Allied Data Publication 34

(ADatP-34(J))

NATO Interoperability Standards and Profiles

Volume 3

The Afghanistan Mission Network (AMN) Profile of NATO Interoperability Standards

DECEMBER 2016

NCI Agency

Table of Contents

This page is intentionally left blank

1. THE AFGHANISTAN MISSION NETWORK (AMN) PROFILE OF NATO INTEROPERABILITY STANDARDS

1.1. GENERAL

001. NATO, through its interoperability directive, has recognized that widespread interoperability is a key component in achieving effective and efficient operations. In many of the operations world-wide in which the military of the NATO nations are engaged, they participate together with a wide variety of the military of other nations and non-military organizations on the ground. The NATO Interoperability Standards and Profile (NISP) provides the necessary guidance and technical components to support project implementations and transition to NATO Network Enabled Capability (NNEC).

1.1.1. Authorised Version

002. The standards extant for the AMN are described in the NISP. This is published as ADatP-34 by the NATO C3 Board. As part of the NISP, an AMN Profile of NATO Interoperability Standards has been published among the several operational profiles permitted as part of ADatP-34. These are the extant and NATO agreed list of practical standards to achieve immediately usable interoperability between the national network extensions of the NATO nations, coalition partners and NATO provided capabilities.

003. Nations participating in the AMN have agreed to comply with the AMN joining instructions, of which these standards form an integral part.

1.1.2. Application

004. The AMN Profile will be used in the implementation of NATO Common Funded Systems. Nations participating in AMN agree to use this profile at Network Interconnection Points (NIPs) and at other Service Interoperability Points as applicable.

005. NNEC Services must be able to function in a network environment containing firewalls and various routing and filtering schemes; therefore, developers must use standard and well-known ports wherever possible, and document non-standard ports as part of their service interface. Service developers must assume network behaviour and performance consistent with the existing limits of these networks, taking bandwidth limitations and potentially unreliable networks into account.

1.1.3. Life-Cycle of Standards

006. ADatP-34 defines four stages within the life-cycle of a standard: **emerging, mandatory, fading and retired**[1]. In those situations where multiple stages are mentioned, the AMN Profile

[1]The FMN Profile has been further refined and also additionally uses 4 obligation categories of Mandatory, Conditional, Recommended and Optional to assist with conformity assessments. Where relevant these have also been used in an AMN context.

recommends dates by which the transition to the next stage is to be completed by all AMN members. If a TCN (or NCI Agency) decides to implement emerging standards it is her responsibility to maintain backwards compatibility to the mandatory standard.

1.1.4. Forthcoming/Agreed Changes

1.1.4.1. Indicating Changes to the AMN Profile

007. The AMN Profile is managed within volume 4 of the Joining, Membership and Exit Instructions (JMEI) (i.e. Vol 4 of the JMEI as currently published as NCI Agency Technical Report TR-2013/ACO008868/04). This document is oriented around the AMN Profile of NATO Interoperability Standards.

008. All changes proposed to this profile must be via the process outlined at section 2.7 of the JMEI Volume 4. All changes are to be first collectively agreed via the AMN Architecture Working Group (AWG). The NCI Agency acts as the custodian for the AMN Profile and is to be used as the conduit for changes (via her dual membership of the AMN AWG and IPCat).

1.1.4.2. Summary of Changes to the AMN Profile

009. The table below summarizes the main changes between the AMN Profile as published in ADaTP-34(I) to the standards cited in the tables of this document.

Table 1.1. Summary of Changes to the AMN Profile

Table/Subject	Key updates

1.1.5. Relationship to NATO C3 Classification Taxonomy

010. The AMN has been designed and is managed as far as possible using a service approach. The AMN Services are based on the NATO C3 Classification Taxonomy AC/322-N(2012)0092-AS1.

011. The C3 Classification Taxonomy is used to identify particular services and associated Service Interoperability Point where two entities will interface and the standards in use by the relevant systems.

012. Within Volume 4 of the AMN JMEI, the implementation of a standard (where required) is described within an annex associated with each service.

013. The C3 Classification Taxonomy has been used to structure the AMN Profile, commencing with Communications and working up the Taxonomy.

