JSP 602 Instruction	1010	**Applicability**	Applications, Infrastructure, Security
Configuration Identity	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-16	**Epoch Applicability**	2005 - 2009

JSP 602: 1010 - File Services

Outline

Description: File Services covers the standards and protocols that allow systems and/or services to access files stored on a remote storage devices, usually file servers, as though they were local to a system or service. This enables the provision of centrally managed data repositories to which multiple systems/services can gain access. Other policy relating to the data management and security of storage devices is contained in related JSP 602.

Reasons for Implementation: The purpose of this policy is to allow MOD CIS to access file stores on remote computers. The sharing of file and storage devices provides an important interoperability mechanism. File services enable systems to ’cross-mount’ or ’map’ remote file stores so that they appear to an application as a logical device that is local to the system or service.

Issues: File service protocols provide a richer functionality than other file sharing protocols such as FTP. However they are less secure and would not be allowed to pass through network security devices such as firewalls. They also tend to be less bandwidth efficient and less resilient than FTP.

Guidance: This policy is outside the scope of the e-GIF.

This policy is within the scope of the current NC3TA but the following caveats apply:

- No standards are mandated within the current NC3TA for distributed file services;

- XNFS (of which NFS is a part) is specified as an emerging standard for distributed file services.

Policy

Strategic

1010.01: File Store Remote Access

1010.01.01 All systems and/or services providing remote access to file storage devices shall do so using as a minimum the following standard:

> **1010.01.01.01** NFS: Network File System protocol specification (RFC 3010:1989)
>
> *A de facto network file server standard with cross-platform support that enables a computer to view, store and update files on a remote computer.*
>
> *Comment:* NFS is a client-server protocol, i.e. local systems require the NFS client application and servers require the NFS server application. When mounting remote file stores, NFS requires users to have an account on the remote machine. This policy does not preclude the provision of other protocols such as SMB. However, such proprietary protocols do not offer cross-platform support. To ensure data access across the GII cross-platform support is essential.

1010.02: Data Archiving

1010.02.01 Policy on Data Archiving is contained within JSP602: 1008 **-** Defence Data.

1010.03: Data Security

1010.03.01 Policy on Data Security is contained within JSP602: 1036 **-** Security Architecture.

Deployed

As for Strategic domain.

Tactical

1010.04: File Store Remote Access

1010.04.01 Remote access to file stores are actively discouraged due to bandwidth and security constraints. However where file stores need to be shared within a local area such as a Tactical HQ then the ’Strategic’ policy shall apply.

1010.05: Data Archiving

As for Strategic domain.

1010.06: Data Security

As for Strategic domain.

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 or use remote access to file storage services within the GII.

Procedure

The principal authority for this policy in the strategic environment is DII. For specific guidance on DII, MOD CIS Managers should contact the DII Integrated Design Team with all client and server configuration related queries. Point of Contact - DII IPT Engineering Management EM1Cons3: (D900, 5135MIN, 01793 555135).

Relevant Links

JSP602 1008 - Defence Data

JSP602: 1036 - Security Architecture

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