively. Part V provides a directory intended to help users determine whether an approved standard pertaining to a specific subject is available.

**1016.01.02** Where Message Text Formats are not defined within APP-11, then systems and/or projects shall follow the rules defined within the following standard:

> **1016.01.02.01** STANAG 5500 - NATO Message Text Formatting System (FORMETS), ed.4, Allied Data Publication 3 (ADatP-3) Part 1

**1016.02: Interoperability with US DoD**

**1016.02.01** All systems and/or projects required to interoperate with US DoD systems using character oriented messages shall use the following message text formats:

> **1016.02.01.01** MIL-STD-6040 - United States Message Text Format (USMTF)
>
> *This is the approved standard for use by all Departments and Agencies of the US DoD.*
>
> *Comment:* The USMTF Program, as set forth in MIL-STD-6040, establishes the standards and prescribes the rules and conventions governing message text formats. These rules and conventions apply to all formatted messages falling under the purview of the USMTF Message Text Formatting program. Data elements described within the governing MTFs establish standards for all joint reporting systems.

**1016.02.02** All systems and/or projects required to exchange MTFs with US maritime forces shall do so using the following standards:

> **1016.02.02.01** Operational Specification for Over the Horizon Targeting Gold (OS-OTG),Change 4:2000
>
> *OS-OTG is a predominant standard for MTFs that provide interoperability with US Forces.*

**1016.03: Military Message Formats for use within GII**

1016.03.01 All systems and/or projects required to send and/or receive formatted military messages shall do so using the following standards:

**Strategic** (continued)

**1016.03.01.01** FORMETS/ADatP-3 baseline 12.2 - as defined within APP-11 NATO Message Catalogue

*UK policy is to adopt NATO APP-11 MTFs.*

*Comment:* Military Messaging Formats- For intra UK exchange use appropriate MTFs or construct appropriate MTFs using the NATO rules for designing MTFs.

**1016.03.02** Where Message Text Formats are not defined within APP-11, then systems and/or projects shall follow the rules defined within the following standard:

**1016.03.02.01** STANAG 5500 - NATO Message Text Formatting System (FORMETS), ed.4, Allied Data Publication 3 (ADatP-3) Volume 1 (see comment under Interoperability with NATO)

**1016.03.03** All systems and/or projects required to exchange formatted military messages with UK maritime forces shall do so using the following standards:

**1016.03.03.01** Operational Specification for Over the Horizon Targeting Gold (OS-OTG), Change 4:2000

*OS-OTG is used predominantly for the exchange of maritime situational awareness information by UK maritime forces. It is also widely used for interoperability with US Forces.*

**1016.04: Business Messaging Formats**

**1016.04.01** All systems and/or projects providing messaging services that support business-to-business interactions shall do so using the following standards:

**1016.04.01.01** EDIFACT (ISO 9735:98)

**1016.04.01.02** ebXML Messaging Service v. 2:2002 (OASIS)

*These are the preferred standards.*

*Comment:* The ebXML standards are mandated within MOD policy on XML. (See JSP602: 1031 XML Policy) which in-turn ensures consistency with the e-GIF.

**Deployed**

As for Strategic domain.

**Tactical**

**1016.05: Interoperability with NATO**

As for Strategic domain.

**1016.06: Interoperability with US DoD**

As for Strategic domain.

**Tactical** (continued)

**1016.07: Military Message Formats for use within GII**

As for Strategic domain.

*Comment:* Bowman provides tools and support for the display of ADatP-3 messages.

**1016.08: Business Formatted Messages**

Not applicable.

**Remote**

As for Strategic domain.

## Policy

The following table covers the policy relating to Messaging Protocols and Standards.

**Strategic**

**1016.09: General Messaging Policy**

**1016.09.01** All systems and/or projects providing messaging services both within the GII and between the GII and external organisations shall follow the MOD policy on defence messaging as laid down within:

> **1016.09.01.01** MOD Policy for Defence Messaging - DGINFO/DCBMJ6/J6 Pol/Defence Messaging
>
> *Comment:* This policy document defines the various levels of Defence Messaging (from High Grade to Public Service) and sets the policy on attachments. It identifies the need to address Special Handling, Electronic Security, personnel and training if new messaging services are to be successfully implemented.

