Allied Data Publication 34

(ADatP-34)

NATO Interoperability Standards and Profiles

Volume 2

Near Term

Version 2.0

Date: 7 February 2008

C3 CCSC NATO Open Systems Working Group

Table of Contents

1. Introduction 1
1.1. Scope 1
2. Reference Models: Transition from Platform Centric to Service Oriented Models 3
3. Standards 5
3.1. Introduction 5
3.2. NNEC Application Services 5
3.3. COI Services 6
3.4. NNEC Core Enterprise Services 8
3.4.1. Basic Infrastructure Services 8
3.4.2. Business Service Enablers 9
3.4.3. List of Standards 10
3.5. Networking Information Infrastructure Services 58
4. Interoperability Profiles 85
4.1. Minimum Interoperability profile 85
4.1.1. Architectural Assumptions 85
4.1.2. Shared Services 86
4.1.3. Minimum Architecture 86
4.2. X-TMS-SMTP profile 89
4.3. TACOMS Post-2000 Profile 92
A. Technologies 95
A.1. Data Strategy 95
A.1.1. Data Management Strategy 95
A.1.2. JC3IEDM 96
A.1.3. NATO Discovery Metadata Specification (NDMS) 96
A.1.4. Extensible -up Language (XML) 97
A.2. Information Modelling 98
A.3. Network Infrastructure 99
A.3.1. Background 99
A.3.2. NGCS 2007 Target Architecture 99
A.3.3. Communications & Networking 100
A.3.4. Construction of a robust IP-network infrastructure 103
A.4. Platform Oriented Computing 106
A.4.1. User Terminal/Device 106
A.4.2. User Workstation 107
A.4.3. Administration Workstation 109
A.4.4. Network Server 109
A.4.5. Communications and Messaging Server 110
A.4.6. Document Management Server 111
A.4.7. Web Portal/Application Server 112
A.4.8. Database Application Server 113
A.4.9. Directory Server 114
A.4.10. Imagery Server 115
Index 117

1. INTRODUCTION

001. Volume 2 of the NISP focuses on interoperability standards and profiles in the near-term or a timeframe of 0 to 2 years into the future. This is the short-term step describing the state-of-the-art of NATO systems today and the framework for new systems actually under procurement or specification. For new systems, it describes the initial step towards the NII.

002. The Combined Communications Electronics Board (CCEB) nations will use NISP Volume 2 Chapter 4 tables to publish the interoperability standards for the CCEB under the provisions of the NATO-CCEB List of Understandings (LoU) detailed in Volume 1 Annex B. Sections 1, 2 and 3 of this volume are background information only for the CCEB. Chapter 4 are applicable to the non NATO CCEB Nations when taking part in NATO lead operations.

1.1. SCOPE

003. The scope of this volume will include:

- Identifying the reference models, standards, profiles, and technologies that are relevant to the platform centric environment,
- Describing the near term Standards, profiles and technologies to support the initial step towards NII,
- Planning the transition of legacy systems.

2. REFERENCE MODELS: TRANSITION FROM PLATFORM CENTRIC TO SERVICE ORIENTED MODELS

004. Information technology is undergoing a fundamental shift from platform-oriented computing to network-oriented computing. Platform-oriented computing emerged with the widespread proliferation of personal computers and the global business environment. These factors and related technologies have created the conditions for the emergence of network-oriented computing. This shift from platform to network is what enables the more flexible and more dynamic network-oriented operation. The shift from viewing partners as independent to viewing partners as part of a continuously adapting ecosystem fosters a rich information sharing environment.

005. This shift is most obvious in the explosive growth of the internet, intranets, and extranets. Internet users no doubt will recognize transmission control protocol/internet protocol (TCP/IP), hypertext transfer protocol (HTTP), hypertext markup language (HTML), Web browsers, search engines, and Java[1] Computing. These technologies, combined with high-volume, high-speed data access (enabled by the low-cost laser) and technologies for high-speed data networking (hubs and routers) have led to the emergence of network-oriented computing. Information "content" now can be created, distributed, and easily exploited across the extremely heterogeneous global computing environment. The "power" or "payoff" of network-enabled computing comes from information-intensive interactions between very large numbers of heterogeneous computational nodes in the network, where the network becomes the dynamic information grid established by interconnecting partners participating in a collaborative, coalition environment. At the structural level, network-enabled warfare requires an operational architecture to enable the common processes to be shared by all parties.

006. One of the major drivers for supporting net-enabled operations is Service-Oriented Architectures (SOA). SOA is enterprise architecture that leverages heterogeneity, and thus inherently platform-neutral. It is focused on the composition of Services into flexible processes and is more concerned with the Service interface and above (including composition metadata, security policy, and dynamic binding information), more so than what sits beneath the abstraction of the Service interface. SOA requires a different kind of platform, because runtime execution has different meanings within SOA. SOA enables business users and business process architects to compose Services into processes, and then manage and evolve those processes, in a declarative fashion. Runtime execution of such processes is therefore a metadata-centric operation of a different kind of platform -- a Service-oriented composite application platform.

007. Network-enabled operations are characterized by new concepts of speed of command and self-synchronization.

008. The most important SOA within an enterprise is the one that links all its systems. Existing platforms can be wrapped or extended in order to participate in a wider SOA environment.

[1]Registered Trademark of SUN Microsystems, INC.

NATO use of the NISP will provide a template for new systems development, as well as assist in defining the path for existing systems to migrate towards net-enabled operations.

3. STANDARDS

3.1. INTRODUCTION

009. This purpose of this chapter is to specify the NISP near term standards. Based on the NNEC FS, the document organises these standards into four service areas and included service categories:

- NNEC Application Services (NAS)
- COI Services (COI)
- NNEC Core Enterprise Services (CES)
  - Discovery (DIS)
  - Information Assurance (IAS)
  - Messaging (MES)
  - Enterprise Services Management (ESM)
  - Storage (STO)
  - Application (APP)
  - Mediation (MED)
  - Collaboration (COL)
  - User Assistant (UAS)
- Networking Information Infrastructure Services (NIIS)

010. This section describes the role and requirements of each service area, and presents all associated standards in tabular form. The tables refine each service area into one or more service categories, with service components mapping to one or more mandatory, emerging near term, fading or retired standards categories (see NISP vol. 1). A remarks column provides optional supplementary information on each standard plus CCEB-specific information. The NISP Rationale Document (RD) provides further explanation on why service and standards categories have been selected.

3.2. NNEC APPLICATION SERVICES

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC APPLICATION SERVICES					
Communication Services / Application Layer					

3.3. COI SERVICES

011. COI services provide more specialized services in order to give the business more specific business benefits within a "domain" or "area of interest".

012. A COI is a collaborative group of users who have shared goals, interests, missions or business processes that result in information exchange and shared vocabulary.

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC VALUE ADDED SERVICES / COMMUNITY OF INTEREST SERVICES (COI)					
Communicate and Inform					
Battlespace Mgmt					
Orbat Mgmt					
Overlay Mgmt					
Symbol Mgmt					
Tracking					
		NFFI, STANAG 5527 (study)			Until the development of STANAG 5527 is more stable, document AC/322(SC/5)N(2006)0025 should be used.

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC VALUE ADDED SERVICES / COMMUNITY OF INTEREST SERVICES (COI)					
					For CCEB in-teroperability this standard is not applicable.
Synchronisa-tion					
Distribution					
Notification					
Aggregation					
Collaborate and Plan					
Plan Work-space					
Plan Analysis					
Plan Briefing					
Plan Replay					
Plan Synchron-isation					
Plan Collabora-tion					
Simulation					
Collaboration analysis					
Sense and Re-spond					
Tasking					
Plan Deviation Monitor					
General					
Meteo					
Map View					
Map Mgmt					
Spatial Geo-					

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC VALUE ADDED SERVICES / COMMUNITY OF INTEREST SERVICES (COI)					
graphy Visual-isation					
JCOP					

3.4. NNEC CORE ENTERPRISE SERVICES

013. Core services provide fundamental support to service based frameworks both in the form of infrastructure and enabler services, and in the form of COI independent general service building blocks.

014. Core services includes services that are either made available to all users by the infra-structure, or are mandatory to be provided by all users, by all providers or by all consumers. Core services also include specification of services of general interest that may be voluntarily exchanged by any parties on the network

015. Any service based framework, such as the Business Process Infrastructure Framework (BPIF), needs to provide a basic set of services that support and facilitate implementation and deployment of actual business services and processes. Such basic services are usually referred to as Core services.

016. Here we will provide an overview of such Core Services in a BPIF context in terms of the way such services are categorized. A few examples of core services in each category is also provided, but a complete set of well defined core services cannot be provided as it to a large extent will depend on the actual implementation of the BPIF.

017. Core services in a BPIF context are divided into two main categories according to their primary role in the implementation of business services and processes.

3.4.1. Basic Infrastructure Services

018. The first main category of core services, here referred to as Basic Infrastructure Services (BIS), are used to support the infrastructure (BPIF) that support deployment, operation and management of business processes. BIS is further divided into three subcategories according to three of the main aspects of a BPIF.

- Service Selection BIS are concerned with the basic mechanisms for discovery and visibility of services. Typically this encompasses basic service directories with support for syntactic description and lookup of services.

- Management and operation BIS are concerned with various types of management and operation of services and infrastructure. There are at least four subcategories.
  - BIS handling policies, including required security level, conditions for service delivery, availability, quality of service undertakings etc.
  - Security BIS include basic functions for managing information security, and a typical example is a service that keeps track of role and person oriented authorization, distribution of keys, handling of certificates etc.
  - Service Management BIS handle life cycle management of other services, including for example monitoring and configuration.
  - Resource Management BIS are used to manage infrastructure resources and will be highly dependent on infrastructure implementation. A typical example is resource management in a Grid.
  - Network Management BIS are concerned with networking and communication aspects of the infrastructure, and involve for example router configuration.
- Process Composition BIS are concerned with support for business processes.

3.4.2. Business Service Enablers

019. The second of the main core service categories is Business Service Enablers (BSE). While BIS services are concerned with the BPIF infrastructure per se, they are not used a foundation for implementation of business services. This is instead the role of BSE, which provide basic functionality that is shared by many business services independently of Community of Interest (COI).

020. BSE are divided into three main subcategories based on the types of functionality they offer.

- Collaboration BSE support basic exchange of data between services. Examples include message passing (uni- and multicast, email, etc.), distributed file sharing, publication (web pages etc.), and data format conversion.
- Synchronization BSE support synchronization of service and process interaction, and includes for example time services, and event notification.
- Common Information Services (CIS) is the third and last subcategory of BSE. CIS provide COI-independent support for access to general information like maps, glossaries, standards, and document registries.

021. Note: Not all functions in this category are necessarily service oriented in a SOA sense.

They are nevertheless important for a network-oriented capability.

3.4.3. List of Standards

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
Discovery (DIS)					
Service Catalogue/Subscriber/Publisher					
Information Catalogue/Subscriber/Publisher					
Information Assurance (IAS)					
	Common Criteria (ISO/IEC 15408-1to-3:2005)			**Security**	Procedural document dealing with the evaluation criteria for IT security.
	Radius, IETF RFC 2865:2000 updated by RFC 2868:2000, 3575:2003	Radius and IPv6, IETF RFC 3162:2001		**Security**	
	Virtual Router Redundancy Protocol (VRRP), IETF RFC 3768:2004			**Security**	
		Single sign on (SSO, the Open Group)		**Security**	

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	Dir Authentication Framework (ITU-T X.509 v3, ISO 9594:2001)			**Security**	
					For CCEB interoperability the standard is S/MIME Version 3 ESS, application layer data confidentiality or link level encryption
	Key Wrap Advanced Encryption Standard 128 (AES 128, NIST FIPS 197)	Key Wrap Advanced Encryption Standard 256 (AES 256, NIST FIPS 197)		**Security**	PKI components and applications should utilise AES for key wrap functions. AES 256 should be utilized post 2008 for Root CA and Sub CA PKI components together with SHA-384 and 512. End entities can still utilize AES 128 together with SHA-256. For CCEB interoperability the AES standard is emerging.

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	TLS (IETF RFC 4346:2006 updated by RFC 4366:2006, 4680:2006, 4681:2006)		SSL excluded in NCSP v.6	**Security**	Used as a transport layer security protocol.
	IP ESP (RFC 2412:1998 updated by RFC 3168:2001, 4301:2005)			**Security**	Encapsulating Security Payload (ESP) may support integrity and authentication depending on the use of algorithms
					For CCEB interoperability the standard is S/MIME Version 3 ESS, application layer digital signatures or link level encryption
	Digital Signature Algorithm 1024 (DSA-1024, NIST FIPS 186-2 with Change Notice 1, Oct 2001)	Elliptic Curve Digital Signature Algorithm (ECDSA 384, NIST FIPS 186-2 with Change Notice 1, Oct 2001)	Digital Signature Algorithm (original version) not for new systems	**Security**	Authentication and integrity algorithm for ?End Entities? as mandated by the interoperability protocol PCT for implementing digital signatures for a NATO Public Key Infrastructure (PKI) in the NATO mes-

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					saging system. ECDSA 384 is planned for post 2008. Guidance is provided in AC/ 322-D(2004)0035. For CCEB interoperability the Digital Signature Algorithm (DSA) NIST FIPS 186-2 is mandatory. DSA FIPS 186-2 can be used in NATO for verification purposes only.
	RSA 2048 (PKCS#1 v2.1 RSA Cryptography Standard, RSA Laboratories, June 2002)	Elliptic Curve Digital Signature Algorithm (ECDSA 384, NIST FIPS 186-2 with Change Notice 1, Oct 2001)		**Security**	Authentication and integrity algorithm for ?Sub CA and other PKI components (such as Key Recovery Agents)? as mandated by the interoperability protocol PCT for implementing digital signatures for a NATO Public Key Infrastructure (PKI) in the NATO mes-

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					saging system. ECDSA 384 is planned for post 2008. Guidance is provided in AC/ 322-D(2004)00 35. For CCEB in-teroperability the Digital Sig-nature Al-gorithm (DSA) NIST FIPS 186-2 is man-datory.
	Secure Hash Algorithm 256 (SHA-256, NIST FIPS 180-2 with Change Notice 1, Feb 2004)	Secure Hash Algorithm 384 (SHA-384, NIST FIPS 180-2 with Change Notice 1, Feb 2004)	Secure Hash Algorithm (SHA-1), NIST FIPS 180-1 replaced by SHA-256	**Security**	Hash algorithm to accompany the DSA and RSA for use in NMS. SHA-384 is planned for post 2008. Guidance is provided in AC/ 322-D(2004)00 35. For CCEB in-teroperability the standard is SHA-1, NIST FIPS 180-1 is mandatory. SHA-1 can be used in NATO for verification purposes only.

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	Physical characteristics (ISO/IEC 7810:2003)			**Security**	
	Identification of Issuers (ISO 7812:2007)			**Security**	
	Integrated circuit(s) with electrical contacts (ISO/IEC 7816:2006)			**Security**	
	Interface between the card aware applications and cards, PC/SC Specs. 1.0			**Security**	
	Card-resistance allications, JAVACard			**Security**	
	Contactless cards (ISO/IEC 14443:2001)			**Security**	
					For CCEB interoperability the Security Ascertion Markup Language (SAML) v1.1 is mandatory
	S/MIME with Encrypted Security Service (ESS) (IETF RFCs		ACP120 replaced by ACP145	**Security**	Messaging System independent encapsulation syntax supporting signa-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	3850:2004, 3851:2004)				ture and confidentiality functions based on DSA. For CCEB interoperability the mandatory standard is ACP145 (Gateway-to-Gateway Messaging Protocols)
	STANAG 4406 Ed.2		ACP120 replaced by ACP145	**Security**	This includes PCT (protected content type). PCT may be used for protection of data objects in systems. For CCEB interoperability the mandatory standard is ACP145 (Gateway-to-Gateway Messaging Protocols)
					See General Security Key Management and Distribution. For CCEB interoperability the mandatory

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					standard is ACP145 (Gateway-to-Gateway Messaging Protocols) and X.500 (based on CMI authentication framework)
					For CCEB interoperability the mandatory standard is ACP145 (Gateway-to-Gateway Messaging Protocols) (based on digital signatures within the CMI authentication framework and associated PKI)
					For CCEB interoperability the mandatory standard is ACP145 (Gateway-to-Gateway Messaging Protocols) (based on digital signatures within the CMI authentication framework and associated PKI)
		X.411:1999		**Security**	

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					For CCEB interoperability the mandatory standard is ACP145 (Gateway-to-Gateway Messaging Protocols) (based on digitally signed receipts and PKI)
Accessability					
Confidentiality					
Availability					
Managebility					
Integrity					
Auditing					
Single-Sign On					
Non-Repudiation					
Intrusion Detection					
Malicious Code Detection					
Time Stamping					
Messaging (MES)					
Messaging					
	STANAG 4406 Ed.2		Use of PCT within STANAG 4406 is fading	**Comms**	Used for Formal Messaging. STANAG 4406 contains the upper layer protocol profile down to the requested Trans-

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					port Service. For CCEB in-teroperability the mandatory standard is ACP123A.
		STANAG 4631		**Comms**	STANAG 4631 contains an ad-ditional S/ MIME profile for MMMHS (in addition to PCT) For CCEB in-teroperability the mandatory standard is ACP123A.
	SMTP (IETF RFCs 1870:1995, 1985:1996, 2034:1996, 2554:1999, 2821:2001, 2920:2000, 3207:2002, 3461:2003 up-dated by 3798:2004, 3885:2004)			**Comms**	Used for inter-personal mes-saging (email)
	POP3 (IETF RFC 1939:1996 up-dated by 1957:1996, 2449:1998)			**Comms**	For CCEB in-teroperability this standard is not applicable
	IMAP4 (IETF			**Comms**	For CCEB in-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	RFC 3501:2003 updated by 4466:2006, 4469:2006, 4551:2006)				teroperability this standard is not applicable
Mail Gateway					
		ACP 145		**Comms**	Provides gateway between ACP 123A messaging services. For CCEB interoperability this standard is mandatory
Streaming Video					
Fax GW					
Mail					
Streaming Video					
Instant messaging					
		XMPP (IETF RFC 3920:2004 - 3923:2004)			For CCEB interoperability this standard is mandatory
Voice GW					
Video GW					
Telex GW					
Enterprise message bus					
Voice and Video conferencing					

