JSP 602 Instruction	1018	**Applicability**	Infrastructure, Network/Communications
Configuration Identity	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-21	**Epoch Applicability**	2005 - 2009

JSP 602: 1018 - Minimum Standards Profile

Outline

Description: This policy leaflet covers the definition of a minimum profile of services and standards that provide a boundary within which systems must be implemented, as well as enabling a basic level of interoperability between component networks and systems. It defines a coherent set of standards that provide what is deemed to be the minimum useful capability.

Reasons for Implementation: To support the goal of widespread interoperability, this policy leaflet defines a minimum profile of services and standards that are sufficient to provide a useful level of interoperability. This profile uses only those services and standards that are already part of the JSP602 series of policies, however it presents them as a simple, yet comprehensive protocol and service stack.

Issues: Users will attach and authenticate to their local system/network. Information will only be shared using the limited set of services provided.

Guidance: This policy leaflet assumes that interoperability will be supported through tightly controlled boundaries between component networks and systems; these may be connected directly or via third-party WAN(s). A limited set of services will be supported at the boundary, these requiring server-to-server interactions only.

The complete set of shared services will be a combination of the user-level services supported across the boundary and the infrastructure services necessary to deliver them. The user-level services that realistically can be shared are:

• E-mail with attachments

• Web publishing/access

• File transfer

• News (Usenet)

To implement these services, other services must also be defined: Application layer services (including Domain Naming and IP Addressing), Transport layer services, Internetworking services (including Router/boundary services) and Data Interchange formats & standards.

The e-GIF does not address policy in the form of specific standards profiles, however the standards identified in this policy are consistent with the e-GIF.

The NC3TA includes a minimum profile of standards with which this policy is wholly consistent.

Policy

Strategic
1018.01: Application layer services **1018.01.01** The following application layer service standards are mandated: **1018.01.01.01** SMTP IETF STD 10 (RFC 821:1982, 1869:1995, 1870:1995) – Interpersonal (email) messaging service   **1018.01.01.02** DNS IETF STD 13 (RFC 1034:1987, 1035:1987) - Name/Address resolution service   **1018.01.01.03** FTP, IETF STD 9 (RFC 959:1985) - File transfer service   **1018.01.01.04** HTTP v1.1 (RFC 2616), URL (RFC 1738), URI (RFC 2396) - Hypertext transfer service *Ubiquitous standards for the provision of these services with extensive cross-platform product support.* **1018.01.02** The following standard is mandated where bandwidth constraints apply and security rules permit: **1018.01.02.01** NNTP (RFC 977) - Bulletin board service (see comment)   *Ubiquitous standards for the provision of news services with cross-platform product support. Propagation of postings between servers across a network are more bandwidth-efficient than email.*   *Comment:* Many of the features of Network News can be achieved using email with properly managed address lists. This requires a separate mechanism and database for users to subscribe to mailing lists over and above the functionality of the email client. News group servers & clients include functionality to manage and maintain subscriber lists. NNTP, is however, becoming less popular as a service but can still perform a useful role within MOD. *Comment:* These standards provide the application layer services for the minimum standards profile. They include 'push', 'pull' and subscription services. **1018.02: Transport layer services** **1018.02.01** The following transport layer service standards are mandated: **1018.02.01.01** TCP (IETF STD 7)   **1018.02.01.02** UDP (IETF STD 6) *Comment:* The standard connection oriented and connectionless protocols used by the application layer services. **1018.03: Internetworking and routing services** **1018.03.01** The following internetworking service standards are mandated:

Strategic (continued)

1018.03.01.01 IPv4 (RFC 791, 792, 919, 922,1112)

1018.03.01.02 BGP4 (RFC 1771)

Comment: Boundary/advertised addresses must be valid public addresses (i.e. no private addresses to be routed across boundary)

1018.04: Data Interchange formats & standards

1018.04.01 Graphical Data Exchange - the following standards are mandated:

1018.04.01.01 SVG - Scalable Vector Graphics 1.0 Specification, W3C RECSVG-20010904:2001

1018.04.01.02 JPEG File Interchange Format v1.02 - Digital Compression and Coding of Continuous Tone Still Images, JPEG, ISO/IEC 10918:1994