1.2. COMMUNICATION SERVICES

014. **Definition**: *Communications Services interconnect systems and mechanisms for the opaque transfer of selected data between or among access points, in accordance with agreed quality parameters and without change in the form or content of the data as sent and received.*

015. Communications Services can be further defined as:

- Transmission Services
- Transport Services
- Communications Access Services

1.2.1. Transmission Services

016. **Definition**: *Transmission Services cover the physical layer (also referred to as media layer or air-interface in wireless/satellite (SATCOM) communications) supporting Transport Services, as well as Communications Access Services. Support for the latter is relevant to personal communications systems, in which the User Appliances directly connect to the transmission element without any transport elements in between.*

1.2.1.1. Standards

017. Although the implementation scope of AMN technically does not cover Transmission Services, there is one area that provides the foundation for the provision of federated services on the AMN. The Standards listed in Table 1.2 need to be adhered to.

Table 1.2. Transmission IA Services Standards

ID: Service/Purpose	Standards	Implementation Guidance
1:Information Assurance during Transmission	Mandatory: ACP 176 NATO SUPP 1 (NC)	ACP 176 NATO SUPP 1 (NC) provides configuration settings necessary to ensure interoperability when different cryptographic devices (e.g. KIV-7/ KG84/BID1650) are employed together.

1.2.2. Transport Services

018. **Definition**: *Transport Services provide resource-facing services, providing metro and wide-area connectivity to the Communications Access Services that operate at the edges of the network. In that role, Transport Services interact with the Transmission Services using them as the physical layer fabric supporting the transfer of data over a variety of transmission bearers as and where needed.*

019. Transport Services are further defined in the C3 Taxonomy, however the area that is most relevant to the AMN are:

- Edge Transport Services

020. **Definition**: *Edge Transport Services provide the delivery or exchange of traffic flows over different Transmission Services. The traffic flows are formatted and delivered by the Communications Access Services at the edges of the network. This "edge" in Edge Transport is the Wide Area Network (WAN) edge (i.e. the provider edge). In Protected Core Networking (PCN) terms, the edge can be considered as the entry point into the Protected Core.*

1.2.2.1. Standards

021. The AMN is a converged IP network applying open standards and industry best practices. The AMN architecture uses interconnection based on IPv4 between the Mission Networks (also referred to as autonomous systems).

022. The AMN was originally conceived with IPv6 as the target for interconnecting autonomous systems (although no TCN has yet indicated that they wish to implement this on the AMN).

023. It is now advised that all new equipment, services and applications must support a dual IPv4/IPv6 stack implementation to future-proof the AMN for the long term .

024. The interconnection between Mission Networks is based on STANAG 5067 enhanced with a non-tactical connector and optional 1Gb/s Ethernet. STANAG 5067 provides additional implementation, security and management guidance. Due to the classification level of the AMN, dedicated transmission security (crypto) equipment is used.

025. The standards for Transport and corresponding Communications Equipment are given in Table 1.3.

Table 1.3. Edge Transport Services and Communications Equipment Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Edge Transport Services between autonomous systems (IP over point-to-point Ethernet links on optical fibre)	• Mandatory: ISO/IEC 11801: 2002-09, Information technology –Generic cabling for customer premises, Clause 9. Single-mode optical fibre OS1 wavelength 1310nm. • Mandatory: ITU-T G.652 (11/2009), Characteristics of a single-mode optical fibre and cable. (9/125µm)	Use 1Gb/s Ethernet over Single-mode optical fibre (SMF).

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: IEC 61754-20: 2012(E), Fibre optic interconnecting devices and passive components - Fibre optic connector interfaces - Part 20: Type LC connector family. LC-duplex single-mode connector. • Mandatory: IEEE Std 802.3-2013, Standard for Ethernet- Section 5 - Clause 58 - 1000BASE-LX10, Nominal transmit wavelength 1310nm. IPv4 over Ethernet: • Mandatory: IETF STD 37: 1982 / IETF RFC 826: 1982, An Ethernet Address Resolution Protocol IPv6 over Ethernet (Optional): • Mandatory (if option taken):IETF RFC 4861: 2007, Neighbor Discovery for IP version 6 (IPv6)	
2: Inter-Autonomous System (AS) routing	IPv4 over Ethernet: • Mandatory: IETF RFC 1997:1996, BGP Communities Attribute. • Emerging: IETF RFC 3392: 2002, Capabilities Advertisement with BGP-4. • Mandatory: Border Gateway Protocol V4 (IETF RFC 1771, March 1995).	BGP deployment guidance in: IETF RFC 1772: 1995, Application of the Border Gateway Protocol in the Internet. Detailed Interface Control Document for “Connection Between CISAF network and TCN networks” [Thales ICD NIP Dec 2012]