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	Packet-based Multimedia Comms Sys-tem (ITU-T H.323:2006)			**Comms**	
	Multinational Videoconfer-encing Ser-vices (ACP 220:2003)			**Comms**	
	Circuit-based Multimedia Comms Sys-tem (ITU-T H.320:2004)			**Comms**	
	Media Gate-way Control Protocol v3(ITU-T H.248.1:2005)			**Comms**	Protocol for managing the multi-media gateways between circuit switched and packet switched networks.
	ITU Multi-point still im-age and An-notation Con-ference Pro-tocol Spec (ITU-T T.120:2006), T.126:1997 (Reference to T.122 - T.125)			**Comms**	
	Data Protocols for Multime-dia Conferen-cing (ITU-T T.120:2006, T.128:1998)			**Comms**	

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
Management					
Enterprise Service Management (ESM)					
					Same standards as within LAN Management for SNMP For CCEB interoperability this standard is not applicable
	SNMPv3 Applications (IETF RFC 3413:2002)		SNMPv1 (IETF Std 15) not for new systems	**Mgmt.**	SNMPv3 is considered emerging because of current lack of agreement on the concept of operations for distributed management For CCEB interoperability this standard is not applicable
	Message Processing and Dispatching for the SNMP (RFC 3412:2002)			**Mgmt.**	For CCEB interoperability this standard is not applicable
	User-based Security Model (USM) for SNMPv3			**Mgmt.**	For CCEB interoperability this standard is not applicable

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	(RFC 3414:2002)				
	View-based Access Con-trol Model (VACM) for the SNMP (RFC 3415:2002)			**Mgmt.**	For CCEB in-teroperability this standard is not applicable
	Structure of Mgt Info (IETF Std 16:1990, IETF RFC 1155:1990 and 1212:1991)			**Mgmt.**	For CCEB in-teroperability this standard is not applicable
	Architecture for SNMP Mgt Frameworks (RFC 3411:2002)			**Mgmt.**	For CCEB in-teroperability this standard is not applicable
	MIB II (IETF Std 17:1991, RFC 1213:1991 up-dated by 4293:2006, 4022:2005, 4113:2005)			**Mgmt.**	For CCEB in-teroperability this standard is not applicable
		IPv6 MIB (IETF RFC 4293:2006)		**Mgmt.**	For CCEB in-teroperability this standard is not applicable
		ICMPv6 MIB (IETF RFC 4293:2006)		**Mgmt.**	For CCEB in-teroperability this standard is not applicable
		IPv6 MIB for MLD (IETF		**Mgmt.**	For CCEB in-teroperability

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
		RFC 3019:2001)			this standard is not applicable
		IPv6 MIB for TCP (IETF RFC 4022:2005)		**Mgmt.**	For CCEB in-teroperability this standard is not applicable
		IPv6 MIB for UDP (IETF RFC 4113:2005)		**Mgmt.**	For CCEB in-teroperability this standard is not applicable
	Host Re-sources MIB (IETF RFC 2790:2000)			**Mgmt.**	For CCEB in-teroperability this standard is not applicable
	Defs of Mgt Objects for the Ethernet-like Interface types (IETF RFC 2666:1999, 3635:2003, 3638:2003)			**Mgmt.**	For CCEB in-teroperability this standard is not applicable
	RMON MIB v. 1 (RFC 2819:2000)	RMON 2 MIB (RFC 4502:2006)		**Mgmt.**	For CCEB in-teroperability this standard is not applicable
	OSPF MIB v.2 (RFC 1850:1995)			**Mgmt.**	For CCEB in-teroperability this standard is not applicable
	RIP-2 MIB (RFC 1724:1994)			**Mgmt.**	For CCEB in-teroperability this standard is not applicable
					In addition same standards as within LAN Management for SNMP can

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					be used Quad C used for man-agement of co-alition WANs
		Common In-formation Model (CIM)	CMIS (ISO 9595:1998) deleted in NISP v.1	**Mgmt.**	For CCEB in-teroperability this standard is not applicable
Mgmt Info Publisher					
Mgmt Info Subscriber					
Mgmt Info Col-lector					
Mgmt Info Pro-vider					
Asset Mgmt					
User Mgmt					
Storage (STO)					
Storage					
Storage Access					
Storage Mgmt Provider					
Information Object Envir-onment					
Distributed Storage					
Centraliced Storage					
Structured Stor-age					
Unstructured Storage					
Application (APP)					

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
Service Runtime Envir-onment					
Service In-staller / Unin-staller					
Snapshot Pro-vider					
Browser					
Application					
	ACP 133B	ACP 133C	ACP 133B not to be used for new systems	**Comms**	Contains schema.ACP 133B contains the upper layer protocol profile down to the re-quested Trans-port Service
	DAP (ITU-T X.500:2005)		DAP not to be used for new systems	**Comms**	DAP is in the X.500 access protocol. For CCEB in-teroperability this standard is not applicable
	LDAP v3 (IETF RFC 4510:2006, 4511:2006, 4512:2006, 4513:2006)			**Comms**	LDAP is an IETF protocol and close to a functional sub-set of DAP. Many Web-browsers can act as LDAP clients, which is highly desir-able.
	LDIF (IETF RFC			**Comms**	LDIF defines a flexible and al-

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	2849:2000)				most universally accepted means of exchanging directory information via flat files.
	DSP (ITU-T X.500:2005)		DSP not to be used in new systems	**Comms**	DSP defines X.500 server to server communication, including chaining. For CCEB interoperability this standard is not applicable
	DISP (ITU-T X.500:2005)		DSIP not to be used in new systems	**Comms**	DISP defines X.500 based information shadowing/replication. For CCEB interoperability this standard is not applicable
		DOP (ITU-T X.500:2005)	DOP not to be used in new systems	**Comms**	Contains operational management. For CCEB interoperability this standard is not applicable
	FTP (IETF STD 9:1985,IETF RFC			**Comms**	

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	0959:1985 updated by RFC 2228:1997, 2640:1999, 2773:2000, 3659:2007)				
		FTP Extensions for IPv6 and NATs (IETF RFC 2428:1998)		**Comms**	
	Telnet (IETF STD 8:1983, IETF RFC 0854:1983, 0855:1983)			**Comms**	
	HTTP v. 1.1 (IETF RFC 2616:1999 updated by RFC 2817:2000), URL (RFC 4248:2005, 4266:2005), URI (RFC 3986:2005)			**Comms**	
	Network News Transfer Protocol NNTP (IETF RFC 3977:2006)			**Comms**	
	Network Time Protocol (NTP)(RFC 1305:1992)			**Comms**	
	MPEG-1 (ISO/IEC 11172:1993)		MPEG-1 not to be used for new systems	**Data Interchange**	
	MPEG-2			**Data In-**	

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	(ISO/IEC 13818:2000)			**terchange**	
	MPEG-4 (ISO/IEC 14496:2004)			**Data In-terchange**	Encoding standard for video conferen-cing
	Compact Disc File System (CDFS) (ISO 9660:1988)			**Data In-terchange**	For physical media distribu-tion (CD)
	Pulse Code Modulation (PCM) (ISO/IEC 11172-3:1993, ITU-T G.711:1988)			**Data In-terchange**	PCM used for audio in ISDN Systems
	Differential PCM (ITU-T G.726:1990)			**Data In-terchange**	
	Delta-Modulation DM, EURO-COM D/0		DM not to be used for new systems	**Data In-terchange**	
	GSM-Modulation (GSM 06.10, GSM 06.20)			**Data In-terchange**	Used for mo-bile phones
	Voice Coding Algorithm (STANAG 4444 ed.1).			**Data In-terchange**	Used for HF voice commu-nications as defined in STANAG 4444.
	Linear Predict-ive Coding-10 (STANAG 4198 ed.1:1984)		LPC-10 not to be used for new systems	**Data In-terchange**	

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	Code Excited Linear Prediction coding (CELP) (FS 1016:1991)			**Data Interchange**	CELP is used military aircraft voice communications in narrow band UHF networks. CELP has higher throughput than LPC-10, but a lower range.
		Mixed Excitation Linear Predictive coding (MELP) (STANAG 4591 ed.1)		**Data Interchange**	MELP is used for HF voice communications in narrow band systems.
	Parameters and Coding Standards for 800 bps. Digital Speech Encoder/Decoder (STANAG 4479 ed.1:2002)			**Data Interchange**	For CCEB interoperability this standard is not applicable
	SIMPLE (STANAG 5602 ed.2)			**Data Interchange**	SIMPLE provides specifications to interconnect ground rigs of all types for TDL interoperability testing
	Nato Secondary Imagery Format (NSIF), STANAG			**Data Interchange**	NSIF establishes the format for exchange of electronic second-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	4545 ed 1.:1998				ary imagery
	BIIF (ISO 12087-5:1998)			**Data Interchange**	
	NSILI (STANAG 4559 ed.1:2003)	NSILI (STANAG 4559 ed.2)		**Data Interchange**	NSILI provides interoperability between NATO nations reconnaissance databases and product libraries
	NADS (STANAG 4575 ed.2)			**Data Interchange**	NADS defines an interface for advanced digital storage systems.
	GMTIF (STANAG 4607 ed.1:2005)				GMTIF defines a ground moving target indicator format.
	DMIS (STANAG 4609 ed.1:2005; ed.2:2007)				DMIS defines a digital motion imagery standard. For CCEB interoperability this standard is not applicable.
	NPIF (STANAG 7023 ed.3:2004)	NPIF (STANAG 7023 ed.4)		**Data Interchange**	NPIF establishes a standard data format and a standard transport architecture for the transfer of reconnaissance and surveillance imagery

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					and associated auxiliary
	AR-TRI (STANAG 7024 ed.2:2001)			**Data In-terchange**	AR-TRI estab-lishes the phys-ical format for the exchange of magnetic tape cartridges
	Exchange of Imagery (STANAG 3764 ed.4:2002)	Exchange of Imagery (STANAG 3764 ed.5)		**Data In-terchange**	
	Implementing JPEG 2000 in NITFS/ BIIF/NSIF (SC24 ISO Registered Profile)			**Data In-terchange**	This profile defines the lim-its of the inter-national stand-ard that can be used within NITF 2.1.
	Link-11 (STANAG 5511 ed.5, M-Series)			**Data In-terchange**	For further guidance refer to the Data Link Migration Strategy, MNCs SACLANT 3000 C-03/Ser: NU0606, Sept 1998. For CCEB in-teroperability the standard is MIL-STD 6011C
	Link-16 (STANAG 5516 ed.3, J-Series)	Link-16 (STANAG 5516 ed.4, J-Series)		**Data In-terchange**	For CCEB in-teroperability the mandatory standard is

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					MIL-STD 6016C and the emerging standard is MIL-STD 6016C Change 1
	Link-22 (STANAG 5522 ed.1, J-Series)	Link-22 (STANAG 5522 ed.2, J-Series)		**Data Interchange**	
	PDF-Format 1.4		Formets deleted in NCSP v.6	**Data Interchange**	Portable document presentation format, realised in Adobe product versions 5 and 6. Used in Minerva system at NATO HQ For CCEB interoperability the primary standard is Adobe Postscript (level I and II)/ Encapsulated Postscript (EPS), and the secondary standard is Adobe PDF
	Rich Text Format (RTF)			**Data Interchange**	Basic document interchange format
	ASCII Text, ISO 646:1991			**Data Interchange**	For constrained environments
	Document Ob-		Not to be used	**Data In-**	Basic Docu-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	ject Model (DOM) Level 2		for new systems	**terchange**	ment Object Model .
	Document Object Model (DOM) Level 3			**Data Interchange**	
	Office 2000 formats: Office XP			**Data Interchange**	Not to be used for new systems.
	Office XP formats			**Data Interchange**	Pertains to the interchange formats of MS Word, Excel and PowerPoint, irrespective of the actual MS Office version or general office automation package being used.
	OpenDocument ISO/IEC 26300:2006			**Data Interchange**	Formerly published as OASIS standard.
	HTML 4.01 (RFC 2854:2000)			**Data Interchange**	
	XHTML 1.0:2002 (W3C)			**Data Interchange**	XHTML is specified in XML
	SGML (ISO 8879:1986)			**Data Interchange**	For high value complex documents
	XML 1.0 2nd ed:2003, W3C			**Data Interchange**	Where semantic tags are required, the NC3 Repository serves as an

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					XML registry (see Data Management).
		XML 1.0 3rd ed:2004, W3C		**Data Interchange**	
		XLink 1.0:2001, W3C		**Data Interchange**	XLink is used to point to resources from XML documents.
		XPointer 1.0:2001, W3C		**Data Interchange**	XPointer is used to identify XML fragment inside any given XML documents.
		Relax NG (ISO/IEC 19757-2:2003)		**Data Interchange**	Relax NG may be a replacement for XML schema languages.
	XML Base:2001, W3C			**Data Interchange**	
	XML Infoset:2001, W3C			**Data Interchange**	
	XSL Association:1999, W3C			**Data Interchange**	
	Namespaces in XML (xml-names-19990114:1999)			**Data Interchange**	
	Extensible Stylesheet Language Transforma-			**Data Interchange**	

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	tion (XSLT) 1.0:1999				
	Extensible Stylesheet Language (XSL) 1.0:2001			**Data Interchange**	
	XML Schema, Part 0-2:2001			**Data Interchange**	
	Wireless Markup Language (WML) 2.0:2001			**Data Interchange**	WML to be used with Wireless Application Protocol (WAP) for constrained environments
		Efficient XML Interchange Format (EXI) v1.0			Efficient implementations of XML in the tactical environment
Mediation (MED)					
	NC3 Repository			**Data Mgmt**	Common repository for standard data elements and their related tool for the NATO Corporate Data Model for Data Administration. See also XML. For CCEB interoperability this standard is

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					partially applic-able
	SQL 3 (ISO/IEC 9075(-1 to -14):2003)		Full Level and ISO/IEC 9075:1999 canceled, new Version ISO/ IEC 9075(-1 to -14):2003, Parts 1, 2 and 11 encompass the minimum requirements of the lan-guage. Other parts define extensions.	**Data Mg-mt**	
	ODMG 3.0:2000			**Data Mg-mt**	
	ODBC 3.0 (ISO/IEC 9579:2000)			**Data Mg-mt**	
	JAVA DBC (JDBC)		JDBC separ-ated from ODBC	**Data Mg-mt**	
	SQL CLI (ISO/IEC 9075-3:2003)			**Data Mg-mt**	
	ATCCIS Rep-lication Mech-anism (ARM) from STANAG 5525 ed. 1:2007			**Data Mg-mt**	
	Spatial Schema ISO 19107:2003, DGIWG/			**Data Mg-mt**	ISO 19107 provides con-ceptual schem-as for describ-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	TSMAD profiles of ISO 19107				ing and manipulating the spatial characteristics of geographic features. The DGIWG/ TSMAD profiles are intended to define sub-schemas of ISO 19107 to be used for defining data interchange formats. For CCEB interoperability this standard is emerging
	Rules for application schema ISO 19109:2005			**Data Mgmt**	ISO 19109 defines rules for creating and documenting application schemas, including the principles for the definition of features. Required for Geo to ensure consistency of use in the definition and use of the geographic features. For CCEB in-

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					teroperability this standard is emerging
	Methodology for feature cataloguing ISO 19110:2005			**Data Mg-mt**	ISO 19110 defines the methodology for cataloguing feature types and specifies how the classi-fication of fea-ture types is or-ganized into a feature cata-logue and presented to the user of a set of geographic data. For CCEB in-teroperability this standard is emerging
	Spatial Refer-encing by geo-graphic identi-fiers ISO 19112:2003			**Data Mg-mt**	ISO 19112 defines the con-ceptual schema for spatial ref-erences based on geographic identifiers. This standard en-ables gazetteers to be construc-ted in a consist-ent manner. For CCEB in-teroperability this standard is

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					emerging
	ISO 19125-1:2004 and ISO 19125-2:2004			**Data Mg-mt**	ISO 19125-1 establishes a common architecture for geographic information (simple feature profile of ISO 19107) and defines terms to use within the architecture. It also standardizes names and geometric definitions for Types for Geometry. ISO 19125-2 specifies and SQL schema that support storage, retrieval, query and update of simple geospatial feature collections via the SQL Call Level Interface (SQL/CLI) and establishes and architecture for the implementation of feature tables. For CCEB in-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					teroperability this standard is emerging
	Joint C3 Information Exchange Data Model (JC3IEDM, STANAG 5525 ed.1:2007) for the Land environment	Joint C3 Information Exchange Data Model (JC3IEDM, STANAG 5525 ed.1:2007) for the Joint, Maritime and Air environments	C2IEDM replaced by JC3IEDM	**Data Mgmt**	C2IEDM replaced by JC3IEDM. For CCEB JC3IEDM is mandatory for all environments.
	WebCGM (Web Computer Graphics Metafile), W3C REC 20011217, 2001		CGM (ISO/IEC 8632:1999) not for new systems	**Data Interchange**	Primarily intended for vector-based images.
	SVG 1.2			**Data Interchange**	The preferred format to visualize maps in the Web browser.
	Mobile SVG Profiles: SVG Tiny and SVG Basic, W3C REC 20030114, 2003			**Data Interchange**	SVG profiles for cellphones and PDAs
	JPEG 2000 (ISO/IEC 15444-1:2004, ISO/IEC 15444-2:2004,			**Data Interchange**	JPEG 2000 is the standard used to store raster data (imagery,

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	ISO/IEC 15444-3:2007, including Amd 2:2003, ISO/ IEC 15444-4:2004, ISO/IEC 15444-5:2003, ISO/IEC 15444-6:2003,)				scanned maps, matrix data) and provides the ability to include spatial referencing information within the standard. For CCEB interoperability ISO/IEC 15444-2 Cor. 3 is not applicable.
		JPEG LS (ISO/IEC 14495:2003)		**Data Interchange**	Loss-less and near loss-less compression of continuous tone still images.
	PNG 1.0 (RFC 2083:1997)			**Data Interchange**	Portable Network Graphics PNG is intended for the com-pressed storage of raster images. PNG provides a patent-free replacement for GIF.
	ITU-T T.4:2003			**Data Interchange**	
	ITU-T T.30:2005			**Data Interchange**	
	TDF (STANAG 5000 ed.3:2006)			**Data Interchange**	For CCEB interoperability Secure Telephone Equipment (STE) is