**1016.10: Formal Messaging Protocols**

**1016.10.01** All systems and/or projects providing formal messaging services shall implement one or both of the following standards:

> **1016.10.01.01** STANAG 4406 edition 1 - Military Message Handling System
>
> **1016.10.01.02** ACP 123(A) - Common Messaging Strategy and Procedures

*These are x.400 based formal messaging services with additional military extensions. These standards include the client/user agent access protocols.*

Comment: STANAG 4406 and ACP 123(A) provide essentially the same messaging service. However, they use different security mechanisms, STANAG 4406 using PCT and ACP123(A) using the CSP as defined in ACP 120. These security mechanisms are non-interoperable. Consequently, for both to be adopted an ACP 145 compliant gateway is necessary.

**1016.10.02** All systems and/or projects implementing either of the formal messaging standards shall also implement the following standard:

> **1016.10.02.01** ACP 145 - Gateway-to-Gateway Implementation Guide for ACP123/STANAG 4406 Messaging Services
>
> *This is the internationally agreed standard for messaging interoperability between nations.*

*Comment:* Formal military messages are legally binding in Civil and Military Law and are subject to formal release and commitment. They use Precedence and require guaranteed delivery and archiving.

**1016.11: Legacy System Protocols**

**1016.11.01** Systems and/or projects required to interface with legacy systems, which provide High Grade Message services using Tape Relay Procedures, shall do so using the following standard:

**Strategic** (continued)

**1016.11.01.01** ACP 127(G) - Communications Instruction Tape Relay Procedures and ACP127 UK Supplement 1(C) - Communications Instructions Legacy ACP 127 Messaging Procedures.

Comment: ACP127-based legacy systems will remain in-service with MOD beyond 2010. These legacy systems will be phased out as newer messaging services are procured by MOD. A number of NATO legacy systems also use ACP127-based messaging. This standard will be required where interoperability is required.

**1016.12: Formal Message Attachments**

**1016.12.01** All systems and/or projects implementing messaging services using STANAG 4406 shall use the attachment definition within the standard.

**1016.12.02** All systems and/or projects implementing messaging services using ACP123(A) shall use the attachment standard as defined in the P772 Content Type.

*These are standards adopted by the UK's major allies including NATO and the CCEB to allow formal message attachments to be sent and received.*

*Comment:* See comment on Formal Messaging Protocols above.

**1016.13: Interpersonal Messaging protocols**

**1016.13.01** All systems and/or projects providing interpersonal messaging (Basic Grade or Public Service) shall implement one or more of the following standards (see comment):

**1016.13.01.01** eSMTP (RFC 1869), SMTP (RFC 821, 1869, 1870) with MIME (RFC 2045) and S/MIME (RFC 2630-2633) encoding.

**1016.13.01.02** ITU-T X.400:1999/ISO 10021 - Message Handling System

*These are the ubiquitous standards for e-mail with extensive product support.*

*Comment:* SMTP is the predominant non-proprietary open standard for e-mail with the most product support. X.400 should only be used where absolutely necessary.

**1016.14: Interpersonal Message Attachments**

**1016.14.01** All systems and/or projects providing interpersonal messaging services shall permit as a minimum the following attachment types and standards:

**1016.14.01.01** Office automation - for standards see JSP602: 1012 - Information Interchange

*Comment:* Office automation attachments include documents (both simple and complex), presentations, spreadsheets, databases and project plans

**1016.14.01.02** Compressed files - for standards see JSP602: 1012 - Information Interchange

**1016.14.01.03** Graphics - for standards see JSP602: 1012 - Information Interchange

**Strategic** (continued)

*Comment:* Sending messages with large attachments across low bandwidth bearer systems/networks should avoided unless absolutely necessary

**1016.15: Interpersonal Messaging Client Access**

**1016.15.01** All systems and/or projects providing client access to interpersonal messaging services shall do so using one or more of the following standards:

**1016.15.01.01** POP3 (RFC 1939:96) - for use with SMTP-based e-mail where there are no client-to-server bandwidth or other communications bearer constraints and mail boxes do not have to be shared with other users