ID: Service/Purpose	Standards	Implementation Guidance
	• Emerging: IETF RFC 4760: 2007, Multiprotocol Extensions for BGP-4. 32-bit autonomous system numbers: • Mandatory: IETF RFC 6793: 2012, BGP Support for Four-Octet Autonomous System (AS) Number Space. • Mandatory: IETF RFC 4360: 2006, BGP Extended Communities Attribute. • Mandatory: IETF RFC 5668: 2009, 4-Octet AS Specific BGP Extended Community. IPv6 over Ethernet (Optional): • Mandatory (if option taken): IETF RFC 2545: 1999, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing.	
3: Inter-Autonomous System (AS) multicast routing	IPv4 over Ethernet: • Mandatory: IETF RFC 3618: 2003, Multicast Source Discovery Protocol (MSDP). • Mandatory: IETF RFC 3376: 2002, Internet Group Management Protocol, Version 3 (IGMPv3). • Mandatory: IETF RFC 4601, Protocol Independent Multicast version 2 (PIMv2) Sparse Mode (SM).	

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: IETF RFC 4760: 2007 “Multiprotocol Extensions for BGP (MBGP)”. IPv6 over Ethernet: • Note: No standard solution for IPv6 multicast routing has yet been widely accepted. More research and experimentation is required in this area.	
4: Unicast routing	• Mandatory: IETF RFC 4632: 2006, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.	
5: Multicast routing	• Mandatory: IETF RFC 1112: 1989, Host Extensions for IP Multicasting. • Mandatory: IETF RFC 2908: 2000, The Internet Multicast Address Allocation Architecture • Mandatory: IETF RFC 3171: 2001, IANA Guidelines for IPv4 Multicast Address Assignments. • Mandatory: IETF RFC 2365: 1998, Administratively Scoped IP Multicast.	

1.2.2.2. Implementation

026. The Network Interconnection Point (NIP) provides a network interconnection at the IP layer for the ISAF SECRET environment making up the AMN. It serves 3 major purposes:

- Intra autonomous system (AS) routing (routing of traffic between nations or between nations and NATO, where each nation is a BGP Autonomous System).

- QoS policy enforcement (to provide end-to-end QoS for the required services).

- IPSLA compliance verification (to verify end-to-end performance compliance).

1.2.3. Communications Access Services

027. **Definition**: *Transport Communications Access Services provide end-to-end connectivity of communications or computing devices. Communications Access Services can be interfaced directly to Transmission Services (e.g. in the case of personal communications systems) or to Transport Services, which in turn interact with Transmission Services for the actual physical transport. Communications Access Services correspond to customer-facing communications services. As such, they can also be referred to as Subscriber Services, or Customer-Edge (CE) Services.*

028. With respect to the current implementation scope of AMN, the following Communications Access services apply:

- Packet-Based Communications Access Services
- Communications Access Information Assurance (IA) Services
- Communications Access Service Management Control (SMC) Services.
- Multimedia Services

1.2.3.1. Standards

029. To provide federated services, the standards listed in Table 1.4 and Table 1.5 should be adhered to.

Table 1.4. Packet-based Communications Access Services Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Host-to-host transport services	• Mandatory: IETF STD 6: 1980 /IETF RFC 768: 1980, User Datagram Protocol. • Mandatory: IETF STD 7: 1981 / RFC 793: 1981, Transmission Control Protocol.	
2: host-to-host datagram services	Internet Protocol: • Mandatory: IETF RFC 791: 1981, Internet Protocol. • Mandatory: IETF RFC 792: 1981, Internet Control Message Protocol.	IP networking. Accommodate both IPv4 and IPv6 addressing[a] Max Transmission Unit (MTU) reduced to 1300 bytes, Max Segment Size (MSS) set to 1260 bytes in order to accommodate IP crypto tunneling within autonomous systems