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					used for secure fax. The emerging standard is Secure Communication Interoperability Protocol (SCIP).
	ADatP-3, CONFORMETS/Change 4 (STANAG 5500, ed. 5:2006), Database Baseline 12.2.	ADatP-3 Database Baseline 13		**Data Mgmt**	For CCEB interoperability the standard is MIL-STD 6040 and OTH-T GOLD standards baseline 14 is actually under construction
	APP-11(A)/ STANAG 7149ed.2 NATO Message Catalogue	APP-11(B)/ STANAG 7149ed.3 APP-11(C)/ STANAG 7149ed.4		**Data Mgmt**	APP-11 (STANAG 7149) as the single source for NATO Military Messages for command and control of NATO forces at all levels of the Chain of Command down to and including individual units. For CCEB interoperability this standard is not applicable
	EDIFACT (ISO			**Data Interchange**	EDIFACT can be used to

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	9735:2002)				transfer business documents such as purchase orders, invoices, and electronic funds transfer information. ebXML is a UN standard
	ebXML Messaging Service v. 2:2002 (OASIS)			**Data Interchange**	
	DIGEST V2.0 and DIGEST V2.1, STANAG 7074, AgeoP-3 (VMaps, USRP, ASRP)			**Data Interchange**	Source data may be provided in this format for conversion to the neutral database format by the CWS. Note: DGIWG is in the process of restructuring DIGEST based on the ISO 19100 series. They are generating military specific profiles of the ISO standards. Of particular interest to the Core GIS project are profiles of: Spatial Schema (19107), Gener-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					al Feature Model (19109), Metadata (19115), Portrayal (19117), and FACC Data Dictionary (19126). For CCEB interoperability the mandatory standard is DGIWG Feature Data Directory 2006 and DIGEST v2.1 is fading.
	ISO 19136 (GML 3.2)		Not to be used in new systems	**Data Interchange**	This OpenGIS Consortium recommendation standard may be used as the transfer format between the FA providing the published operational data (e.g. COP) and the Core Map Application Server. For CCEB interoperability GML 3.1 is emerging
	DLMS/DTED (STANAG 3809 ed.4)			**Data Interchange**	Digital Terrain Elevation Exchange Format

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	DLMS/ DFAD1			**Data Interchange**	DLMS/DFAD1 must be used until DIGEST/ VMAP 1 covers the whole world. For CCEB interoperability this standard is not applicable
	World Geodetic System (WGS) 84			**Data Interchange**	WGS specifies the set of parameters that define mathematically the shape of the earth
	Geographic Information - Metadata - ISO 19115:2003			**Data Interchange**	This provides the most comprehensive metadata specification for digital geographic data. This shall be used for the geo metadata which forms the foundation of the Core Geo Catalogue. It is likely that a NATO profile of this standard will have to be produced based on the DGIWG profile. For CCEB in-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					teroperability this standard is emerging.
		WECDIS (STANAG 4564 ed.1)		**Data Interchange**	Standard for Warship Electronic Chart Display and Information Systems.
	SEDRIS (ISO/IEC 18023-1:2006)			**Data Interchange**	Environmental data representation and interchange specification
	EDCS (ISO/IEC 18025:2005)			**Data Interchange**	Environmental data coding specification
	SRM (ISO/IEC 18026:2006)			**Data Interchange**	Spatial reference model
	Geodetic Projections, STANAG 2211 ed.6			**Data Interchange**	
	AML, STANAG 7170 ed.1			**Data Interchange**	
				Data Interchange	For CCEB interoperability the mandatory standard is Warfighter Symbology (MIL-STD 2525B)
	Military Symbols for Land-based Systems	Military Symbols for Land-based Systems		**Data Interchange**	APP6(A) is a superset of STANAG

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	(APP6(A)/ST ANAG 2019 ed.4)	(APP6(A)/ST ANAG 2019 ed.5)			2019. Recently defined by the US in MIL-STD 2525B. Provides a more complete range of sym-bols than APP6a.includin g maritime symbols and rules.
		Portrayal ISO/ DIS 19117:2005		**Data In-terchange**	Currently in Draft. Interna-tional Standard specifies the in-terface to stand-ard symbol sets, not the symbols them-selves.
	Symbols on Land Maps, Aeronautical Charts and special Naval Charts (STANAG 3675 ed.2)			**Data In-terchange**	
	IHO S-57, Version 3.1, 2000	IHO S-57, Version 4.0		**Data In-terchange**	Standard defined by IHO for digital mari-time informa-tion. Currently in harmonisa-tion with DI-GEST. Access to S-57 data may be re-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					quired by maritime users. S-57, Version 4.0 should support a greater variety of hydrographic-related digital data sources, products and customers. For CCEB interoperability IHO S-52, S-57, S-61 and S-63 standards are mandatory.
	Web Map Service v.1.3 (OGC 04-024)	ISO 19128:2005 Web Map Service		**Data Interchange**	Used as a means of distributing compiled mapping data between applications.
	Web Feature Service v.1.1 (OGC 04-094)			**Data Interchange**	Used as a means of distributing geo feature (vector) data between applications. For CCEB interoperability this standard is emerging
	Web Coverage Service v.1.0 (OGC 03-065r6)			**Data Interchange**	Used as a means of distributing geo coverages (raster) data

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					between applic-ations. For CCEB in-teroperability this standard is emerging
		GML in JPEG 2000 for Geo-graphic Im-agery (GMLJP2) (OGC 05-047r)		**Data In-terchange**	This evolving OGC standard describes min-imally required GML definition for georeferen-cing images and gives guidelines for augmenting that definition to address the additional en-coding of metadata, fea-tures, annota-tions, styles, coordinate ref-erence systems, and units of measure for data encoded in JP2K
		OGC Web Terrain Ser-vice and OGC Web3DServic e		**Data In-terchange**	Used as a means to per-form Web Ser-vice based Ter-rain analysis and communic-ate terrain data to clients
		OGC - ISO 19115:2003/ ISO		**Data In-terchange**	Describes the organisation and implement-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
		19119:2005 Application Profile for CSW 2.0			ation of Catalogue Services based on the ISO 19115 / ISO 19119 Application Profile
		Web Registry Service v.0.0.2 (OGC Ref. 01-024r1)		**Data Interchange**	Used as a means of publishing and finding geo services.
		Catalog Interface v.1.1.1 (OGC Ref. 02-087r3)		**Data Interchange**	Used as a means of discovering geo metadata.
	Computer Graphics Interface (CGI ISO/IEC 9636:1991)		Computer Graphics Interface (CGI ISO/IEC 9636:1991) not for use in new systems	**Data Interchange**	For CCEB interoperability this standard is not applicable
	OpenGL v2.0:2004		OpenGL v1.5:2003 not to be used for new systems	**Data Interchange**	For CCEB interoperability this standard is not applicable
	UML v2.0:2003 (OMG)			**Data Interchange**	For CCEB interoperability this standard is not applicable
	Codes for the representation of Currencies and Funds (ISO 4217:2001)			**Internationalisation**	
	Letters for Geographic			**Internationalisa-**	For CCEB interoperability

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	Entities, STANAG 1059, ed.8			**tion**	the country codes standard is ISO 3166 trigraphs except for military messaging - see CCEB COMAG Policy On Security Labelling
	ECMA Script Language Specification (ECMA 262)			**SW Engineering**	Scripting required for enhanced Web pages For CCEB interoperability this standard is not applicable
Translator					
	Zip			**Data Interchange**	Implementations of zip (e.g. Winzip) also includes gzip (RFC 1952:1996) and tar/compress
	7-bit Coded Character-set for Info Exchange (ASCII) (ISO/IEC 646:1991)		Not to be used for new systems.	**Data Interchange**	
	8-bit Single-Byte Coded Graphic Char Sets (ISO/IEC 8859-1-6,8-10: 1999; 7:2003)		Not to be used for new systems	**Data Interchange**	

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	Universal Multiple Octet Coded Char Set (UCS) - Part 1 (ISO/IEC 10646:2003)			**Data In-terchange**	
	NATO Stand-ard Bar Code Symbology (STANAG 4329 ed.2:2004)			**Data In-terchange**	STANAG 4329 is a cover STANAG of ISO 16388:1999 - Bar code sym-bology spe-cifications - Code 39.
	Bar code sym-bology spe-cification - Code 128 (ISO/IEC 15417:2000), Bar code print quality test specification - Linear sym-bols (ISO/IEC 15416:2000)			**Data In-terchange**	
	Representation of Dates and Times (ISO 8601:2004)			**Data In-terchange**	
	UUENCODE (UNIX 98), MIME (IETF RFC 2045:1996, 2047:1996 up-dated by 2231:1997;	S/MIME ESS (IETF RFC 3850:2004, 3851:2004)		**Data In-terchange**	Base64 is in-cluded in RFC 2045:1996

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	2046:1996 up-dated by 3676:2004, 3798:2004; 2048:1996 up-dated by 4288:2005, 4289:2005; 2049:1996, 4288:2005, 4289:2005)				
Collaboration (COL)					
Message based Conferencing					
Audio Based Conferencing					
Video Based Conferencing					
Shared Distrib-uted Work-space					
Doc Mgmt					
Customer Rela-tionship					
Human Re-source Mgmt					
Supply Chain Mgmt					
Learning Mgmt					
Workflow Mg-mt					
Web services					
		WS-BPEL			
		WSCI			
		BPML			

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
		OpenSIS			
		J2EE			
		JRMI			
		DSML v2.0:2001, OASIS		**Distr. Comp.**	DSML provides a Dir-cetory Access via a Web in-terface
	UDDI v2.0, W3C	UDDI v3.0, W3C		**Distr. Comp.**	UDDI 2.0 provides a plat-form-in-dependent way of describing- and disovering service. For CCEB interop-erability UDDI 3.0 is mandat-ory
		WSDL v1.1:2001, W3C		**Distr. Comp.**	For CCEB in-teroperability WSDL v1.1 is mandatory
		ISO/TS 15000-1:2004, -2:2004, -3:2004, -4:2004, -5:2005 Elec-tronic Busi-ness Extens-ible Markup Language (ebXML)		**Distr. Comp.**	ebXML is a suite of spe-cifications for standardizing XML based business mes-sages to facilit-ate trading between organ-isation.
		XML Path Language (XPath) v2.0:2003, W3C		**Distr. Comp.**	For CCEB in-teroperability this standard is mandatory

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	WS-I Web Service Basic Profile, v1.1:2nd ed. 2006	WS-I Web Service Basic Profile, v1.2:3rd ed. 2007		**Distr. Comp.**	For CCEB interoperability this profile is mandatory
	Simple Object Access Protocol v1.2 (SOAP), W3C			**Distr. Comp.**	Could be used in support of the Geo Web Services.
		WS-I Simple SOAP Binding Profile v1.0:2004		**Distr. Comp.**	For CCEB interoperability this profile is mandatory
		WS-I Attachments Profile v1.0:2nd ed. 2006		**Distr. Comp.**	For CCEB interoperability this profile is mandatory
User Assistance (UAS)					
Portal					
Knowledge Mgmt					
Content Mgmt					
User Workspace Mgr					
Notifier					
Device Independent Console					
	X Window System 11 R6.6		X Window System 11 R5	**Graphical UI**	The R6.6 release addresses a portion of the backlog of bug reports since Release 6.5.1 patch 1, along with additional fixes from the

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
					Xfree86 community. R5 should not be used for future systems. For CCEB interoperability this standard is not applicable
	Win 32 APIs			**UAS**	As part of MS Windows 2000 Interfaces For CCEB interoperability this standard is not applicable
	CDE 2.1		CDE 1.0	**Graphical UI**	Common Desktop Environment is the UNIX Windows Desktop equivalent. For CCEB interoperability this standard is not applicable
	Motif/CDE Style Guide Rev 2.1		Motif Style Guide Rev 1.2	**Graphical UI**	Toolkit specific style guides For CCEB interoperability this standard is not applicable
	MS Windows Interface Guidelines for Software			**Graphical UI**	Toolkit specific style guides. As part of MS Windows 2000

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NNEC CORE ENTERPRISE SERVICES					
	Design				Interfaces. For CCEB in-teroperability this standard is not applicable
	Motif 2.1		Motif 1.2	**Graphical UI**	For CCEB in-teroperability this standard is not applicable
Report Gener-ator					

3.5. NETWORKING INFORMATION INFRASTRUCTURE SERVICES

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
Distributed Computing					
Distributed Computing					
		DCE v1.1		**Distr. Comp.**	
		ONC 1.1 (The Open Group)		**Distr. Comp.**	
		DCE RPC v1.1		**Distr. Comp.**	
		MS-RPC		**Distr. Comp.**	As part of MS Windows 2000 Interfaces
	X Window (see UI Svc)			**Distr. Comp.**	

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
		DCE DFS v1.1		**Distr. Comp.**	
		XNFS 3W (The Open Group)		**Distr. Comp.**	Includes RFC 1094:1989 (NFS 89) and RFC 1813:1995 (NFS95)
		MS-SMB		**Distr. Comp.**	As part of MS Windows 2000
		DCE DTS v1.1		**Distr. Comp.**	DCE DTS uses TPI (Time Provider Interface) to access other distributed time services (such as NTP as mentioned under Comms Service).
		CORBA/IIOP 2.2		**Distr. Comp.**	
		MS-DCOM		**Distr. Comp.**	As part of MS Windows 2000 Interfaces; DCOM only in local environment, not for outside.
	Standardised Information technology Protocols for Distributed Interactive Simulation (DIS)(STANAG 4482 ed.1:1995)		STANAG 4482 should be migrated to IEEE Std 1278:1998	**Distr. Comp.**	For CCEB interoperability the mandatory standard is IEEE Std 1278.1a:1998 STANAG 4482 should also be migrated to IEEE Std 1278:1998

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
		HLA (IEEE 1516:2000)		**Distr. Comp.**	For CCEB in-teroperability this standard is mandatory
Information Structure					
Meta data					
Relational Data					
Document					
Information Objects					
Ontology					
Business Rules					
Access					
Directory					
	DNS (IETF STD 13:1987, RFC 1034:1987 and RFC 1035:1987 up-dated by RFC 1101:1989, 1183:1990, 1706:1994, 1876:1996, 1982:1996, 1995:1996, 1996:1996, 2136:1997, 2181:1997, 2308:1998, 2845:2000, 2931:2000, 3007:2000, 3226:2004, 3425:2002, 3597:2004,		RFC 1034:1987 and RFC 1035:1987 up-dated by RFC 1101:1989, 1183:1990, 1706:1994, 1876:1996, 1982:1996, 1995:1996, 1996:1996, 2136:1997, 2181:1997, 2308:1998, 2845:2000, 2931:2000, 3007:2000, 3226:2004, 3425:2002, 3597:2004, 3645:2003, 4033:2005,	**Comms**	Bind version 9 or later should be used.

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	3645:2003, 4033:2005, 4034:2005, 4035:2005, 4343:2006, 4470:2006, 592:2006)		4034:2005, 4035:2005 changed in NCSP v.6		
		IPSec Material in DNS (RFC 4025:2005)		**Comms**	
				Comms	NACOSA Operating Instructions A-03-06 deals with the TCP/IP environment and A-03-07 deals with the OSI environment. Both are due for re-write.
	Assigned Numbers (RFC 3232:2002)			**Comms**	
Web Access					
Dial-in Access					
WAN Access					
LAN Access					
Roaming					
Proxy					
Structured Information Exchange					
Datalink GW					
Replication					

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
GW					
Message GW					
Property Based P2P					
Non-real Time Info Transport					
Real-time Info Transport Se-cure info rrans-port non-secure Info Transport					
Unstructured Information Exchange					
File Transfer					
File Based P2P					
Network Ser-vices					
Core IP					
	IPv4 (STD 5, RFC 791:1981, 792:1981, 894:1984, 919:1984, 922:1984, 950:1985 up-dated by RFC 1112:1989, 2474:1998, 2507:1999, 2508:1999, 3168:2001, 3260:2002, 3376:2002, 4604:2006, 4884:2007)	IPv6 (RFC 1981:1996, 2375:1998, 2460:1998, 2461:1998, 2462:1998, 2464:1998, 2467:1998, 2470:1998, 2491:1999, 2492:1999, 2497:1999, 2526:1999, 2529:1999, 2590:1999, 2710:1999 up-dated by 3590:2003, 2711:1999,		**Comms**	Note: Category of RFC 2375:1998 is ´Informal´

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
		2894:2000, 3041:2001, 3056:2001, 3111:2001, 3122:2001, 3146:2001, 3306:2002, 3307:2002, 3483:2003, 3510:2003, 3544:2003, 3587:2003, 3595:2003, 3697:2004, 3736:2004, 3810:2004, 3879:2004, 3956:2004, 4001:2005, 4007:2005, 4213:2005, 4291:2006, 4311:2005, 4338:2006, 4489:2006, 4443:2006, 4489:2006, 4604:2006, 4884:2007)			
		IGMP v.3 (RFC 3376:2002 up-dated by 4604:2006)		**Comms**	RFC 3367:2002 obsoleted 2236:1997 up-dates RFC 1112:1989 and is widely im-plemented, RFC 3376:2002 obsoleted RFC 2236:1997
	Host require-ments (STD 3,			**Comms**	

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	IETF RFC 1122:1989 updated by 2474:1998, 2181:1997, 3168:2001, 3260:2002, 4033:2005, 4034:2005, 4035:2005, 4343:2006, 4379:2006)				
	Bootstrap Protocol, BOOTP (RFC 951:1985 updated by RFC 1542:1993, 2132:1997, 3442:2002, 3942:2004, 4361:2006, 4833:2007)		Not to be used for new systems.	**Comms**	Will be overtaken by the richer DHCP. BOOTP is still available in older implementations and is expected to phase out.
	Clarifications and Extensions for the Bootstrap Protocol (RFC 1542:1993)			**Comms**	Not to be used for new systems.
		DHCP for IPv6 (RFC 3315:2003 updated by 4361:2006)	DHCP Options and BOOTP Vendor Extensions not to be used in new systems	**Comms**	
		IPv6 Prefix Options for DHCPv6 (RFC		**Comms**	

