JSP 602 Instruction	1009	**Applicability**	Applications, Infrastructure, Network/Communications
Configuration Identity	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-21	**Epoch Applicability**	2005 - 2009

JSP 602: 1009 - Directory Services

Outline

Description: This policy leaflet covers the protocols, standards and formats that are necessary to provide end-to-end directory services across the GII. Electronic Directories are managed repositories of user and network resource-related information. They provide accurate and relevant information concerning the people and objects that are part of the organisation to enable Defence staff and their partners to work effectively.

Reasons for Implementation: Directories are essential enablers, making it possible to refer to information that would otherwise be difficult to locate, even by other electronic means, because of the sheer volume available and the lack of time for extensive searches. A Metadirectory aggregates selected data items currently held in multiple other directories to hold only a single instance of each data item. This aggregated data can be merged, manipulated, accessed and, if appropriate, promulgated back out to the user community in a variety of ways.

Issues: None.

Guidance: All systems and/or projects providing directory services within the GII should follow the guidance given in JSP 457 Volume 4 for the development, maintenance and operation of MOD systems holding naming and/or addressing information; they should also consult CDMA/DDR for all data definition enquiries.

This policy is consistent with the NC3TA.

This policy is consistent with the e-GIF.

Policy

Strategic

1009.01: Directory Services and Structure

1009.01.01 The following standard(s) are mandated for all systems and/or projects providing directory services within the GII:

1009.01.01.01 x.500 (RFC2256)

This is the de facto standard for directory services and structure.

1009.02: Directory Access

1009.02.01 The following standard(s) are mandated on all systems and/or projects providing access to directory services within the GII:

1009.02.01.01 LDAP v3 (RFC3377)

This is the de facto standard with extensive product support. It provides methods for both directory access and user authentication. It also provides a mechanism for querying and modifying information that resides within a DIT.

1009.03: Directory Replication and Interfacing

1009.03.01 The following standard(s) are mandated on all systems and/or projects providing directory replication and interfacing services within the GII:

1009.03.01.01 LDIF (RFC2849)

1009.03.01.02 CSV standard file format

Comment: There is no specific reference for the CSV file format. However, it is widely supported. CSV files are standard text files where fields are separated by commas and each line of text represents a single record

These are de facto standards with extensive product support for interfacing and replicating directories.

1009.04: Directory Service Management

1009.04.01 All systems and/or projects providing directory services within the GII shall provide the following minimum set of management processes:

1009.04.01.01 Grafting (where a branch of one directory tree is grafted onto a branch of another directory tree)

1009.04.01.02 Entity relocation

1009.04.01.03 Repair

1009.04.01.04 Attribute and Object Creation

These are standard management processes that are necessary to deploy a MOD-wide directory service.

Strategic (continued)

1009.05: Naming Conventions

1009.05.01 All systems and/or projects providing directory services shall support naming conventions as specified in the following standards:

1009.05.01.01 JSP 457 - The Defence Manual Of Interoperable Network and Enabling Services, Volume 4 Electronic Directory services

Comment: JSP 457 contains naming standards for directories and messaging, specifically Electronic Unit Names (EUNs) and other unique identifiers. Object identifiers are globally unique numeric values that are granted by various issuing authorities to identify data elements, syntaxes, and other parts of distributed applications. They ensure that the objects do not conflict with one another when, for example, different directories, such as Active Directory and Novell e-Directory, are brought together in a global directory namespace. Object identifiers are based on a tree structure in which a superior issuing authority allocates a branch of the tree to a subordinate authority, which in turn allocates sub-branches of the tree.

1009.05.01.02 IETF naming conventions

1009.05.01.03 ISO naming conventions

1009.05.01.04 ISO/IEC 8824-1:2002/FDAmd 2 - Alignment with changes made to ITU-T Rec.X.660 — ISO/IEC 9834-1 for identifiers in object identifier value notation

This is necessary to support both Internet and x.500 naming conventions.

1009.06: Directory Distribution

1009.06.01 All systems and/or projects providing part of the MOD's overall distributed Directory Information Tree shall ensure that the following attributes can be achieved:

1009.06.01.01 Be capable of being partitioned

1009.06.01.02 Be capable of mirroring

1009.06.01.04 Permit any partition to operate autonomously from the parent for all of its child entities

1009.06.01.05 Be capable of providing filtered views

1009.06.01.06 Be capable of supporting schema extensions by object and object attributes - those extensions applying to all instances of that object type within a given instance of the schema

1009.06.01.07 Provide a managed replication service between disparate elements of the DS, controlling frequency, priority and replicating only those elements that have changed

1009.06.01.08 Replicate and synchronise in accordance with the following standards:

1009.06.01.08.01 RFC 1275 Replication Requirements to provide an Internet Directory
using X.500

Strategic (continued)

1009.06.01.08.02 RFC 1276 Replication and Distributed Operations extensions to provide an Internet Directory using X.500

1009.06.01.08.03 RFC 3384 Lightweight Directory Access Protocol(version 3)Replication Requirements

1009.06.01.09 Support chaining and replication by the use of zone transfers between directories (vendor independent)

1009.06.01.10 Be capable of accepting different crypto keys

These features and attributes are necessary to provide a MOD-wide heterogeneous Directory Information Tree.