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: IETF RFC 919: 1994, Broadcasting Internet Datagrams. • Mandatory: IETF RFC 922: 1984, Broadcasting Internet Datagrams in the Presence of Subnets. • Mandatory: IETF RFC 950: 1985, Internet Standard Subnetting Procedure. • Mandatory: IETF RFC 1112: 1989, Host Extensions for IP Multicasting. • Mandatory: IETF RFC 1812: 1995, Requirements for IP Version 4 Routers. • Advised: IETF RFC 2644: 1999, Changing the Default for Directed Broadcasts in Routers. • Discouraged: IETF RFC 1918:1996, Address Allocation for Private Internets • Discouraged: IETF RFC 1631:1994, The IP Network Address Translation (NAT) IPv6 over Ethernet (Optional): • Recommended: IETF RFC 2460: 1998, Internet Protocol, Version 6 (IPv6) Specification. • Recommended: IETF RFC 3484: 2003, Default Address Selection for Internet Protocol version 6 (IPv6).	Use of private range addressing (IETF RFC 1918) should be avoided by the TCNs to prevent addressing conflicts with existing networks. IP address space provided by the AMN Naming and Addressing Authority is to be enforced. An option however may exist, for Nations to bring in IP space assigned to the Nation by an Internet Registry under IANA and certified by the nation as globally unique within their networks. This must be coordinated via the AMN Secretariat Technical Management Office On the AMN, NAT has always been highly discouraged within the TCN networks[b]. From Jan 2011 it has been removed as an option for all subsequent joining nations[c]. Regarding IETF RFC 4291: Only IPv6 addresses may be used which are assigned to the nation/NATO out of the pool for global unicast by an Internet Registry under IANA and guaranteed by the nation/NATO as globally unique within their networks

ID: Service/Purpose	Standards	Implementation Guidance
	• Recommended: IETF RFC 3810: 2004, Multicast Listener Discovery Version 2 (MLDv2) for IPv6. • Recommended: IETF RFC 4291: 2006, IP Version 6 Addressing Architecture. • Recommended: IETF RFC 4443: 2006, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. • Recommended: IETF RFC 4861: 2007, Neighbor Discovery for IP version 6 (IPv6). • Recommended: IETF RFC 5095: 2007, Deprecation of Type 0 Routing Headers in IPv6.	
3: Differentiated host-to-host datagram services (IP Quality of Service)	• Mandatory: IETF RFC 2474: 1998, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. • updated by IETF RFC 3260: 2002, New Terminology and Clarifications for DiffServ. • Mandatory: IETF RFC 4594: 2006, Configuration Guidelines for DiffServ Service Classes. • Mandatory: ITU-T Y.1540 (03/2011), Internet protocol data communication service – IP packet transfer and avail-	The AMN QoS standard was constructed based on the NATO QoS Enabled Network Infrastructure (QENI). The QoS model adopted is however not quite fully compliant with IP QoS Maturity level QoS-1 as defined in the NII IP QoS Standard [NC3A TN-1417] (the deviation has largely to do with the DSCP markings). AMN IP QoS aggregates all IP traffic into 4x classes - (Real Time (RT); Near Real Time (NRT); Network (routing, signalling, management); Best Effort).

ID: Service/Purpose	Standards	Implementation Guidance
	ability performance parameters. • Mandatory: ITU-T Y.1541 (12/2011), Network performance objectives for IP-based services. • Mandatory: ITU-T Y.1542 (06/2010), Framework for achieving end-to-end IP performance objectives. • Mandatory: ITU-T M.2301 (07/2002), Performance objectives and procedures for provisioning and maintenance of IP-based networks. • Mandatory: ITU-T J.241 (04/2005), Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks.	

[a]Note that although IPv6 has always been part of the AMN Profile it has never been taken up. There has always been the intent to provide a tunnel of v6 over v4 or via a dual stack, should a TCN require it.

[b]Due to the fact that one of the early founding TCN networks of the AMN had already implemented NAT on the already existing network that became the extension, historically NAT has had to be presented as an option for the AMN. NAT however is not in line with the openness required on the AMN and has always been highly discouraged within the TCN network.

[c]Nations that implemented NAT at the foundation of the AMN will remain unaffected and will not be required to change.

Table 1.5. Communications Access IA Services Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Provide communications security over the network above the Transport Layer	• Mandatory: IETF RFC 5246: 2008, Transport Layer Security (TLS) Protocol Version 1.2.	