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
		3633:2003)			
		DNS Config-uration Op-tions for DH-CPv6 (RFC 3646:2003)		**Comms**	
		NIS-Options for DHCPv6 (RFC 3898:2004)		**Comms**	
	Dynamic Host Configuration Protocol, DH-CP (RFC 2131:1997 up-dated by RFC 3396:2002, 4361:2006)			**Comms**	
	Differentiated Services Field (RFC 2474:1998 up-dated by 3168:2001, 3260:2002)			**Comms**	DiffServ re-defines use of former TOS field; first, but not sufficient RFC to differ-entiate traffic classes. RFC for DiffServ still missing. Applicable to both IPv4 and IPv6
	Requirements for IPv4 routers (RFC 1812:1995 up-dated by 2644:1999)			**Comms**	
	Open Shortest Path First (OSPFv2)	OSPF for IPv6 (RFC 2740:1999)		**Comms**	Suitable for LANs as well as WANs

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	(RFC 2328:1998)				(including tactical networks) with sufficient bandwidth
	Router Internet Protocol (RIP v2) (IETF STD 56/RFC 2453:1998 updated by 4822:2007)	RIPng for IPv6 (RFC 2080:1997)		**Comms**	
	Border Gateway Protocol (BGP4) (RFC 4271:2006)	Multiprotocol Extensions for BGP-4 (RFC 2858:2000); Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing (RFC 2545:1999)		**Comms**	
		BGMP (RFC 3913:2004)		**Comms**	
	Application of BGP-4 (RFC 1772:1995)			**Comms**	
	Protocol Independent Multicast Sparse Mode(PIM-SM) (RFC 4601:2006)			**Comms**	PIM-SM is implemented by the router market leaders.
		Protocol Independent Multicasting Dense Mode(PIM-DM) (RFC		**Comms**	PIM-DM is included as a second concept for tactical networks

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
		3973:2005)			
		Generic Routing Encapsulation (GRE) (RFC 4023:2005)		**Comms**	GRE is included as a general routing encapsulation mechanism
	Traditional IP Network Address Translator (RFC 3022:2001)	Network Address Translation - Protocol Translation (NAT-PT) (RFC 2766:2000 updated by 3596:2003)		**Comms**	NAT-PT is the translation of an IP PDU within one IP network into an IP PDU of another IP network.
		Stateless IP/ ICMP Translation Algorithm (SIIT) (RFC 2765:2000		**Comms**	
		Generic Packet Tunneling in IPv6 (RFC 2473:1998)		**Comms**	This RFC is a generic tunnel mechanism, which can be applied for several protocols.
	Router Internet Protocol (RIP v2) MIB extension (RFC 1724:1994)		To be used only in static networks.	**Comms**	To be used in static networks. See also System Management.
	Classless Inter Domain Routing (CIDR) (RFC 4632:2006)			**Comms**	CIDR is only valid for IPv4
	Mobile IPv4 (RFC	Mobile IPv6 (RFC		**Comms**	

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	3344:2002 up-dated by 4721:2007)	3775:2004)			
		IPSec and Mo-bile IPv6 (RFC 3776:2004 up-dated by 4877:2007)		**Comms**	
		Policy-based Network Man-agement - General (RFC 1104:1989, 2753:2000, 3198:2001, 3334:2002)		**Comms**	
		Policy-based Network Man-agement - DiffServ (RFC 2963:2000, 2998:2000, 3086:2001, 3260:2002, 3287:2002, 3289:2002, 3290:2002, 3308:2002, 3496:2003)		**Comms**	
		Policy-based Network Man-agement - Int-Serv (RFC 2205:1997 up-dated by 2750:2000, 3936:2004, 4495:2006, 2206 -		**Comms**	

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
		2210:1997, 2370:1998 up-dated by 3630:2003 up-dated by 4203:2005, 2380:1998, 2382:1998, 2430:1998, 2490:1999, 2745 - 2746:2000, 2747:2000 up-dated by 3097:2001, 2749:2000, 2750:2000, 2755:2000, 2814:2000, 2872:2000, 2961:2001, 2996:2000, 3097:2001, 3175:2001, 3181:2001, 3182:2001, 3209:2001 up-dated by 3936:2004, 4420:2006, 4874:2007; 3210:2001, 3468:2003, 3473:2003 up-dated by 4003:2005, 4201:2005, 4420:2006, 4783:2006, 4783:2006, 4873:2007,			

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
		4874:2007; 3474:2003, 3476:2003, 3477:2003			
	Point to Point Protocol (PPP) Internet Protocol Control Protocol (IPCP) (RFC 1332:1992 updated by 3241:2002, 4815:2007)			**Comms**	To allow packet switched services over circuit switched interconnections.
	Link Control Protocol (LCP) extensions (RFC 1570:1994 updated by 2484:1999)			**Comms**	Addition to LLC1 (see Link Layer).
	Point to Point Protocol (PPP) (STD 51, RFC 1661:1994 updated by 2153:1997, 1662:1994)	IPv6 over PPP (RFC 2472:1998)		**Comms**	
	PPP Challenge Handshake Authentication Protocol (CHAP) (RFC 1994:1996 updated by 2484:1999)			**Comms**	Used in routers
	PPP Multilink (MP) (RFC 1990:1996)			**Comms**	Allows for aggregation of bandwidth via multiple simul-

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
					taneous data link connections
External Networks					
	X.25 (1996, Cor.1:1998)		Not to be used for new systems.	**Comms**	
	NATO Multi Channel Digital Strategic Tactical Gateway (DSTG) (STANAG 4578 ed. 1:2003)	Enhanced Digital Strategic Tactical Gateway (EDSTG) (STANAG 4578 ed. 2 (Draft))	STANAG 4249 replaced by the more fundamental STANAG 4206. STANAG 4206 not to be used for new systems.	**Comms**	STANAG is currently under review for a new edition. For CCEB interoperability this standard is not applicable STANAG 4206 not to be used for new systems.
	NATO Multichannel tactical digital Gateway (STANAG 4206: Ed.3:1999)			**Comms**	The overlapping area between STANAG 4206 and STANAG 4578 has to be resolved by SC/6. For CCEB interoperability this standard is not applicable
					For CCEB interoperability the mandatory standard is ACP 200:

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
					Maritime Tactical Wide Area Networking
		Tactical Communications Post 2000, Draft STANAGs 4637 - 4647:2005		**Comms**	
	ISDN: ITU-T G, I Series			**Comms**	ISDN Telephony
	ITU-T E, P, Q, V Series			**Comms**	Not to be used for new systems.
	ITU-T V.90:1998		ITU-T V.90:1998 not to be used for new systems.	**Comms**	
	ITU-T V.42:2002 Corrigendum 1:2003		ITU-T V.42:2002 Corrigendum 1:2003 not to be used for new systems.	**Comms**	
	User Network Interface - UNI v4.0 (af-sig-0061.000)		UNI v4.0 and v4.1 not to be used for new systems	**Comms**	
	Private Network - Network Interface - PNNI v1 (af-pnni-0055.000)	PNNI v1 and v1.1 bot to be used for new systems		**Comms**	
	LAN Emulation over ATM - LANE v2.0		Not to be used for new systems.	**Comms**	For CCEB interoperability this standard is

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	(af-lane-0084.000, af-lane-0112.000)				not applicable.
	Standards for Data Forwarding between Tactical Data Systems employing Link-11/11B and Link-16 (STANAG 5616 ed.3:2006)	Standards for Data Forwarding between Tactical Data Systems employing Link-11/11B and Link-16 (STANAG 5616 ed.4)		**Comms**	Gateway between Link-11 and Link-16. For CCEB interoperability the mandatory standard is MIL-STD 6020
	Link 11 STANAG 5511 ed.5:2006	Link 11 STANAG 5511 ed.6		**Comms**	Communications part for Link-11 For CCEB interoperability the standard is MIL-STD 6011C
	STANAG 4175 ed.3:2001	STANAG 4175 ed.4		**Comms**	Communications part for Link-16
	STANAG 4372 ed.2:2006 (Saturn)	STANAG 4372 ed.3 (Saturn)		**Comms**	UHF standard for Link-22, but can also carry Link-11 and Link-16 messages.
	STANAG 7085 ed.2:2004 (IDL for Imaging Systems)			**Comms**	STANAG 7085 provides the interoperability standards for 3 classes of imagery DL used for primary im-

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
					agery data transmission.
	STANAG 4586 ed.1:2004	STANAG 4586 ed.2		**Comms**	STANAG 4586 facilitates com-munication between a UCS and different UAVs and their payloads as well as multiple C4I users.
Mixed DISA standards					
Transport Ser-vices					
	Winsock 2 (Revision 2.2)			**Comms**	
	TCP (IETF STD 7:1981, RFC 0793:1981 up-dated by RFC 3168:2001)			**Comms**	
	UDP (IETF STD 6:1980, RFC 0768:1980)			**Comms**	
	OSI transport svc over TCP/ IP (RFC 2126:1997)			**Comms**	Includes the ISO Transport Protocol
Transmission					
		STANAG 4444 ed.1 (Slow hop EC-CM)		**Comms**	HF standard for Link-22. For CCEB in-

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
					teroperability this STANAG is mandatory.
		JREAP, MIL-STD 3011		**Comms**	
	ISO/IEC 8802-3:2000 (CSMA/CD)			**Comms**	
					For CCEB in-teroperability the mandatory standard is In-teroperability and Perform-ance Standard for SATCOM (MIL-STD 188-164).
					For CCEB in-teroperability the mandatory standard is MIL-STD-188-181B
					For CCEB in-teroperability the mandatory standard is In-teroperability Standard for 5-Khz UHF DAMA Ter-minal Wave-form MIL-STD-188-182A
	Interoperabil-ity Standard for 25 kHz UHF/ TDMA/	Interoperabil-ity Standard for 25 kHz UHF/ TDMA/		**Comms**	STANAG 4231 ed.4 is identical with MILSTD-188-183B.

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	DAMA ter-minal Wave-form STANAG 4231 ed.4:2003	DAMA ter-minal Wave-form STANAG 4231 ed.5			For CCEB in-teroperability the mandatory standard is MIL-STD-188-183D
					For CCEB in-teroperability the mandatory standard is In-teroperability and Perform-ance Standard for the Data Control Wave-form MIL-STD-188-184
					For CCEB in-teroperability the mandatory standard is DoD Interface Standard, Inter-operability of UHF MILSAT-COM DAMA Control System MIL-STD-188-185
					For CCEB in-teroperability the mandatory standard is In-teroperability and Perform-ance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Com-

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
					munications Earth Terminals, 13 Jan 1995 MIL-STD-188-164
					For CCEB interoperability the mandatory standard is Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995, with Notice of Change 1, 9 September 1998, MIL-STD-188-165
	Digital interoperability between EHF Tactical Satellite Communications Terminals (STANAG 4233 ed.1:1998)			**Comms**	For CCEB interoperability the mandatory standard is MIL-STD-1582D
		ECM-resistant digital traffic exchange between tac-		**Comms**	For CCEB interoperability this standard is not applicable

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
		tical satellite communications terminals (STANAG 4271 ed.1)			
	Super High Frequency (SHF) Military Satellite (MILSATCOM) jam- resistant modem (STANAG 4376 ed.1)			**Comms**	For CCEB interoperability this standard is not applicable
	Overall Super High Frequency (SHF) Military Satellite COMmunications (MILSATCOM) interoperability standards (STANAG 4484 ed.2:2003)			**Comms**	For CCEB interoperability this standard is not applicable
	SHF MILSATCOM Non-EPM modem for services conforming to class-A of STANAG 4484 (STANAG 4485 ed.1:2002)			**Comms**	For CCEB interoperability this standard is not applicable
	Super High Frequency			**Comms**	For CCEB interoperability

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	(SHF) Military Satellite COMmunica-tions (MILSATCOM) Frequency Division Multiple Access (FDMA) Non-EPM modem for services conforming to class-B of STANAG 4484 (STANAG 4486 ed.2:2002)				this standard is not applicable
		UHF MILSATCOM interoperability standards for paging receiver (Draft) (STANAG 4492 ed. 1)		**Comms**	For CCEB interoperability this standard is not applicable
		SHF MILSATCOM network management and control (Draft) (STANAG 4505 ed.1)		**Comms**	For CCEB interoperability this standard is not applicable
	EHF MIL SATCOM interoperability standards for medium data rate services STANAG 4522			**Comms**	For CCEB interoperability the mandatory standard is MIL-STD-188-136

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	ed.1:2006				
		Link control for Super High Frequency (SHF) Military Satellite COMmunications (MILSATCOM) Frequency Division Multiple Access (FDMA) Non-Electronic Protective Measure (Non-EPM) modem for services confirming to class-B of STANAG 4484 (Draft) (STANAG 4577 ed.1)		**Comms**	For CCEB interoperability this standard is not applicable
		Super High Frequency (SHF) Medium Data Rate (MDR) Military Satellite COMmunications (MILSATCOM) jam-resistant modem interoperability standards (Draft) (STANAG 4606 ed.1)		**Comms**	For CCEB interoperability this standard is not applicable

SERVICE CATEGORY / CATEGORY	MANDATORY STANDARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
		Interoperability standard for Satellite Broadcast Services (SBS) (Draft) (STANAG 4622 ed.1)		**Comms**	For CCEB interoperability this standard is not applicable
	ACP 190 (B)			**Comms**	
	ACP 190 (B) NATO Suppl 1A			**Comms**	For CCEB interoperability this standard is not applicable
	ACP 190 (B) NATO Suppl 2			**Comms**	For CCEB interoperability this standard is not applicable
					For CCEB interoperability the mandatory standard is Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the LF Band and Lower Frequency Bands MIL STD 188-140A
	Technical standards for single channel HF radio equipment STANAG	Technical standards for single channel HF radio equipment STANAG		**Comms**	For CCEB interoperability the mandatory standard is MIL STD 188-141A

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	4203 ed.2:1988	4203 ed.3			
	Technical standards for single channel VHF radio equipment STANAG 4204 ed.2:1988			**Comms**	For CCEB in-teroperability the mandatory standard is MIL STD 188-242
	Technical standards for single channel UHF radio equipment STANAG 4205 ed.3:2005			**Comms**	For CCEB in-teroperability the mandatory standard is MIL STD 188-243
					For CCEB in-teroperability the mandatory standard is Di-gital Line-of-Sight (LOS) Microwave Ra-dio Equipment, 7 May 1987 MIL STD 188-145
	Conditions for interoperabil-ity of 2400 BPS / HF (STANAG 4197 ed.1:1984)			**Comms**	(QSTAG 1108)
	Characteristics of 1200/2400/ 3600 bps single tone			**Comms**	For CCEB in-teroperability the mandatory standard is

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	modulators/ demodulators for HF Radio links (STANAG 4285 ed.1:1989)				MIL-STD-188-110A
		HF Radios STANAG 4444 ed.1		**Comms**	
		Automatic Ra-dio Control System for HF Links STANAG 4538 ed.1		**Comms**	
	Non-hopping HF Commu-nications Waveforms STANAG 4539 ed.1:2006			**Comms**	
	Profile for HF radio data communica-tions (STANAG 5066 ed.1:2004)	Profile for HF radio data communica-tions (STANAG 5066 ed.2)		**Comms**	
	UHF Radios STANAG 4246 ed.2:1987			**Comms**	For CCEB in-teroperability this standard is not applicable
	MIDS termin-als STANAG 4175 ed. 3:2001	MIDS termin-als STANAG 4175 ed. 4		**Comms**	
	Single serial		RS.232 not to	**Comms**	

SERVICE CATEGORY / CATEGORY	MANDAT-ORY STAND-ARDS	EMERGING NEAR TERM	FADING	NTRM	Remarks
NETWORK AND INFORMATION INFRASTRUCTURE SERVICES (NIIS)					
	line interface (RS-232)		be used for new systems		
	Multi-point serial line (RS-422/RS-423)			**Comms**	Not to be used for new sys-tems.
	Serial binary data exchange at DTE and DCE (RS-530)			**Comms**	
	Generic spe-cification for optical wave-guide fibers (EIA 4920000: 1997)			**Comms**	
QoS					

4. INTEROPERABILITY PROFILES

4.1. MINIMUM INTEROPERABILITY PROFILE

022. NATO, through its interoperability directive, has recognised that widespread interoperability is a key component in achieving effective and efficient operations. In many of the operations world-wide in which NATO nations are engaged, they participate together with a wide variety of other organisations on the ground. Such organisations include coalition partners from non-NATO nations, Non-Governmental Organisation (NGOs - e.g. Aid Agencies) and industrial partners. It is clear that the overall military and humanitarian objectives of an operation could usefully be supported if a basic level of system interoperability existed to enhanced the exchange of information.

023. To support the goal of widespread interoperability this section 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 NISP, however it presents them as a simple and easy to follow, yet comprehensive protocol and service stack.

4.1.1. Architectural Assumptions

024. This document assumes that all participants are using IP v4 packet-switched, routed networks (at least at the boundaries to their networks) and that interoperability will be supported through tightly controlled boundaries between component networks and systems; these may be connected directly or via a third-party WAN (see Figure 4.1 below). A limited set of services will be supported at the boundary, these requiring server-to-server interactions only. Each nation/organisation will be responsible for the security of information exchanged.

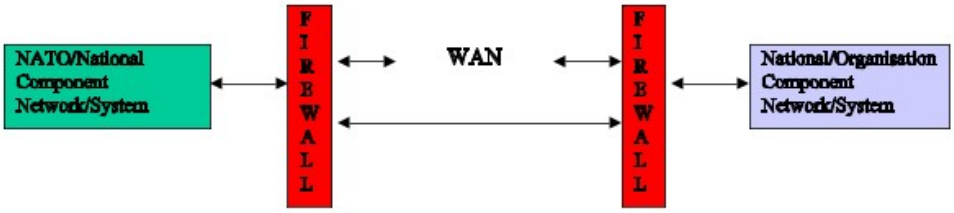

Figure 4.1. NATO to National Connectivity

025. Users will attach and authenticate to their local system/network. Information will only be shared using the limited set of services provided. It is also assumed that the information to be exchanged will predominantly be unclassified.

4.1.2. Shared Services

026. 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:

- Voice
- Mail
- FAX
- C2 information
- E-mail with attachments
- Web publishing/access
- News (Usenet)
- File transfer
- VTC
- Instant Messaging

027. To implement these services in a network enabled environment, the following must also be defined:

- NNEC Application Services
- COI Services
- NNEC Core Enterprise Services
- Network and Information Infrastructure Services

4.1.3. Minimum Architecture

028. The following table defines the service areas, classes and standards that make up the minimum architecture. They represent a subset of the NISP.