*This (together with IMAP4) is a de facto standard for SMTP-based e-mail access with extensive product support.*

**1016.15.01.02** IMAP4 (RFC 2060:96) - for use with SMTP-based e-mail where bandwidth or other communications bearer constraints apply and/or mail boxes must be shared by more than one user

*This (together with POP3) is a de facto standard for SMTP-based e-mail access with extensive product support. Where possible an IMAP4 service should be provided in preference to POP3.*

*Comment:* With IMAP, messages are retained on the server and clients view the contents. This has particular benefits for low bandwidth connections and when mailboxes need to be shared by several users (e.g. where several users share a common role). With POP3, messages are downloaded from the server onto the client. Consequently POP3 tends to be more bandwidth hungry and it is more difficult to share mailboxes without sharing passwords.

**1016.15.01.03** ITU-T X.400:1999/ISO 10021 - Message Handling System (see comment)

*Comment:* X.400 clients can only be used with the X.400 MHS and should only be used where absolutely necessary.

**1016.16: Electronic Labelling of Messages**

**1016.16.01** All systems and/or projects providing required to provide electronic labelling of messages shall do so in accordance with:

**1016.16.01.01** JSP 457 - The Defence Manual Of Interoperable Network and Enabling Services, Volume 7 Electronic Labelling Services

*This is the current defence standard for the electronic labelling of messages*

*Comment:* JSP457 volume 7 contains information on ASN.1 and XML syntax and includes security classifications as well as national and organisational groupings.

**1016.17: Message Addressing Schema**

**1016.17.01** All systems and/or projects providing formal and/or interpersonal messages shall conform to the message addressing schema defined at:

**1016.17.01.01** DCSA DINSA web site http://www.dinsa.r.mil.uk/directories.htm

*This is the current defence standard and covers both formal and interpersonal messaging.*

**Strategic** (continued)

Comment: The UK Defence Directory Core Schema is not defined in JSP 457; instead it is currently hosted on the DINSA web site so that it can be amended without affecting the issue state of JSP457 volume 4.

**1016.18: Naming Conventions**

**1016.18.01** All systems and/or projects providing formal and/or interpersonal messages shall conform to the naming conventions defined in:

**1016.18.01.01** JSP 457 - The Defence Manual Of Interoperable Network and Enabling Services, Volume 4 Electronic Directory services

*This is the defence standard covering messaging and directory naming conventions.*

*Comment:* JSP 457 contains naming standards for directories and messaging, specifically Electronic Unit Names (EUNs) and other unique identifiers.

**Deployed**

As for Strategic domain.

**Tactical**

**1016.19: Formal Messaging Protocols**

**1016.19.01** For systems and/or projects providing messaging service shall support at least one of the following standards at their boundary: the boundary CIP (hosted on Bowman) may support STANAG 4406.

**1016.19.01.01** STANAG 4406 edition 1 - Military Message Handling System

**1016.19.01.02** ACP 123 - Common Messaging Strategy and Procedures

*Tactical systems typically use bespoke messaging services internally because of the severe constraints under which they must operate. To share messaging services with the rest of the GII they must support these standards at their boundary only.*

Comment: Store and forward is not suitable for tactical command because mailboxes are vulnerable single points of failure, and the mobility of users makes this impractical. More importantly, command messages cannot be left 'pending' within a mail system. Hence systems such as Bowman provide a forward-and-store (as opposed to a store-and-forward) service. Messages are forwarded to the recipient but will only be stored if the user is connected to the radio net at time of delivery. Consequently messages sent to non-connected users will be lost.

**1016.20: Formal Message Attachments**

**1016.20.01** Nothing is mandated in this area (see comment).

*Comment:* Whereas it is not practical to impose size limits on total message size (including any attachments), it is clear that bandwidth constraints will impose limitations on the amount of messaging traffic. To prevent network congestion messaging service providers should ensure that implementation designs seek to make efficient use of the available bandwidth.

| **Tactical** (continued) |
| --- |
| **1016.21: Message Addressing Schema**<br>**1016.21.01** There are no mandatory standards for message addressing schemas. However, systems and/or projects that interoperate with strategic or deployed formal messaging services shall conform to the 'Strategic' and 'Deployed' policy at their boundary/gateway.<br><br>*Comment:* Tactical systems such as Bowman generally define their own message addressing schema for use internally; this is typically a role based naming scheme. Addresses within this scheme are deducible given sufficient knowledge of the current ORBAT. |

| **Remote** |
| --- |
| As for Strategic domain. |

## Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all MOD projects (and their suppliers) that use character-based Message Text Formats (either Military or Business) and/or provide messaging services (either formal or interpersonal).