1.3. CORE ENTERPRISE SERVICES

030. **Definition**: *Core Enterprise Services (CES) provide generic, domain independent, technical functionality that enables or facilitates the operation and use of Information Technology (IT) resources.*

031. CES will be broken up further into:

- Infrastructure Services (incl. Information Assurance (IA) services)
- Service Oriented Architecture (SOA) Platform Services
- Enterprise Support Services

1.3.1. Infrastructure Services

032. **Definition**: *Infrastructure Services provide software resources required to host services in a distributed and federated environment. They include computing, storage and high-level networking capabilities that can be used as the foundation for data centre or cloud computing implementations.*

1.3.1.1. Standards

033. To provide federated services the standards listed in Table Table 1.6 should be adhered to.

Table 1.6. Infrastructure Services Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Distributed Time Services: Time synchronization	• Mandatory: IETF RFC 5905: June 2010, Network Time Protocol version 4 (NTPv4). • Fading: IETF RFC 1305: March 1992, NTPv3. To aid rapid post event reconstruction, ALL networked equipment will be set to process time as Coordinated Universal Time (UTC). i.e. ZULU Time Zone should apply to the whole Mission Network [AMN TPT CES Sept 2011].	All new capabilities shall use NTPv4. Some legacy systems may still need to use NTPv3. TCN connecting to the AMN Core must use the time service of the AMN Core. A stratum-1 time server is directly linked (not over a network path) to a reliable source of UTC time (Universal Time Coordinate) such as GPS, WWV, or CDMA transmissions through a modem connection, satellite, or radio. Stratum-1 devices must implement IPv4 and IPv6 so that they

ID: Service/Purpose	Standards	Implementation Guidance
		can be used as timeservers for IPv4 and IPv6 Mission Network Elements The W32Time service on all Windows Domain Controllers is to synchronize time through the Domain hierarchy (NT5DS type). Databases are to implement TIMESTAMP as specified in point 4 below
2: Domain Name Services: Naming and Addressing	• Mandatory: IETF STD 13: 1987 /, IETF RFC 1034: 1987, Domain Names – Concepts and Facilities. • Mandatory: IETF RFC 1035: 1987, Domain Names – Implementation and specification. • Mandatory: IETF RFC 1032: 1987, Domain Administrators Guide.	
3: Identification and addressing of objects on the network.	• Mandatory: IETF RFC 1738: 1994, Uniform Resource Locators (URL). • Mandatory: IETF RFC 3986: 2005, Uniform Resource Identifiers (URI), Generic Syntax., January 2005 (updates IETF RFC 1738)	Namespaces within XML documents shall use unique URLs or URIs for the namespace designation.
4: Infrastructure Storage Services: storing and accessing information about the time of events and transactions	• Mandatory: ISO/IEC 9075(Parts 1 to 14):2011, Information technology - Database languages – SQL Databases shall stores date and time values everything	As the AMN user community spans several time zones, applications will increasingly need to conduct transactions across different time zones. Timestamps are essential for auditing purposes. It is important that the integrity of timestamps is main-

ID: Service/Purpose	Standards	Implementation Guidance
	in TIMESTAMP WITH TIME ZONE or TIMESTAMPTZ	tained across all Mission Network Elements. From Oracle 9i, PostgreSQL 7.3 and MS SQL Server 2008 onwards, the time zone can be stored with the time directly by using the TIMESTAMP WITH TIME ZONE (Oracle, PostgreSQL) or datetimeoffset (MS-SQL) data types. On the AMN, human interfaces may convert the time for display to the user as (e.g.) D30 (i.e. Local) as required. See also Table 1.15 for details on representing time within applications
5: Infrastructure IA Services: Facilitate the access and authorization between users and services. Directory access and management service	• Mandatory: IETF RFC 4510: 2006, version 3 of the Lightweight Directory Access Protocol (LDAPv3), (LDAP) Technical Specification Road Map (LDAPv3). • Mandatory: IETF RFC 4511-4519:2006, RFC 4510 and associated LDAP Technical Specification. (RFC 4511-4519) • Mandatory: IETF RFC 2849: 2000, The LDAP Interchange Format 9 (LDIF)., RFC 2849	There are three options available to a Troop Contributing Nation (TCN) when joining their national network extension to the AMN: 1. Join the ISAF SECRET AD forest on AMN Core 2. Join the AD forest of an existing AMN TCN 3. Create own AD forest for the new AMN TCN (Option 1 and 2 should be considered by the prospective Joining TCN before Option 3). Whilst LDAP is a vendor independent standard, in practice Microsoft Active Directory (AD) is a common product providing directory services on national and NATO owned Mission Network elements. It should be noted that