1009.07: Directory Schema

1009.07.01 All systems and/or projects providing part of the MOD's overall distributed Directory Information Tree shall implement the schema as defined in the following standards:

1009.07.01.01 ACP 133 - Common Directory Services and Procedures

1009.07.01.02 UK Defence Mandatory Core Schema - latest version and references to the current standards upon which it is based at http://www.dinsa.r.mil.uk/directories.htm (RLI only).

These are the nationally and internationally adopted standards.

Comment: ACP133 defines the directory services, architecture, protocols, schema, policies and procedures to support messaging communications between allied nations, including NATO and the CCEB. Due to the fact that the UK Defence Mandatory Core Schema evolves more quickly than JSP 457 is updated, implementers of new directories are directed to the DNAA intranet web site.

1009.08: Voice Numbering Scheme

1009.08.01 All systems and/or projects providing secure and/or insecure telephone services shall implement the following numbering scheme standards:

1009.08.01.01 STANAG 4214 – NIAC

1009.08.01.02 STANAG 5046 – NDD

There is currently no international standard for access (std or area) codes. This is currently a NATO-only standard.

Comment: DCSA DINSA is drafting a volume of JSP 457 entitled Volume 8 - Circuit Switched Numbering; this will include chapters on NIAC and NDD.

1009.09: Voice Registration

1009.09.01 All systems and/or projects providing secure and/or insecure telephone services shall implement registration in accordance with the following standards:

1009.09.01.01 ITU-T H.323

Strategic (continued)

1009.09.01.02 SIP (RFC 3261)

Deployed

As for Strategic domain.

Tactical

1009.10: Directory Services and Structure

As for Strategic domain.

1009.11: Directory Access

1009.11.01 The following standard(s) are mandated on all systems and/or projects providing access to directory services within the GII:

1009.11.01.01 LDAP v3 (RFC3377) supported at boundary

Within tactical systems such as CIP (hosted on Bowman) any implementation of a directory service is likely to be bespoke because of bandwidth and other communications constraints. However, at their boundary tactical systems must support the de facto standard.

1009.12: Directory Replication and Interfacing

As for Strategic domain.

1009.13: Directory Schema

As for Strategic domain.

Remote

1009.14: Directory Services and Structure

As for Strategic domain.

1009.15: Directory Access

As for Strategic domain.

1009.16: Directory Replication and Interfacing

As for Strategic domain.

1009.17: Directory Service Management

As for Strategic domain.

1009.18: Naming Conventions

As for Strategic domain.

1009.19: Directory Distribution

As for Strategic domain.

Remote (continued)

1009.20: Directory Schema
As for Strategic domain.

1009.21: Voice Numbering Scheme
1009.21.01 To support remote users dialling-in to the MOD telephone system. any gateway between MOD and civilian telephone systems shall support the following numbering scheme standards:

1009.21.01.01 STANAG 4214 – NIAC

1009.21.01.02 STANAG 5046 – NDD

1009.22: Voice Registration
1009.22.01 To support remote users dialing-in to the MOD telephone system. any gateway between MOD and civilian telephone systems shall support registration in accordance with the following standards:

1009.22.01.01 PSTN-SIP Gateway (RFC 3372)

Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all IPTs (and their suppliers) that provide any components of the MOD-wide directory service.

Procedure

Before embarking on implementation of a directory schema, the following organisations must be contacted for advice:-

- In the first instance, DCSA DII EM1c Neil Bedford (dcsadii-em1c@mod.uk)
- DG Info CDMA
- DCSA DINSA

The DII IPT is responsible for providing Directory Services for all CIS in the Strategic, Deployed and Remote domains.

Enquiries as to the maintaining and updating of JSP457 and ACP133 should go to DCSA CMDINSA Hd.

Relevant Links

JSP602: 1014 – Legislation

JSP457 The Defence Manual Of Interoperable Network and Enabling Services can be found here (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)

ACP133 can be found here. (http://www.dtic.mil/jcs/j6/cceb/acps/)

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. Evidence of conformance with Directory Management and Distribution attributes must also be presented so that they can be confirmed as being compatible with the Directory Services provided by the principal provider of Directory Services within the applicable domain.