1018.04.01.03 GIF, Version 89a, CompuServe gif89a:1990

1018.04.01.04 PNG Specification, Version 1.0, World W3C, 1 October 1996., IETF RFC 2083:1997

1018.04.02 Audio and Video Exchange - the following standards are mandated:

1018.04.02.01 MPEG1 - Coding of Moving Pictures and Associated Audio for Digital Storage Media at up to about 1.5 Mbit/s, ISO/IEC11172:1993

1018.04.02.02 MPEG2 - Generic Coding of Moving Pictures and Associated Audio, ISO/IEC 13818:2000

1018.04.02.03 MP3, see MPEG1 standard above)

1018.04.03 Document Exchange - the following standards are mandated:

1018.04.03.01 XML version 1.0 (Second Edition), W3C REC-xml-20001006:2000 - this standard is only mandated where meta-language data definitions are required

1018.04.03.02 HTML, Version 4.0.1, Reference Specification, W3C REC-html401-19991224:1999 (Dynamic HTML)

1018.04.03.03 PDF - Portable Document Format, Adobe Systems Incorporated, version 1.4, Adobe Systems Incorporated ISBN 0 200 175839 3:2003

1018.04.03.04 RTF, Microsoft Specification, Version 1.5, Microsoft Application Note GC0165:1997

1018.04.03.05 CSV - For spreadsheets

1018.04.03.06 ASCII Text

Strategic (continued)

1018.04.04 Enhanced Web Pages - the following standards are mandated:
 	
    1018.04.04.01 HTML, Version 4.0.1, Reference Specification, W3C REC-html401-19991224:1999 (Dynamic HTML)
 	
    1018.04.04.02 ECMAScript Language Specification, ECMA ECMA-262:1999
 	
1018.04.05 File Compression and Archiving - the following standards are mandated:
 	
    1018.04.05.01 Zip - DEFLATE Compressed Data Format Specification version 1.3, IETF RFC 1951:1996; GZIP file format specification version 4.3, IETF RFC 1952:1996 –
 	
1018.04.06 Character Sets and Alphabets - The following standards are mandated:
 	
    1018.04.06.01 7-bit Coded Character-set for Info Exchange (ASCII) (ISO 646:1991)
 	
    1018.04.06.02 8-Bit Single Byte Coded Graphic Character Sets, Parts 1-15, ISO/IEC 8859:1998
 	
    1018.04.06.03 UCS - Part 1 (ISO 10646-1-3:2000)
 	
1018.04.07 Dates and Times - the following standards are mandated:
 	
    1018.04.07.01 Representation of Dates and Times, ISO 8601:2000
 	
1018.04.08 Data Encoding for email attachments - the following standards are mandated:
 	
    1018.04.08.01 UUENCODE, The Open Group Unix98
 	
    1018.04.08.02 MIME - Part One: Format of Internet Message Bodies, IETF RFC 2045:1996; Part Two: Media Types, IETF RFC 2046:1996; Part Three: Message Header Extensions for Non-ASCII Text, IETF RFC 2047:1996; Part Four: Registration Procedures, IETF RFC 2048:1996; Part Five: Conformance Criteria and Examples, IETF RFC 2049:1996
 	
Comment: These standards will support the exchange of a wide variety of data types that can be exchanged using email (as attachments), downloaded from web pages (using HTTP) or directly transferred (using FTP).

Deployed
As for Strategic domain.

Tactical
Not applicable. *Comment:* Nothing is mandated in this domain; however it is recommended that where possible tactical systems should implement these standards. Although not mandated, the goals of interoperability and flexibility would be supported if systems in the tactical domain supported these standards, assuming security and bandwidth constraints permitted their use.

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 provide Local Area Network infrastructures.

Procedure

Not Applicable.

Relevant Links

JSP602: 1012 - Information Interchange

JSP602: 1013 – Internetworking

JSP602: 1016 - Messaging Services

JSP602: 1023 - Domain Naming and IP Addressing

JSP602: 1019 - MOD LAN to MOD LAN

JSP602: 1020 - MOD LAN to MOD WAN

JSP602: 1021 - MOD LAN/ WAN to External WAN

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

Details of IETF standards listed can be found here. (http://www.apps.ietf.org/rfc/stdlist.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 infrastructure 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.