Service Area	Class	Mandatory Standard	Comments
NNEC Application Services			
COI Services			
NNEC Core Enterprise Services			
	Messaging	SMTP (RFC 1870:1995, 2821:2001)	
	Application	FTP (IETF STD 9, RFC 959:1985 updated by 2228:1997, 2640:1999, 2773:2000)	
		HTTP v1.1 (RFC 2616:1999 updated by 2817:2000), URL (RFC 1738:1994 updated by 1808:1995, 2368:1998, 2396:1998, 2732:1999), URI (RFC 2396:1998 updated by 2732:1999)	
		Network News Transfer Protocol NNTP (RFC 977:1986)	
		MPEG-1 (ISO 11172:1993)	
		MPEG-2 (ISO 13818:2000)	
		MP3 (MPEG1 - Layer 3)	The audio compression format used in MPEG1
	Translator	7-bit Coded Character-set for Info Exchange (ASCII) (ISO 646:1991)	
		8-bit Single-Byte Coded Graphic Char Sets (ISO/IEC 8859-1-4-9:98/98/99)	
		Universal Multiple Octet Coded Char Set (UCS) - Part 1 (ISO 10646-1:2000)	
		Representation of Dates and Times (ISO 8601:2000)	
	Data encoding	UUENCODE (UNIX 98), MIME (RFC	Base64 is used by some email products to encode

Service Area	Class	Mandatory Standard	Comments
		2045:1996-2049:1996)	attachments. It is part of the MIME std.
	Mediation	Scalable Vector Graphics (SVG) 1.1 20030114, W3C	
		JPEG (ISO 10918:1994)	
		PNG vers. 1.0 (RFC 2083:1997)	
		XML 1.0 3rd ed:2004, W3C	
		HTML 4.01 (RFC 2854:2000)	
		PDF (Adobe Specification 5.1)	
		Rich Text Format (RTF)	
		Comma Separated Variable (CSV)	For spreadsheets
		Zip	
Network and Information Infrastructure Services			
	Directory	DNS (IETF STD 13, RFC 1034:1987+1035:1987 updated by 1101:1989, 1183:1990, 1706:1994, 1876:1996, 1982:1996, 1995:1996, 1996:1996, 2136:1997, 2137:1997, 2181:1997, 2308:1998, 2535:1999, 2845:2000, 2931:2000, 3007:2000, 3008:2000, 3090:2001, 3266:2001, 3425:2002, 3445:2002, 3597:2003, 3645:2003, 3655:2003, 3658:2003, 3755:2004, 3757:2004)	
	Transport	TCP (IETF STD 7, RFC 793:1981 updated by 3168:2001)	
		UDP (IETF STD 6, RFC 768:1980)	
	Network	IPv4 (STD 5, RFC 791:1981,	Boundary/advertised ad-

Service Area	Class	Mandatory Standard	Comments
		792:1981, 894:1984, 919:1984, 922:1984, 1112:1989 updated by RFC 950:1985, 2474:1998, 3168:2001, 3260:2002, 3376:2002)	dresses must be valid public addresses (i.e. no private addresses to be routed across boundary)
		Border Gateway Protocol (BGP4) (RFC 1771:1995)	

Table 4.1. NISP Lite

4.2. X-TMS-SMTP PROFILE

029. The following table defines military header fields to be used for SMTP messages that are gatewayed across military mail environment boundaries.

030. It specifies "X-messages" based upon RFC 2821, section "3.8.1 Header Field in Gateways". The profile specifies for each header field the name and possible values of the body.

031. The abbreviation TMS means Tactical Messaging System. The first column indicates an indication of the message property that will actually be represented by a X-TMS-SMTP field. The second and third columns specify the field names and the allowed values of the field bodies. All SMTP field values must be in uppercase

TMS message property	Field name	Field body
Subject	Subject	The Subject is a normal message property, no additional mapping is required.
Handling Name	X-TMS-HANDLING	Handling Name(s): • NO HANDLING • EYES ONLY
Classification Group + Detail	X-TMS-CLASSIFICATION	The field value will be the combination of Classification Group Displayname + Classification Detail in uppercase. Example: NATO SECRET

TMS message property	**Field name**	**Field body**
TMSStatus	X-TMS-STATUS	• NEW MESSAGE • UNTREATED • IN PROCESS • HANDLED
Mission	X-TMS-MISSIONTYPE	Type of the mission. Typical values: • OPERATION • EXERCISE • PROJECT
	X-TMS-MISSIONTITLE	Name of the Mission
	X-TMS-MISSIONDETAILS	Details of the mission. Typical values: • UMPIRE • DISTAFF • CONTROL • NO MISSION DETAILS (default) Note: This field is only used when the Mission type is set to EXERCISE.
Play	X-TMS-PLAY	This field contains either: PLAY or NO PLAY Note: This field is only used when the Mission type is set to EXERCISE.

TMS message property	**Field name**	**Field body**
UserDTG	X-TMS-USERDTG	The UserDTG element contains the DTG-formatted value entered by the user on the TMS Client or automatically set by the system (TMS).
Destinations	TO: (message data)	This is the complete list of action destinations, the SMTP session RCPT TO will dictate for which recipients the system must deliver the message to. Syntax according to RFC 2822.
	CC: (message data)	This is the complete list of info destinations, the SMTP session RCPT TO will dictate for which recipients the system must deliver the message to. Syntax according to RFC 2822.
SICs	X-TMS-SICS	List of SIC elements (separated by semicolon) selected by the user as applicable to the current message.
Precedences	X-TMS-ACTIONPRECEDENCE	Possible values: • FLASH • PRIORITY • IMMEDIATE • ROUTINE
	X-TMS-INFOPRECEDENCE	Possible values: • FLASH • PRIORITY • IMMEDIATE • ROUTINE

TMS message property	Field name	Field body
Related MessageID	X-TMS-RELATEDMESSAGEID	Used to relate TMS-, SMTP- and DSN messages

Table 4.2. X-TMS-SMTP Profile

4.3. TACOMS POST-2000 PROFILE

032. The following table defines the network and application interface, being used between participating nati ns within the NRF. It contains three different time periods (short, middle and long term), based on the modifications, based on the actual implementation and the foreseen updates within the 3 and 8 years cycle. This update cycle is in line with the cycle of the NISP.

033. These technical statements have to be extended by necessary operational regulations (e.g. necessary mapping profile for IP addresses).

034. The following Figure 4.2 describes visually this interface description, both for the network and the application part.

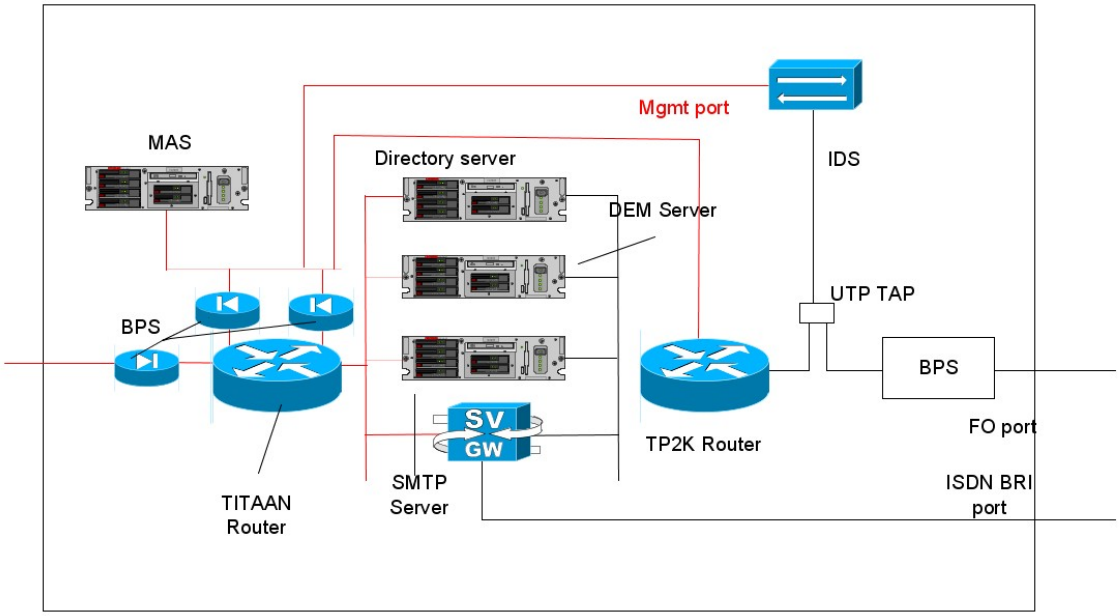

Figure 4.2. Generic TACOMS Post-2000 Profile

Protocol Layer	
Application	VoIP: ITU-T H.225, H.245, H.323 v5 Numbering Plan: Based upon TACOMS template as defined in STANAG 4643, Annex A
	VoIP: H.323v5-ISDN GW:
	MIP GW: MIP Block 2, C2IEDM 6.1.5e, Data Exchange Mechanism (mandatory), Message Exchange Mechanism (optional)
	SMTP GW: RFC 1870:1995, 2821:2001
Transport	TCP: RFC 793
	UDP: RFC 768
	RTP, RTCP: RFC 3550:2001
Network	IPv4: FC 791, 792, 2131
	Routing: static

Protocol Layer	
	IP-Addressing and Naming: Plan based upon TACOMS template as defined in STANAG 4644 Annex A
Data Link	IEEE 802.3
Physical	100BASE-FX, SC FO: ISO 9324-3

Table 4.3. NRF Profile

A. TECHNOLOGIES

035. This annex describes the technologies that are projected to be available today or in the near term period which will enable the transformation towards the NII.

A.1. DATA STRATEGY

A.1.1. Data Management Strategy

036. The ability to share information is a key factor for military success. NATO and National Information Systems have to provide the means for information exchange in any mission. The basic resource for all information systems is data, which, through the right interpretation, becomes information. As the value and cost of data increases, it becomes important that this critical resource be managed in a manner similar to other important resources. NATO Data Management will provide NATO-wide data standards and procedures for C3 requirements. The scope of NATO Data Management for C3 Systems Interoperability focuses on data architecture and data administration, and embraces the planning, organization and control of metadata, which delivers basic rules and standardized data elements (including definitions) to NATO bodies, agencies, common funded projects and is offered to national projects and programs.

037. The DMSWG is the multi-national working group in NATO, responsible to the Information Systems Sub-Committee for the development and maintenance of the NATO Data Management Policy, together with:

- Providing guidance on the coherent implementation of data management and administration across NATO,
- Establishing and operating data administration for the provision of Standard Data Elements (SDEs),
- Developing and maintaining a "NATO Data Administration Repository", which will include for example IER Registry and XML Registry functionalities, to support the provision of relevant data for information requirements.

038. The DMSWG mission is to manage the metadata of all information identified, required and authorized by NATO Tasking Authorities to support their information requirements. In particular, regarding discovery metadata, the DMSWG provides a NATO Metadata Directive and a Discovery Metadata Specification (DMS). The DMSWG mission is to manage the metadata of all information identified, required and authorized by NATO Tasking Authorities to support their information requirements. In particular, regarding discovery metadata, the DMSWG provides a NATO Metadata Directive and a Discovery Metadata Specification (DMS).

A.1.2. JC3IEDM

039. The JC3IEDM is a merger of both the LC2IEDM (Land C2 IEDM, developed by the Mulitlateral Interoperability Programme (MIP)) and the NATO Reference Data Model, which was developed by a predecessor of the DMSWG. The JC3IEDM is published under cover of STANAG 5525.

040. Since DMSWG is responsible for Data Administration not only for the JC3IEDM but also for any other Standard Information Exchange Mechanisms (Adat-P3 messages, Tactical Data Links, XML technologies, etc.) within NATO, it will also register and manage both the Standard Data Elements and the Information Exchange Requirements (IER) used in the development process of any of those mechanisms. DMSWG will as well publish Directive and Guidance documents for Data Administration in NATO.

041. As main tools for the Data Administration process, DMSWG has been tasked to develop and maintain both the NATO Metadata Registry and the NATO XML Registry. The objective is to implement them both with COTS products, if possible as a single system called NATO Metadata Repository, which would integrate both functionalities. Nowadays, the NATO IRDS (Information Resource Dictionary System) is a web-enabled tool that contains NATO Standard Data Elements in the form of a data model, but will in time need to be extended to meet selected requirements of the NATO Metadata Registry, thus becoming part of it. A version of the NATO XML Registry is currently posted under the DoD XML Registry.

A.1.3. NATO Discovery Metadata Specification (NDMS)

042. The NDMS defines discovery metadata elements for resources posted to NATO shared spaces. "Discovery" is the ability to locate data assets through a consistent and flexible search method. The NDMS specifies a set of information fields that are to be used to describe any data or service asset that is made known to NATO, and it serves as a reference for developers, system architects, and engineers by identifying a minimum set of metadata elements in support of Discovery Services. Whilst discovery of data assets is the primary use of the NDMS it is also important to note that widespread use of the metadata elements will also improve documents record management in general. The NDMS will be employed consistently throughout the organization but it is not intended or necessary for it to displace other specifications that offer different semantics.

043. To support data asset discovery, NATO has developed the NDMS as the common set of descriptive metadata elements that are to be associated with each data asset that is made visible to the enterprise discovery capability. Metadata is often defined as being "data that describes and defines other data". Data assets available in the enterprise must be described with metadata, using the elements defined in this document to permit discovery through the enterprise discovery capability. The NDMS defines a minimum set of elements that must be used to describe data assets made visible to the enterprise. Users and system agents acting on their behalf that search the enterprise will discover data assets that have been tagged and entered into catalogues or repositories that respond to search queries specified in terms of NDMS entries as depicted in the NDMS Usage Conceptual Diagram in Figure A.1.

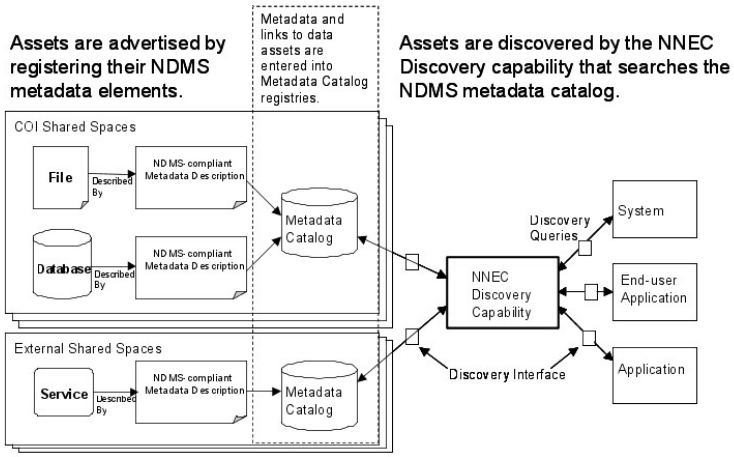

Figure A.1. NDMS Usage Conceptual Diagram

044. The elements specified in the NDMS are designed to be platform, language, and implementation independent. This allows system developers to generate and retain discovery metadata using any implementation approaches, including using COTS products. As future enterprise discovery interface specifications are defined, programs should have the appropriate discovery metadata available for their data assets and will only be required to format this metadata in accordance with the interface specifications.

A.1.4. Extensible -up Language (XML)

045. The Extensible Modelling Language (XML) is a simple, very flexible text format, much like HTML, used to structure, store and to send information. XML was designed to describe data and to focus on what data is. XML is also playing an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere.

046. Role of XML in the Web Services model is lies within communication. When one application talks to another to perform a web service, the application doing the talking must package the message it is sending in a format that is understandable by the listening application. XML is the format of the message content in this communication process.

047. The Extensible Mark-up Language tags provide information about a document's components. The Uniform Resource Identifiers contained in the XML tags expand the concept of Uniform Resource Locators (URLs) by adding IDs for objects, concepts and values that are not dependent on location.

A.2. INFORMATION MODELLING

048. The ability to share information is a key factor for military success. As such, NATO and National Information Systems have to provide the means for information exchange in all mission types. The basic resource for all information systems is data, which, through the right interpretation, becomes information, and knowledge in turn. As NNEC is considered the core theme for C3 systems within NATO transformation, a fundamental requirement is to work in the most effective manner through semantic interoperability at the data level for NATO/national C3 systems. The expanding missions of NATO involve consultation based on the sharing of information. Alliance members and partners are engaged in collective decision-making, with each nation retaining sovereignty and responsibility for its own decisions and taking action only on the basis of unanimity. In this environment, it is critically important that the Alliance members and partners have access to all shared information at the same time and that both the consultation process and the decisions taken are adequately documented. Information modelling and information management initiatives must be formalized throughout the NATO Enterprise to leverage the collective assets of NATO and national systems in support of information operations.

049. Information management is the handling of information acquired by one or many disparate sources in a way that optimizes access by all who have a share in that information or a right to that information. Information modelling establishes a conceptual schema that defines how the managed elements in an information environment are represented as a common set of objects and relationships between them. This allows multiple parties to exchange management information about these managed elements. Additionally, it provides means to actively control and manage these elements. By using a common model of information, management software can be written once and work with many implementations of the common model without complex and costly conversion operations or loss of information.

050. Appropriate Information management will enable:

- Awareness -- Products identified by metadata (keywords) and cataloged with a common schema providing a simple yet integrated query search for the right information (product);
- Access -- with information tags to define privileges; and,
- Delivery -- Assured delivery of the information product over the right network and to the right location.

051. This integrated approach to information modelling leverages the concepts of Net Centricity throughout all information resource providers and consumers in a coalition operation.

Key components of this strategy include a dissemination capability, with associated management services, that directs end-to-end information flows throughout the NII in accordance with command policy. The NISP will contibute to the core technical model for systems designers to develop new platforms capable of the intensive compilation, cataloguing, caching, distribution, and retrieval of data necessary to provide the life cycle information management and necessary information sharing across NATO members.

A.3. NETWORK INFRASTRUCTURE

A.3.1. Background

052. With the NATO Network Enabled Capability Feasibility Study (NNEC FS) a new concept of ensuring service interoperability was introduced that complements and reuses the architectural views. This concept dubbed the Interoperability Performance Parameters (IPP), inspired by the US developed concept of Key Performance Parameters (KPP), forces the system architects and designers to specify a wider context of their capabilities sufficient to allow secure service interoperability in a Federation of Systems (FOS). The interfaces at which interoperability between separate infrastructure capabilities is to be managed are called the Service Inter Operability Points (SIOP).