ID: Service/Purpose	Standards	Implementation Guidance
		AD provides additional services aside from LDAP like functionality. Note: Active Directory Federation Services (ADFS) will not be used on the AMN. The AMN is one logical network based on mutual trust. In such a trusted environment there is no requirement or use case for single sign on for webservices. In those cases where an outside or untrusted subdomain of a Nationally implemented Network desires access to webservices on the AMN, then those services will be granted using "local accounts created on the parent (AMN) domain.
6: Infrastructure IA Services: Digital Certificate Services	• Mandatory: ITU-T X.509 (11/2008), Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks • the version of the encoded public-key certificate shall be v3. • the version of the encoded certificate revocation list (CRL) shall be v2. • Mandatory: NATO Public Key Infrastructure (NPKI) Certificate Policy (CertP) Rev2, AC/322D(2004)0024 REV2	Note: on the AMN, PKI is only used for authentication (encryption of login). It is not used for the encryption of the entire session[a].
7: Infrastructure IA Services: Authentication Services	• Mandatory: IETF RFC 1510:1993, The Kerberos	

ID: Service/Purpose	Standards	Implementation Guidance
	Network Authentication Service (V5).	
8: Infrastructure Processing (Operating System) Services	Operating Systems used on the AMN must be accredited by the respective Security Accreditation Authority. As a minimum the Operating Systems should support the specifications for the above (Infrastructure IA Services).	Clients on the AMN Core and Option 1 TCN National Network Extensions are strongly advised to use Windows 7 Enterprise due to the mid-2014 End of Support provision by Microsoft for Windows XP. Win 7 Enterprise was selected due to the inclusion of AppLocker (remote enforcement of application control policies) and integration with Sharepoint 2010 and MS Office Professional Plus 2010. Windows 2008 R2 Standard Full Edition 64 bit is strongly advised for all Domain Controllers. Note Service Pack SP1 should be installed

[a]If PKI was used for the encryption of the entire session then this would create a flurry of un-monitorable traffic across the AMN. This would then lead to Certificate Proxy Services in order to once again see the traffic, and this would lead to a significant slow-down in information flow – which would have impacts in an operation that requires real time information flows.

1.3.2. SOA Platform Services

034. **Definition**: *SOA Platform Services provide a foundation to implement web-based services in a loosely coupled environment, where flexible and agile service orchestration is a requirement. They offer generic building blocks for SOA implementation (e.g. discovery, message busses, orchestration, information abstraction and access, etc.) and can be used as a capability integration platform in a heterogeneous service-provisioning ecosystem.*

1.3.2.1. Standards

035. To provide federated services the standards listed in Table 1.7 should be adhered to.

Table 1.7. Service Oriented Architecture (SOA) platform services and data standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Web Platform Services	• Mandatory: IETF RFC 2616: 1999, Hypertext Transfer Protocol HTTP/ 1.1. • Mandatory: IETF RFC 2817: 2000, Upgrading to TLS within HTTP/ 1.1. • Mandatory: IETF RFC 3986: 2005, Uniform Resource Identifier (URI): Generic Syntax.	HTTP shall be used as the transport protocol for information without 'need-to-know' caveats between all service providers and consumers (unsecured HTTP traffic). HTTPS shall be used as the transport protocol between all service providers and consumers to ensure Confidentiality requirements (secured HTTP traffic). Unsecured and secured HTTP traffic shall share the same port.
2: Publishing information including text, multimedia, hyperlink features, scripting languages and style sheets on the network	• Mandatory: HyperText Markup Language (HTML) 4.01 (strict) • ISO/IEC 15445:2000, Information technology -- Document description and processing languages -- HyperText Markup Language (HTML). • IETF RFC2854:2000, The 'text/html' Media Type. • Emerging (2014): HyperText Markup Language, Version 5 (HTML 5), W3C Candidate Recommendation, Aug 2013	
3: Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of docu-	• Mandatory: Cascading Style Sheets (CSS), Level 2 revision 1 (CSS 2.1), W3C Recommendation, September 2009.	