## Procedure

*Message Text Formats:* The principal owner of this policy with respect to MTFs is IA6. All systems and/or projects should contact the IA-6b (ia6b@dpa.mod.uk Tel: ABW (0117 91) 34187) and consult the IA MTF web site (See links below).

For further assistance on MTFs contact: IA-6d (ia6d@dpa.mod.uk Tel: ABW (0117 91) 34164.

Any issues with respect to character-based messaging should be addressed to the Formatted Messaging Requirements Working Group (FMRWG), CBMJ6-Pol2.

Any technical issues with respect to character-based messaging should be addressed to the Formatted Messaging Configuration Working Group (FMCWG), IA6.

*Messaging Protocols and Standards:* DCSA AD Defence Messaging Group is responsible for provision of core high grade messaging services. Point of Contact DCSA Msg-DMG AD: (CE-H4 F001, 3144CE, Tel: 01225 813144).

The principal provider of high grade messaging systems is the Comms Messaging IPTs. Point of Contact Comms Msg/IPTL: (Tel: ABW (0117 91) 33127).

Enquiries as to the maintaining and updating of JSP457 should go to DCSA CM-DINSA Hd.

## Relevant Links

JSP602 1008 - Collaboration Services

JSP602 1012 - Information Interchange

JSP602: 1031 - XML Policy

JSP457 The Defence Manual Of Interoperable Network and Enabling Services can be found here (not yet available). (http://www.ams.mod.uk/)

The IA web site for MTFs can be found here (RLI only).
(http://y4.dpa.r.mil.uk/kb/Organisati/SGs/IA/MTF)

DGINFO/DCBMJ6/J6 Pol/Defence Messaging - MOD Policy for Defence Messaging (not yet available) (http://www.ams.mod.uk/)

UK Defence Mandatory Core Schema can be found here (RLI only).
(http://www.dinsa.r.mil.uk/directories.htm)

The DINSA web site can be found here (RLI only). (http://www.dinsa.r.mil.uk/)

ACP123(A) Common Messaging Strategy and Procedures can be found here.
(http://www.dtic.mil/jcs/j6/cceb/acps/)

ACP 127(G) - Communications Instructions Tape Relay Procedures here.
(http://www.dtic.mil/jcs/j6/cceb/acps/)

ACP145 - Gateway-to-Gateway Implementation Guide for ACP 123/STANAG 4406 Messaging Services can be found here (not yet available). (http://www.dtic.mil/jcs/j6/cceb/acps/)

Details of those RFCs listed can be found here. (http://www.rfc-editor.org/rfcsearch.html)

ISO standards can be purchased from the ISO web site here.
(http://www.iso.org/iso/en/CatalogueListPage.CatalogueList)

ITU-T standards can be obtained (subscription required) from the ITU web site here.
(http://www.itu.int/ITU-T/index.html)

A glossary of terms and abbreviations used within this document is available here.

Instructions on how to read a JSP602 leaflet are available here.

## Compliance

| Stage | Compliance Requirements |
|---|---|
| **Initial Gate/DP1** | MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s). |
| **Main Gate/DP2** | MOD Projects shall reference in their SRD (and MODAF technical views) the specific policy elements contained within this leaflet that are applicable to the system, equipment or application they are procuring or updating. |
| **Release Authority/DP5** | MOD Projects (supported by their equipment suppliers) shall provide evidence of their compliance with the elements of this policy defined within the SRD (and MODAF technical views). Evidence of conformance with standards shall be presented; sources of evidence may include: conformance/compliance certificates provided by equipment suppliers (e.g. under type approval or other assessment regimes), demonstrations, inspection, analysis, tests carried out by suppliers (e.g. Factory Acceptance Tests) and tests carried out at Defence Test and Reference Facilities. |