053. The principle is that an individual capability needs to work seamlessly with and within a FOS. The infrastructure services in a FOS and the international interoperability interfaces are described in the context of the total C4ISR systems architecture, often referred to as the Overarching Architecture (OAA).

054. This section describes the NATO General-Purpose Segment Communication System (NGCS) Reference Architecture (RA). NGCS is part of the NII, representing the NATO owned capability. It provides the communication services and associated management and security services. Also it describes the timeframe for NGCS up to 2014, first implementations are in progress.

055. The major change to classical network infrastructures is the coherence and interoperability of infrastructure capabilities brought by different coalition partners that needs to be achieved. In the NNEC FS the concept of a Maturity Model [1]was introduced to describe, qualify and quantify the different levels of infrastructure capability. Increasing levels of maturity are characterised by enhanced sets of services, performances, and support, including advances in the associated Doctrine, Organisation, Training, Materials, Personnel, Leadership, Facilities (DOTMLPF) spectrum.

056. Interoperability of separate infrastructure capabilities is managed by the earlier mentioned concept of IPP. The IPP allows a more comprehensive description and specification of those parameters that are essential for providing scalable end-to-end services over combined infrastructure capabilities.

A.3.2. NGCS 2007 Target Architecture

[1]Capability Maturity Model (CMM)

057. A reference model of the baseline network infrastructure for NGCS RA is depicted in Figure A.2. This architecture is described in the NGCS RA ed1. At the time of writing the NSIE and the NATO IP Cryptographic Equipment / Secure Access Router(NICE/SAR) had not been fielded, but the implementation projects were in progress. The BMF had been fielded.

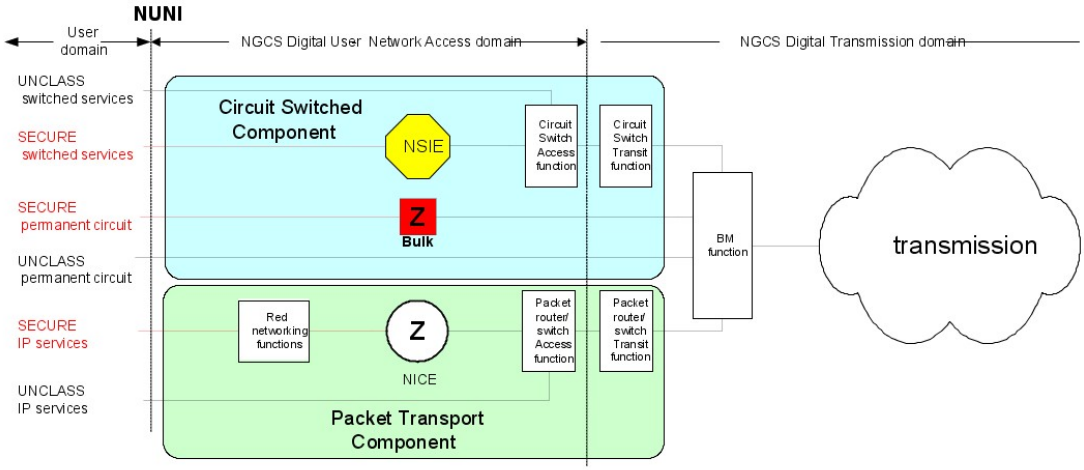

Figure A.2. NGCS Digital User-Network Access Reference Configuration

A.3.3. Communications & Networking

A.3.3.1. Internet Protocol Version 4 (IPv4)

058. Internet Protocol Version 4 (IPv4) is currently the dominant network layer protocol use in the communication between networked devices. IPv4 is a data-oriented protocol to be used on a packet switched inter-network (e.g., Ethernet). It is a best effort protocol in that it doesn't guarantee delivery. It doesn't make any guarantees on the correctness of the data; it may result in duplicated packets and/or packets out-of-order. All of these things are addressed by an upper layer protocol (e.g. UDP).

A.3.3.2. Wireless Area Network (WAN)

A.3.3.2.1. IEEE 802.11 (WiFi)

059. Many are familiar with 802.11, known as WiFi, as a short-range wireless networking protocol for home and office connections. 802.11 represent a family of wireless standards. The 802.11 series has been developed by the IEEE over the past 9 years as part of the range of communications protocols under the 802 standards series.

060. Each family member is identified by a letter suffix to the series name. Currently these letters run from "a" to "y", although there is the original 802.11 wireless standard as well. Note that there is no "l" or "x" standard. Some family members represent amendments (a, b, g, i) to the original standard, whereas some represents enhancements or extensions (c-f, h-j, n).

061. The 802.11 family of protocols share two common frequency bands, the so-called Industrial, Scientific and Medical (ISM) bands. At 2.4GHz and 5GHz, these frequencies are deregulated such that any devices complying with the Radio communications Agencies ISM conditions can operate without a radio licence. The retiring standards in this family are as follows:

062. 802.11: The original wireless standard. Developed in 1997, it had a 2 Mbps maximum air interface rate. Two versions of 802.11 were available, a frequency hopping spread spectrum (FHSS) version and a direct sequence spread spectrum (DSSS) version, both in the 2.4GHz part of the spectrum. The standard suffered limited success and poor interoperability. Status: Largely supplanted by 802.11g.

063. **802.11a**: Until recently, this was the youngest member of the family, and the fastest. Operating in the far less congested 5GHz part of the RF spectrum, 11a offers headline data rates of 54Mbps per second, although in practical application the most users will see is around 20Mbps shared. **Status**: Mature low cost products available today and are shipped in volume.

064. **802.11b**: Not only the most successful member of the family, but also the most successful wireless available, 11b has driven wireless uptake. 11b took the basic DSSS mode of 802.11 and enhanced it with additional data rates up to 11Mbps, although most users in practice will see only around a fifth of this. However, cheap adapter cards and the potential for untethered network access has driven adoption to the point where it is expected more than 20 million 802.11b network cards will be shipped in 2003. **Status**: Mature low cost products available today and are shipped in volume.

065. **802.11c**: This provides mechanisms to bridge wireless LANs together to form a single network. Using the 802.11c standard between multiple access points running across a conventional wired network, multiple access points can coordinate their operation allowing members attached to different access points to exchange data. **Status**: complete and incorporated into available access point products.

066. **802.11d**: Different countries and regions have different conditions of using the ISM frequency bands. For example, wireless devices are permitted to operate at up to 1W transmission power. However, in the end, the maximum transmission power is a comparatively mea-

gre 100mW, thus significantly restricting the range and performance of wireless LANs. The 11d standard was drafted to ensure products were produced that conformed to the local license conditions in each country and region. Primarily effects countries with regulatory standards that are outside of those used by the U.S. **Status**: Standard ratified in 2001.

067. **802.11e**: Whilst the current 802.11 standards family can support voice and video communications, the quality of these exchanges rapidly deteriorates if the network is being heavily used. 802.11e introduces the concept of prioritisation to allow time sensitive information like voice and video data to be sent to users before other data, such as emails and web pages. This will significantly improve the ability of 802.11a, b and g networks to deliver voice and video services, and as proposed will be compatible with existing 802.11 standards and products. **Status**: Ratified in 2005. New products expected mid-2007. Firmware upgrades will be available for existing products.

068. **802.11f**: When developing the 802.11 standards, some features were purposefully omitted from the standard to promote differentiation between products. Inter-access point roaming was one such feature that allows end user devices to talk to different access points as they moved physically through a network. However it was soon realized that not standardizing this meant potential interoperability problems between different vendors' equipment; thus the 802.11f standard has been developed to facilitate an interoperable access point roaming capability. Status: Few products supporting 11f available; security issues and dismissal by vendors has lead to the standard being withdrawn.

069. **802.11g**: The latest member of the family to see products appearing, although the standard is still to be ratified. 11g introduce the same modulation and air interface schemes as 11a, but in the 2.4GHz ISM band. Thus 2.4GHz devices can now enjoy the same data rates (up to 54Mbps, although 20Mbps is more realistic) as 802.11a, although the available number of channels is restricted. Backwards compatible with 11b, there is some concern about the achievable data rates in mixed-mode 11b and 11g networks. **Status**: Standard ratified in 2003. Products are mature and will soon overtake 11b as the most popular standard within the family.

070. **802.11h**: Regulators have mandated that wireless devices operating in the 5GHz ISM band must be polite to one another, and to other users of the spectrum. It is interesting to note though that this has meant the network cards available are common to all countries and regions and it is the network card driver that manages the radio resources to comply with local licence conditions. This has resulted in many European users using US drivers for their wireless cards because of improved range.5GHz spectrum. This means they should detect other networks operating in the same frequencies and try to avoid them. 11h introduces Dynamic Frequency Selection to enable wireless devices to avoid already used frequencies automatically and Transmission Power Control to restrict the transmit power of devices to just that required to maintain the communications. **Status**: Ratified in 2004.

071. **802.11i**: The IEEE has developed stronger security mechanisms under the 802.11i banner. Based on the 802.1x, Port Based Security mechanisms and introducing the significantly more advanced and stronger (Advanced Encryption Standard) cryptographic algorithm, 11i should provide much greater levels of protection than the previous standard, WEP. **Status**: Ratified in 2004. Products are coming to market.

072. **802.11j**: Important for , because they have authorised a slightly different frequency for 802.11 (4.9-5.0 GHz). This standard brings to the Japanese authorised bands. **Status**: Ratified in 2004. Products are available in Japanese market.

Standard	Description	Status
IEEE 802.11	The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard	Approved 1997
IEEE 802.11a	54 Mbit/s, 5 GHz standard	Approved 1999
IEEE 802.11b	Enhancements to 802.11 to support 5.5 and 11 Mbit/s	Approved 1999
IEEE 802.11d	International (country-to-country) roaming extensions	Approved 2001
IEEE 802.11e	Enhancements: QoS, including packet bursting	Approved 2005
IEEE 802.11f	Inter-Access Point Protocol (IAPP)	Withdrawn 2006

Table A.1. 802.11x Summary

A.3.4. Construction of a robust IP-network infrastructure

073. Operational relevant service availability should be one of the main design criteria and operational evaluation criteria for the NGCS. Despite the migration of users onto a single network and the introduction of significant additional complexity, e.g. QoS, the service availability has to be improved. Service availability and performance are exponents of infrastructure, organization, human aspects and others. The assessment of operational service readiness and performance is a structural activity required in the NGCS product life-cycle management. It should give input to transformational processes and for the development of Target Architectures (TA) that underpin infrastructure investment projects.

A.3.4.1. NGCS Overview

074. The NATO General Purpose Communications System (NGCS) has a Circuit Switched

Component (CSC) and a Packet Transport Component (PTC). The services offered are presented at the NGCS User Network Interface (NUNI). The NGCS user-network access domain incorporates functions for user access of circuit switched functions and packet transport functions. The circuit switched component provides on-demand switched access and also access to semi-permanent circuits. Both can be provided either in secure or non-secure modes. The packet transport component provides for both secure and non-secure IP access services.

075. A secure service offered by the network at the NUNI provides for interconnection within a single security domain. If telecommunication services are required for a second security domain, this is implemented by installation of another cryptographic device - e.g. NATO Secure ISDN Equipment (NSIE) offering bulk encryption or NATO IP Cryptographic Equipment (NICE) (with the associated RED networking functions). In order to provide greater throughput, more than one instance of this might exist for a single security domain.

076. In mid-term, a complete migration to a fully IP based network is planned for the NGCS.

A.3.4.2. Definition and implementation of a QoS architecture

077. In the public standardization bodies, e.g. IETF, ITU, ETSI, ANSI, many initiatives are ongoing regarding the specification of a global QoS architecture in support of network convergence. Likewise many government organizations are doing the same.

078. The operation and control of QoS enabled IP-services requires many new Operation and Support Systems as well as a thorough reassessment of the management organization.

079. The complexity and the novelty of IP QoS warrant a step-by-step introduction. The entities affected by the introduction are:

- The end-user;
- The applications;
- The infrastructure;
- The OSS/BSS;
- The policies;
- The third party providers, e.g. SP, NDN;

080. The introduction should follow the developments in the commercial sector, and each successive introduction step in NATO should be done when the technology is stable and mature. Nevertheless NATO may want to implement additional functionality like additional CoS to implement MLPP, but this always be based on an underlying commercial standard based QoS architecture. Eventually the QoS architecture must take account of the requirements in military tactical radio networks and future QoS enabled MANETs. It is envisaged however

that commercial standards for wireless MANETs will be developed among others by the ZigBee Alliance

081. The model of spiral development should be applied. Each step is first tested in the laboratory (applications, infrastructure and OSS/BSS), evaluated against user requirements, operational issues, architectural principles, before it is gradually rolled out in the operational network.

082. Business cases for network convergence are becoming increasingly viable. As more and more services are uniquely available on IP and standardization for IP based service support is becoming mature, it becomes more cost effective to migrate an existing infrastructure based on TDM and IP bearers to a single IP-bearer service system. However, network convergence does not come for free. Following items and activities are required:

- Specification of a comprehensive set of Classes of Service (CoS) for the ultimate network, which can be initially collapsed to a basic set and further expanded with each implementation step.
- Definition of application mapping to telecommunications services (the CoS).
- Specification of CoS handling in the network
- NATO policy with the objective to have uniform QoS handling in the multinational network.
- Supporting management and control systems (NGOSS compliant) that need to be integrated in the total SLM complex.
- Proof of concept testing.

A.3.4.3. The migration of applications onto an IP-bearer

083. All the applications that are often traditionally carried on the CSC, i.e. telephony, switched VTC, leased line (for real-time data, for bandwidth pipe) need to be adapted so that they can also perform on an IP-bearer. Most of the applications require an QoS enabled IP infrastructure. In addition the connection oriented application services require call signalling, DNS, directory (for the gatekeeper) and resource reservation functionality. This infrastructure should be provided as a common core functionality for all application services requiring it. Target architectures for VoIP (SVoIP and VoSIP) and VTCoIP therefore need to be coordinated. For interoperability purposes NATO needs to standardize the signalling at the respective Service Interoperability Points.

A.3.4.4. Transition to IPv6

084. IPv6 is an enabler for establishing coalition wide connectivity in a network enabled NII. The transition strategy of the NATO CIS to IPv6 is described in [TN1088] [2]from which the

top-level roadmap is repeated here in Figure A.3.

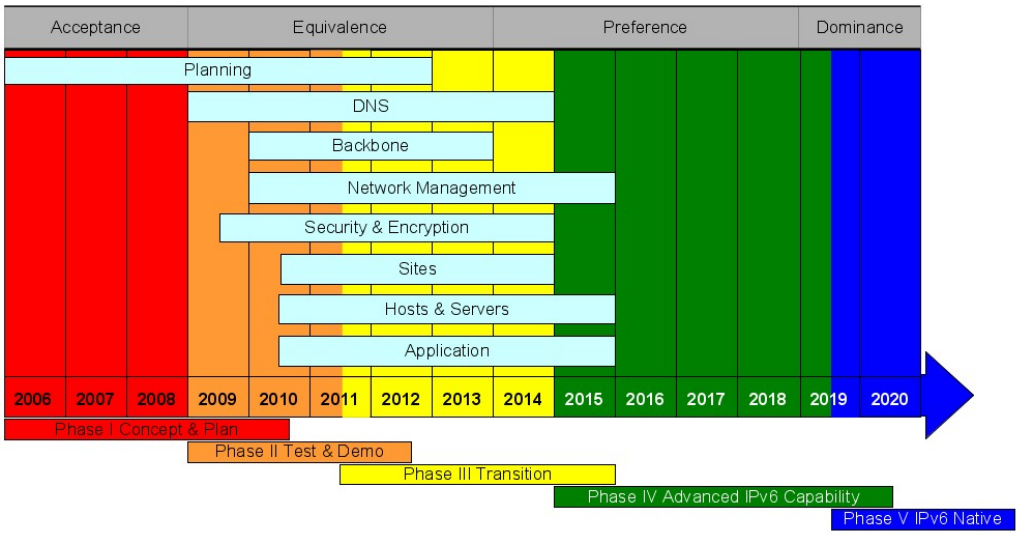

Figure A.3. Roadmap to IPv6

A.4. PLATFORM ORIENTED COMPUTING

085. This section contains the description of the reference models, more specific the NCOE Component Model (NCM), associated with basic functional configurations. Although these Functional Configurations (FC) are not for future systems, they still describe the reality of today's system implementation. Ten baseline FCs have been identified which can each be extended with additional functionality. For a number of FCs a refinement has been made in terms of functionality provided.

A.4.1. User Terminal/Device

086. User Terminals/Devices are appropriate for a large community of NATO users that require light office applications such as email, office automation, browsing capability to view Intranet documents and possibly some specific business applications. The User Terminal is considered a light client station with an embedded operating system, a browser and a virtual

[2]Derived from Technical Note 1088: NATO IPv6 Transition Plan, Preliminary Version, NC3A, June 2006

machine. Devices can be PDAs, or WAP phones. Applications are downloaded from the internal Communications server or the Webportal. User Terminals/Devices are appropriate for a large community of NATO users that require light office applications such as email, office automation, browsing capability to view Intranet documents and possibly some specific business applications.

087. The following options can be provided when required:

- Multi-point Applications,
- DBMS Services,
- Distributed Applications like e.g. Workflow and Alert services.

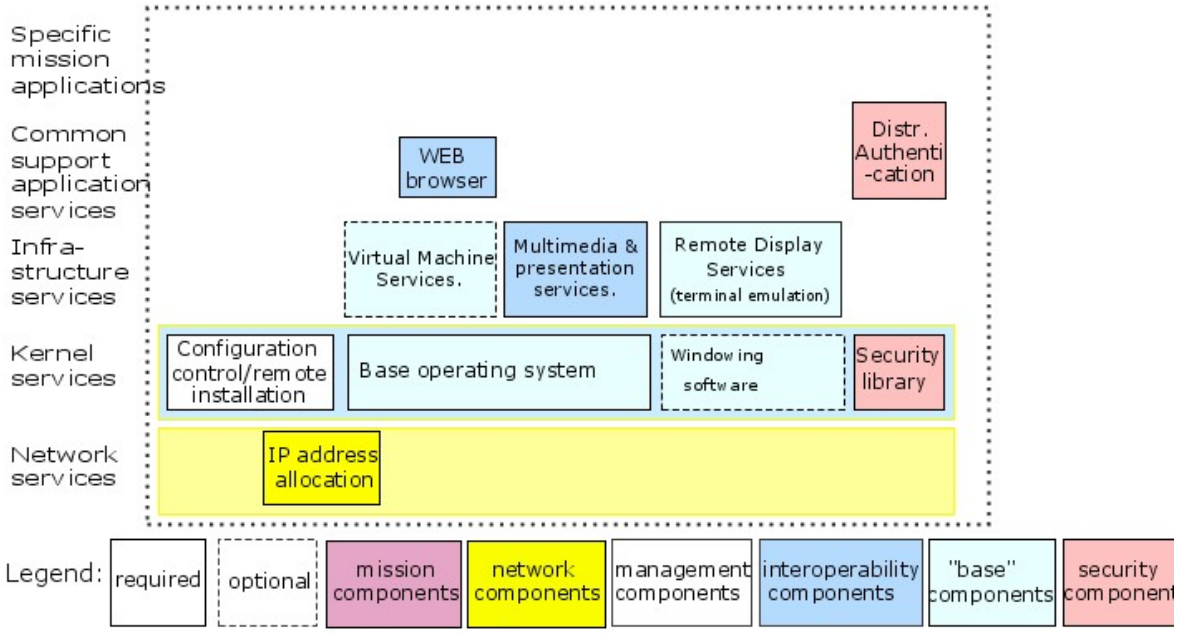

Figure A.4. Functional Components for User Terminal/Device

A.4.2. User Workstation

088. User Workstations are appropriate for users that require heavy applications that are

stored locally to improve response times. This can be a MMHS Client Workstation, a GIS Workstation, a Data Provider Workstation or a laptop. They offer full Office Automation and Formal Military Messaging capabilities with optional functionality as required. Client Network Management Services are considered part of the Operating System. GIS and personal DBMS are optional services for data providers. Data consumers access GIS and data through their browser and data access services respectively. File encryption is an optional feature for user workstations, but very appropriate for mobile users, using laptops. The optional collaborative or multi-point tools are near real-time applications, comprising audio and video conferencing, briefings, real-time chat, white-boarding, and application sharing.

089. The following options are considered:

- Map Overlay and GIS Services,
- Multi-point Applications including VTC,
- Security Management such as PKI,
- Common Information Exchange,
- Distributed Applications like e.g. Workflow and Alert services.

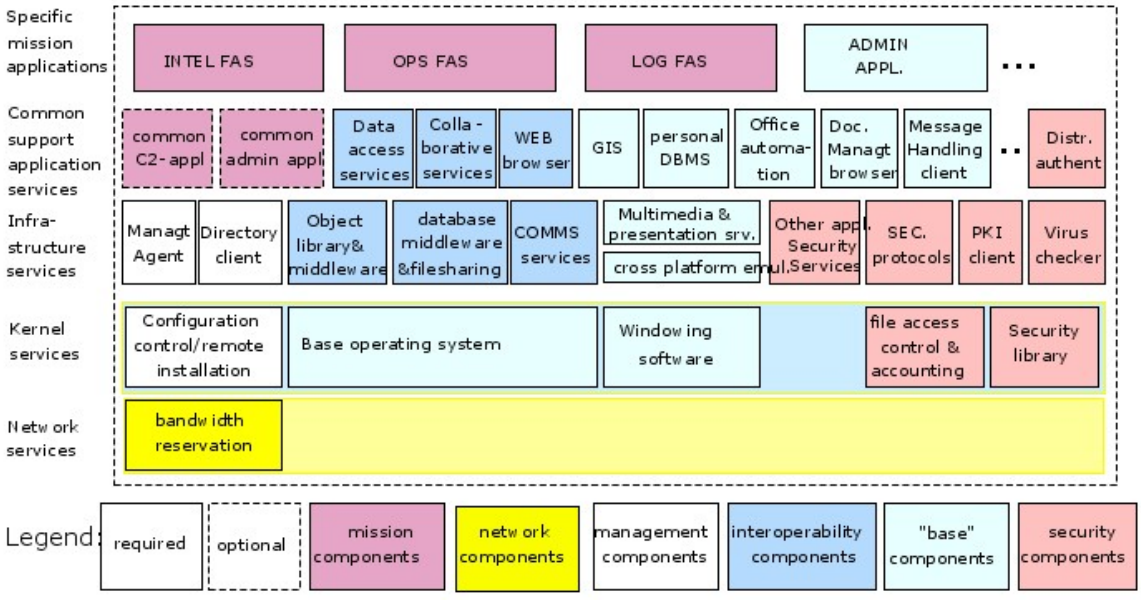

Figure A.5. Functional Components for User Workstation

090. A possible simplification of a User Workstation is an End User Device, which may be appropriate for a large community of NATO users that require light office applications such as e-mail, office automation, browsing capability to view Intranet documents and possibly some specific business applications.

A.4.3. Administration Workstation

091. Administration Workstations are appropriate for system, network, and security administrators. In addition to the User Workstation functionality they offer system administration and full systems and network management services.

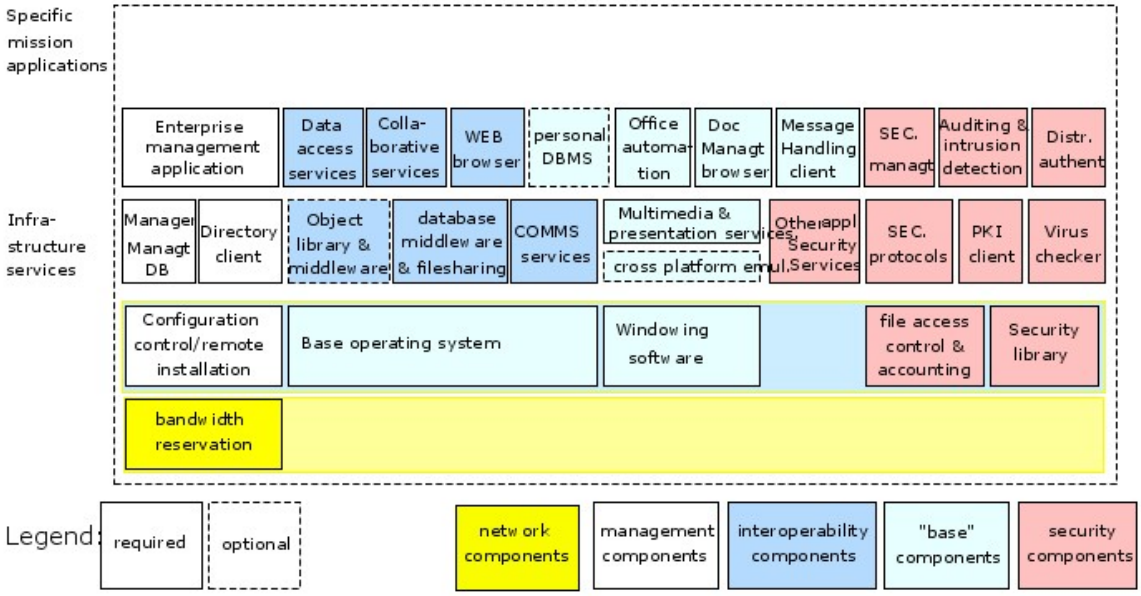

Figure A.6. Functional Components for Administration Workstation

A.4.4. Network Server

092. The Network Server is used for communication with the external WAN and for providing internal LAN services, such as downloading applications to user terminals. Within NATO a strategic choice for the Windows 2000 platform has been made for all network servers.

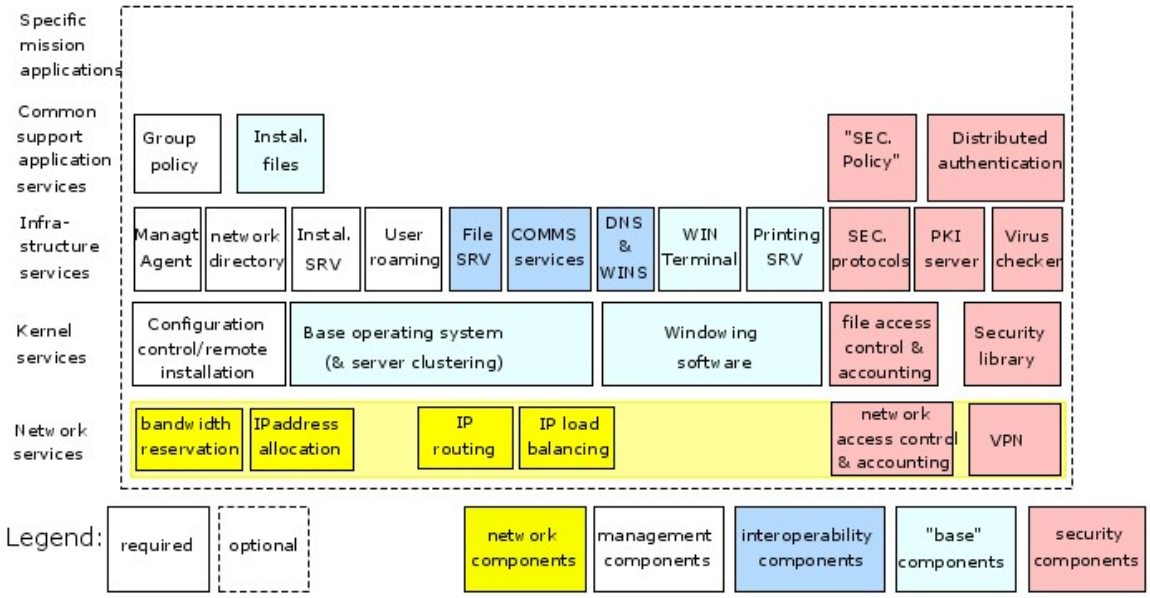

Figure A.7. Functional Components for Network Server

A.4.5. Communications and Messaging Server

093. The communications and messaging server provides all formal and informal mail services and interface with ACP 127 networks.

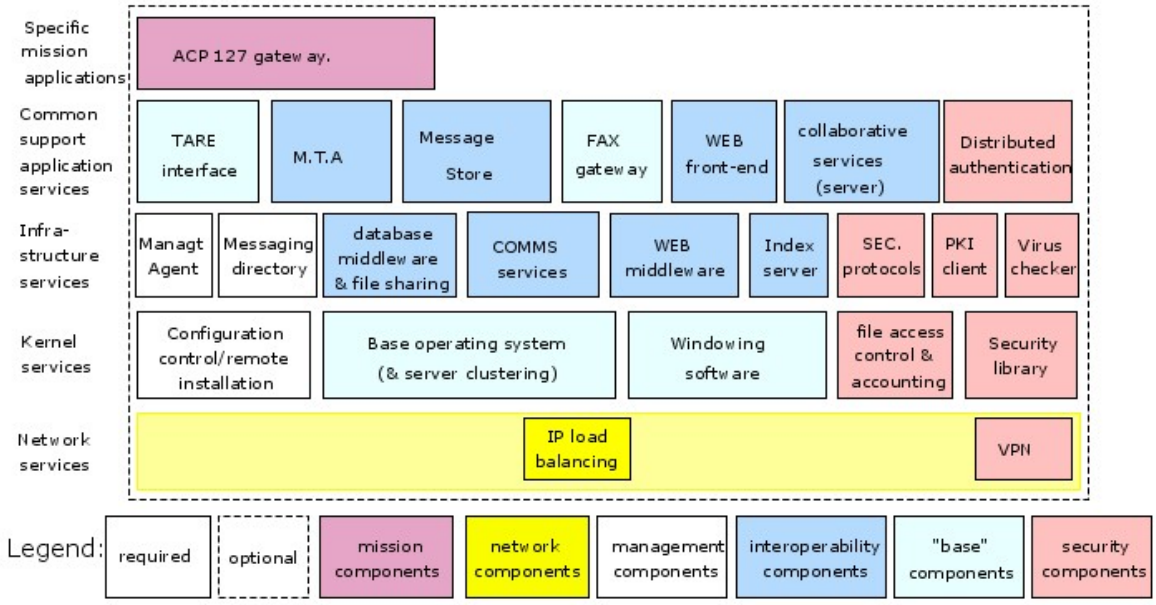

Figure A.8. Functional Components for Communications and Messaging Server

A.4.6. Document Management Server

094. The document management server provides the document storage and retrieval engine and hosts workflow applications. Also collaborative tools are hosted on the document management server because they support the workflow applications.

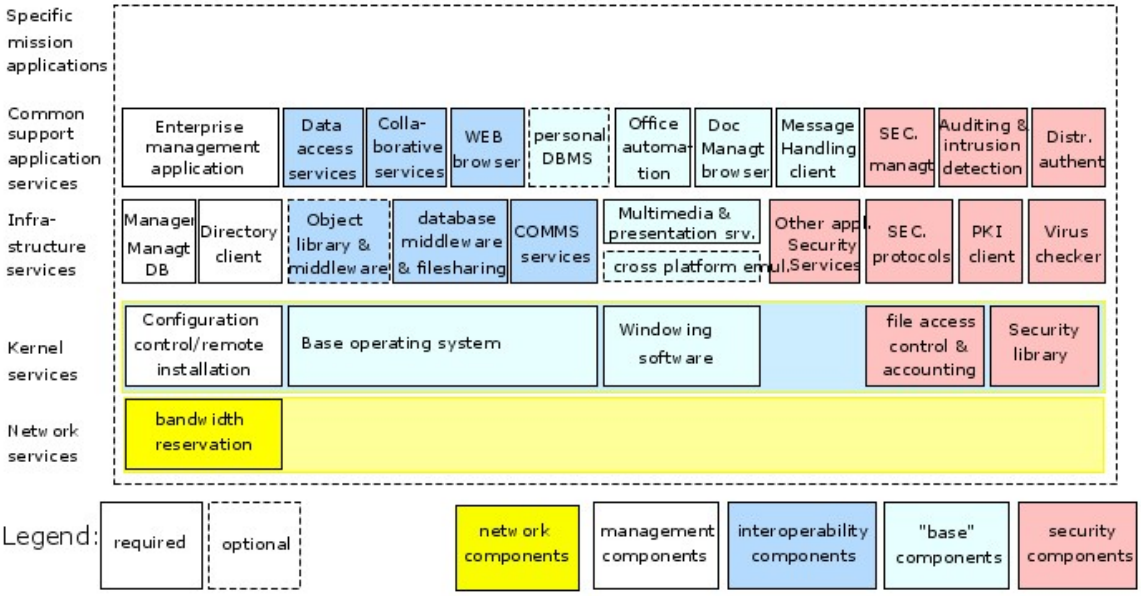

Figure A.9. Functional Components for Document Management Server

A.4.7. Web Portal/Application Server

095. The web portal/application server provides the access to intranet and Internet services. It optionally contains GIS and MHS components to provide geographic mapping and messaging services.

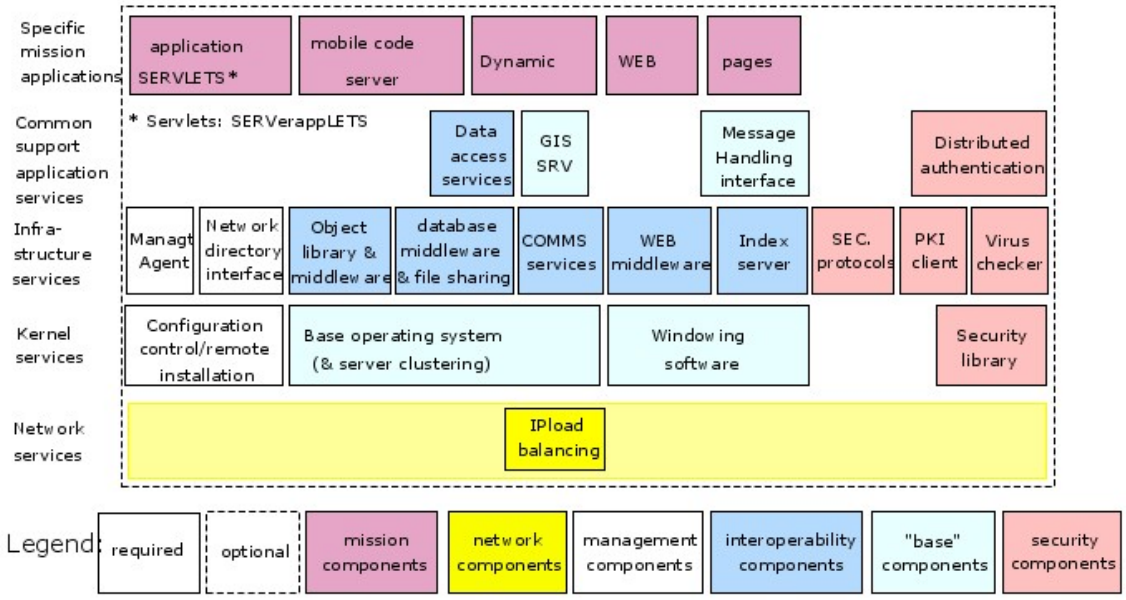

Figure A.10. Functional Components for Web Portal/Application Server

A.4.8. Database Application Server

096. The database application server provides the access to local database services. It optionally contains spatial services to provide storage and retrieval of geographic maps.

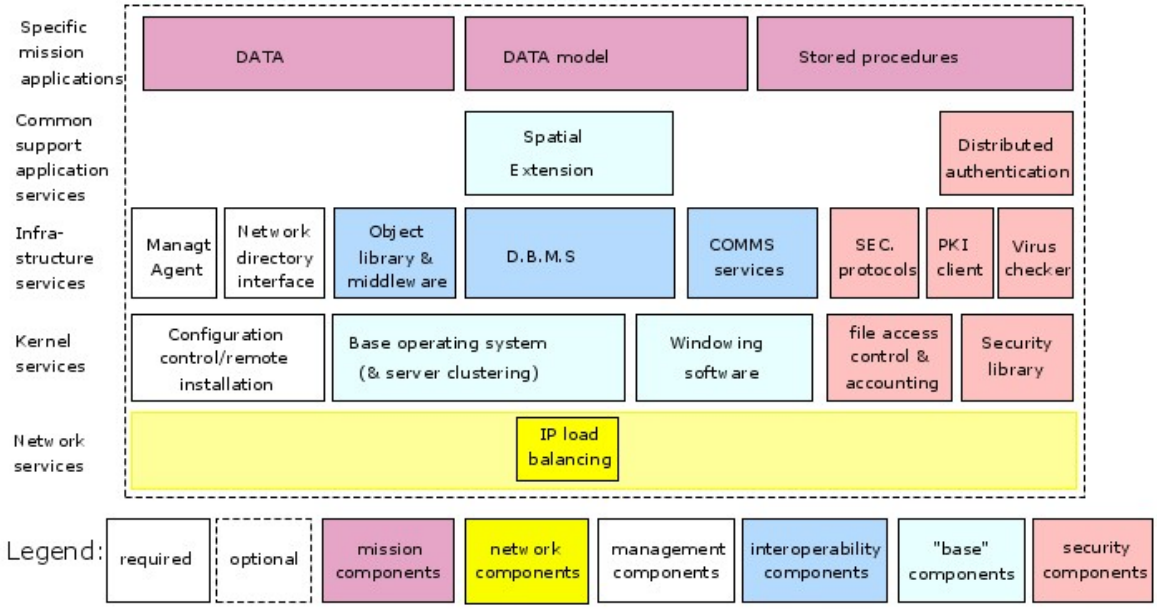

Figure A.11. Functional Components for Database Application Server

A.4.9. Directory Server

097. The directory server offers central information support for users/systems through the provision of standardised information contents in the form of objects, e.g. for the support of addressing within messaging systems and the storage of certificates/CRLs within PKI.

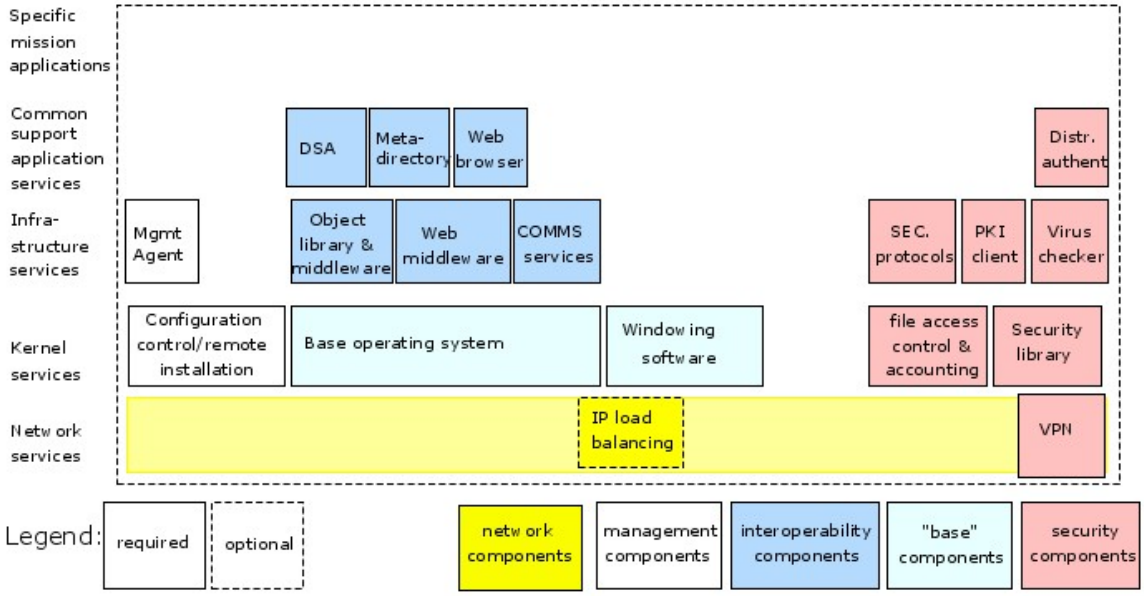

Figure A.12. Functional Components for Directory Server

A.4.10. Imagery Server

098. The imagery server offers data exchange interoperability between NATO reconnaissance and surveillance assets levels of interoperability. The main focus is on the imagery interfaces between airborne and surface-based elements and between the output of the surface-based elements and the rest of the imagery community.

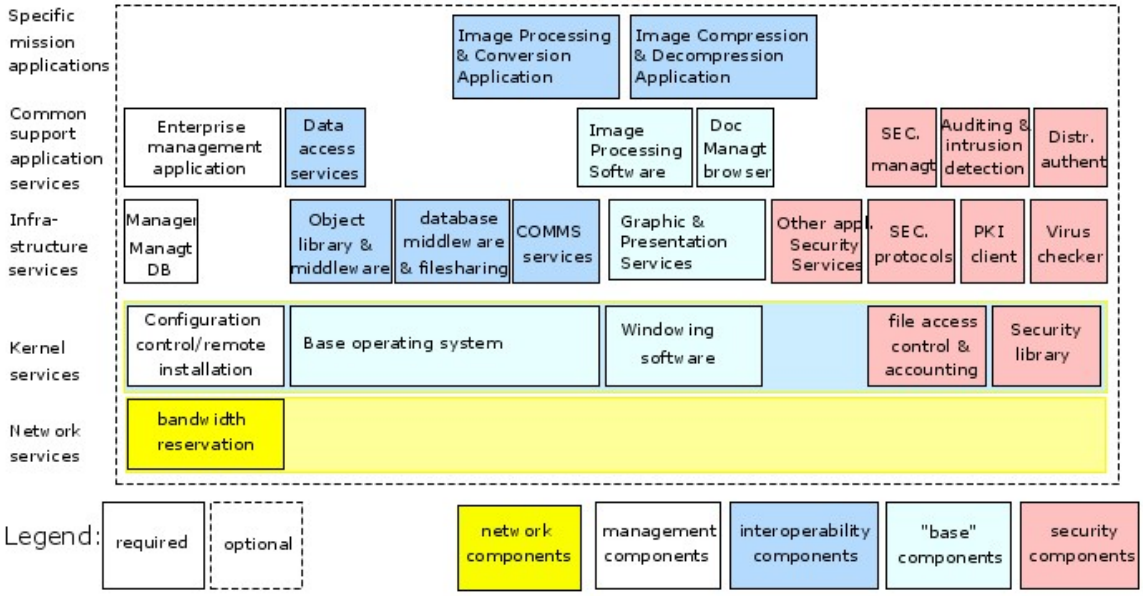

Figure A.13. Functional Components for Imagery Server

Index

A

Adobe Systems Incorporated
- EPS , 33
- ISBN 0 200 175839 3, 33
- PDF v. 1.4, 33
- Postscript (level I and II), 33

ATM-Forum
- af-lane-0084.000, af-lane-0112.000, 73
- af-pnni-0055.000, 72
- af-sig-0061.000, 72

C

Combined Communications and Electronic Board
- ACP 123A, 19, 19
- ACP 133, 26
- ACP 145, 16
- ACP 190(B), 81
- ACP 200, 71
- ACP 220, 21
- ACP145, 16

D

DoD
- MIL-STD 188-110A, 83
- MIL-STD 188-136, 79
- MIL-STD 188-140A, 81
- MIL-STD 188-141A, 81
- MIL-STD 188-145, 82
- MIL-STD 188-164, 75, 77
- MIL-STD 188-165, 77
- MIL-STD 188-181B, 75
- MIL-STD 188-182A , 75
- MIL-STD 188-183D, 76
- MIL-STD 188-184, 76
- MIL-STD 188-185, 76
- MIL-STD 188-1852D, 77
- MIL-STD 188-242, 82
- MIL-STD 188-243, 82
- MIL-STD 2401, 46
- MIL-STD 2525B, 47, 47
- MIL-STD 6011C, 32, 73
- MIL-STD 6016C, 33, 33
- MIL-STD 6040, 43
- OTH-T, 43
- STE, 42

E

EBXML
- ebTA, 44, 55

ECMA
- ECMA-262, 52

Electronic Industries Association
- RS-232, 84
- RS-422/423, 84
- RS-530, 84
- TIA/EIA-492000-A, 84

EUROCOM Specifications
- D/0, 29

European Telecommunication Standardisation Institute
- EN 300 961, 29
- EN 300 969, 29

I

IEEE
- 1278.1a , 59
- P1278, 59
- P1278.1a, 59
- P1278.2, 59
- P1278.3, 59

IETF
- RFC 1034, 61
- RFC 1035, 61
- RFC 1212, 23
- RFC 1213, 23
- RFC 1305, 28
- RFC 1332, 70
- RFC 1519, 67
- RFC 1570, 70
- RFC 1643, 24
- RFC 1661, 70
- RFC 1724, 24, 67
- RFC 1771, 66
- RFC 1772, 66
- RFC 1812, 65
- RFC 1823, 26
- RFC 1850, 24
- RFC 1869, 19
- RFC 1870, 19
- RFC 1883, 74
- RFC 1939, 19

RFC 1951, 52
RFC 1952, 52
RFC 1990, 70
RFC 1994, 70
RFC 2045, 54
RFC 2046, 54
RFC 2047, 54
RFC 2048, 54
RFC 2049, 54
RFC 2058, 10
RFC 2083, 42
RFC 2126, 74
RFC 2131, 65
RFC 2132, 65
RFC 2251, 26
RFC 2252, 26
RFC 2253, 26
RFC 2254, 26
RFC 2255, 26
RFC 2256, 26
RFC 2328, 66
RFC 2362, 66
RFC 2401, 12
RFC 2402, 12
RFC 2403, 12
RFC 2404, 12
RFC 2405, 12
RFC 2406, 12
RFC 2407, 12
RFC 2408, 12
RFC 2409, 12
RFC 2410, 12
RFC 2412, 12
RFC 2453, 66
RFC 2474, 65
RFC 2616, 28
RFC 2632, 16
RFC 2633, 16
RFC 2790, 24
RFC 2819, 24
RFC 2821, 19
RFC 2849, 27
RFC 3022, 67
RFC 3232, 61
RFC 3344, 68
RFC 3411, 22, 22, 23, 23, 23
RFC 3412, 22, 22, 23, 23, 23
RFC 3413, 22, 22, 23, 23, 23
RFC 3414, 22, 22, 23, 23, 23
RFC 3415, 22, 22, 23, 23, 23
RFC 3501, 20
RFC 3768, 10
RFC 3977, 28
RFC 4346, 12
RFC 768, 74
RFC 791, 62, 74
RFC 854, 28
RFC 855, 28
RFC 951, 64, 64
RFC 959, 28
S/MIME Version 3 ESS, 11, 12
STD 89, 64
International Hydrographic Organisation
S-57, 48, 48
ISO
19107, 38
19109, 38
19110, 39
19112, 39
19115, 46
19117, 48
19125-1, 40
19125-2, 40
4217, 51
8601, 53
8879, 34
9735, 44
9735-1, 44
9735-10, 44
9735-2, 44
9735-3, 44
9735-4, 44
9735-5, 44
9735-6, 44
9735-7, 44
9735-8, 44
9735-9, 44
ISO 19128, 49
ISO/IEC
10646, 53
10918-4, 32
11172, 28
11172-1, 28
11172-2, 28
11172-3, 28, 29
11172-4, 28

11172-5, 28
12087-5, 31
13818, 29
13818-1, 29
13818-10, 29
13818-11, 29
13818-2, 29
13818-3, 29
13818-4, 29
13818-6, 29
13818-7, 29
13818-9, 29
14443, 15
14443-1, 15
14443-2, 15
14443-3, 15
14496, 29
14496-1, 29
14496-10, 29
14496-11, 29
14496-12, 29
14496-13, 29
14496-14, 29
14496-15, 29
14496-16, 29
14496-17, 29
14496-18, 29
14496-19, 29
14496-2, 29
14496-20, 29
14496-21, 29
14496-22, 29
14496-3, 29
14496-4, 29
14496-5, 29
14496-6, 29
14496-7, 29
14496-8, 29
14496-9, 29
15408, 10
15408-1, 10
15408-2, 10
15408-3, 10
15416, 53
15417, 53
15444, 42
15444-1, 42
15444-11, 42
15444-12, 42
15444-2, 42
15444-3, 42
15444-4, 42
15444-5, 42
15444-6, 42
15444-8, 42
15444-9, 42
19757-2, 35
26300, 34
646, 33, 52
7810, 15
7812, 15
7812-1, 15
7812-2, 15
7816, 15
7816-1, 15
7816-2, 15
7816-3, 15
7816-4, 15
7816-5, 15
8802-3, 75
8859, 52
8859-1, 52
8859-10, 52
8859-13, 52
8859-14, 52
8859-15, 52
8859-16, 52
8859-2, 52
8859-3, 52
8859-4, 52
8859-5, 52
8859-6, 52
8859-7, 52
8859-8, 52
8859-9, 52
9075, 37, 37
9075-1, 37, 37
9075-10, 37, 37
9075-13, 37, 37
9075-2, 37, 37
9075-3, 37, 37
9075-4, 37, 37
9075-5, 37, 37
9075-9, 37, 37
9594, 27, 27
9594-8, 11

9636, 51
9636-1, 51
9636-2, 51
9636-3, 51
9636-4, 51
9636-5, 51
9636-6, 51
DIS 9660, 29
FCD 18023-1, 47
FCD 18025, 47
TR 13818-5, 29
WD 18026, 47
ITU-T, 72, 72
G.726, 29
H.248.1, 21
H.320, 21
H.323, 21
T.120, 21, 21
T.30, 42
T.4, 42
T.6, 42
V.42, 72, 72
V.90, 72, 72
X.25, 71
X.519, 26

M

Microsoft, 34, 34, 37, 74
Application Note GC0165, 33
ISBN-1-55615-802-5, 57, 58
ISBN-1-55615-804-1, 57, 58

N

NATO
ACP 190(B) NATO Supp 1A, 81
ACP 190(B) NATO Supp 2, 81
APP-11, 43, 43, 43
MIL-STD 6020, 73
STANAG 1059, 52
STANAG 2019, 48
STANAG 2211, ed. 6, 47
STANAG 3675 ed.2, 48
STANAG 3764, 32
STANAG 3809, 45
STANAG 4175 ed.3, 73, 83
STANAG 4197 ed.1, 82
STANAG 4198, 29
STANAG 4203, 82
STANAG 4204 ed.2, 82
STANAG 4205, 82
STANAG 4206 ed.3, 71
STANAG 4231 ed.4, 76
STANAG 4233, 77
STANAG 4246 ed.2, 83
STANAG 4285, 83
STANAG 4329, 53
STANAG 4372 ed.3, 73
STANAG 4376 ed.1, 78
STANAG 4406, 16, 18
STANAG 4444 ed.1 (Draft), 29
STANAG 4479 ed.1, 30
STANAG 4484 ed.2, 78
STANAG 4485 ed.1, 78
STANAG 4486 ed.2, 79
STANAG 4522 ed.1, 80
STANAG 4539, 83
STANAG 4545 ed.1, 31
STANAG 4559 ed. 1, 31
STANAG 4575 ed. 2, 31
STANAG 4578 ed.1, 71
STANAG 4586, 74
STANAG 4607 ed.1, 31
STANAG 4609 ed.1, 31
STANAG 4609 ed.2, 31
STANAG 5000, 42
STANAG 5066, 83
STANAG 5500, 43
STANAG 5511 Ed.5, 32, 73
STANAG 5516 (Edition 3), 32
STANAG 5522, J-Series, 33
STANAG 5523, 36
STANAG 5525 ed.1, 41, 41
STANAG 5527, 6
STANAG 5602 ed.2, 30
STANAG 5616 ed.3, 73
STANAG 7023 ed.3, 31
STANAG 7024 ed.2, 32
STANAG 7074, 44
STANAG 7085 ed.2, 73
STANAG 7170, 47
WP14-3_Ed5.0_20020318.pdf, 37
NIMA
MIL-PRF 89005, 46
NIST
FIPS 180-2 with Change Notice 1, 14
FIPS 186-2 with Change Notice 1, 12

FIPS PUB 197, 11
FS 1016, 30

O

OASIS, 35, 35, 35, 35
DataStructure_v2, 55
Operators_v2, 55
ProgrammersAPI_v2, 55
Replication_v2, 55
SAML 1.1, 15
uddi_v2.xsd, 55
uddi_v2custody.xsd, 55
uddi_v2replication.xsd, 55
ODMG
ISBN 1-55860-647-5, 37
OMG
formal/03-03-01, 51
Open GIS Consortium
OGC 01-024r1, 51
OGC 02-065r6, 49
OGC 02-087r3, 51
OGC 03-081r2, 50
OGC 04-024, 49
OGC 04-038r1, 51
OGC 04-094, 49
OGC 05-047r2, 50
Open GIS Forum (OGIS)
OGC 01-029, 45
OpenGL
glspec14, 51

P

PS/SC Working Group, 15
PCSC_Part_1, 15
PCSC_Part_2, 15
PCSC_Part_3, 15
PCSC_Part_4, 15
PCSC_Part_5, 15
PCSC_Part_6, 15
PCSC_Part_7, 15
PCSC_Part_8, 15

R

RSA
PKCS#1 v2.1, 13

S

SUN Microsystems
java_card_kit-2_2_1-fr-spec, 15
JSR 221, 37

T

The Open Group
T525, 57, 57, 58

W

W3C, 34, 34, 34, 34, 34, 34, 34, 34
NOTE-wsdl-20010315, 55
REC-html401-19991224, 34
REC-soap12-part0-20030624, 56
REC-soap12-part1-20030624, 56
REC-soap12-part2-20030624, 56
REC-soap12-testcollection-20030624, 56
REC-SVGMobile-20030114, 41
REC-WebCGM-20011217, 41
REC-xhtml1-20020801, 34
REC-xlink-20010627, 35
REC-xml-20040204, 34
REC-xml-infoset-20011024, 35
REC-xml-names-19990114, 35
REC-xml-stylesheet-19990629, 35
REC-xmlbase-20010627, 35
REC-xmlschema-0-20010502, 36, 36, 36
REC-xpath-19991119, 55
REC-xptr-element-20030325, 35
REC-xptr-framework-20030325, 35
REC-xptr-xmlns-20030325, 35
REC-xsl-20011015, 36
REC-xslt-19991116, 36
WD-SVG12-20050413, 41
WAP Forum
WAP-238-WML-20010911-a, 36
Web Services Interoperability Organisation
ws-i, 56, 56, 56, 56

X

X Consortium
X11R6.6, 56, 58