ID: Service/Purpose	Standards	Implementation Guidance
ments written in mark-up languages like HTML.	• Emerging (2014): Cascading Style Sheets (CSS) Level 3: • Cascading Style Sheets (CSS), Level 2 revision 1 (including errata) (CSS 2.1), W3C Recommendation, June 2011. • CSS Style Attributes, W3C Candidate Recommendation, 12 October 2010 • Media Queries, W3C Recommendation, 19 June 2012. • CSS Namespaces Module, W3C Recommendation, 29 September 2011. • Selectors Level 3, W3C Recommendation, 29 September 2011. • CSS Color Module Level 3, W3C Recommendation, 07 June 2011.	
4: General formatting of information for sharing or exchange.	• Mandatory: Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation, 26 November 2008. • Mandatory: XML Schema Part 1: Structures Second Edition, W3C Recommendation, 28 October 2004. • Mandatory: XML Schema Part 2: Datatypes Second Edition, W3C Recommendation, 28 October 2004.	XML shall be used for data exchange to satisfy those IERs on the AMN that are not addressed by a specific information exchange standard. XML Schemas and namespaces are required for all XML documents.

ID: Service/Purpose	Standards	Implementation Guidance
5: Providing web content or web feeds for syndication to web sites as well as directly to user agents.	• Mandatory: (Really Simple Syndication) RSS 2.0 Specification Version 2.0.11, 30 March 2009. • Emerging: IETF RFC 4287: 2005, The Atom Syndication Format. (Atom 1.0). • Emerging: IETF RFC 5023: 2007, The Atom Publishing Protocol.	
6: Encoding of location as part of web feeds	• Mandatory: GeoRSS Simple encoding: Geographically Encoded Objects for RSS feeds: GeoRSS Simple encoding for <georss:point>, <georss:line>, <georss:polygon>, <georss:box>. • Recommended: GeoRSS GML Profile 1.0 a GML subset for <gml:Point>, <gml:LineString>, <gml:Polygon>, <gml:Envelope> of • Recommended: Where GeoRSS Simple is not appropriate the OGC GeoRSS 03-105r1: 2004-02-07, OpenGIS Geography Markup Language (GML) Implementation Specification version 3.1.1.	GML allows you to specify a coordinate reference system (CRS) other than WGS84 decimal degrees (think lat/long). If there is a need to express geography in a CRS other than WGS84, it is recommended to specify the geographic object multiple times, one in WGS84 and the others in your other desired CRSes. Please also see Table 1.10 Regarding Coordinate Reference Systems Schema location for GeoRSS GML Profile 1.0: http://georss.org /xml/1.0/gmlgeorss.xsd
7: Message Security for web services	• Mandatory: WS-Security: SOAP Message Security 1.1. • Mandatory: XML Encryption Syntax and Processing, W3C Recommendation, 10 December2002.	Specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509v3. Its main focus is the use of XML Sig-

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: XML Signature Syntax and Processing (Second Edition), W3C Recommendation, 10 June 2008. • Mandatory: OASIS WS-I Basic Security Profile Version 1.1, 24 January 2010.	nature and XML Encryption to provide end-to-end security. Specifies a process for encrypting data and representing the result in XML. Referenced by WS-Security specification. Specifies XML digital signature processing rules and syntax. Referenced by WS-Security specification
8: Security token format	• Mandatory: OASIS Standard, Security Assertion Markup Language (SAML) 2.0), March 2005. • Mandatory: OASIS Standard, Web Services Security: SAML Token Profile 1.1 incorporating approved errata 1, Nov 2006.	Provides XML-based syntax to describe uses security tokens containing assertions to pass information about a principal (usually an end-user) between an identity provider and a web service. Describes how to use SAML security tokens with WS-Security specification.
9: Security token issuing	• Mandatory: OASIS Standard, WS-Trust 1.4, incorporating Approved Errata 01, 25 April 2012. • Mandatory: Web Services Federation Language (WS-Federation) Version 1.1, December 2006.[a] • Mandatory: Web Services Policy 1.5 – Framework, W3C Recommendation, 04 September 2007. • Mandatory: WS-Security Policy 1.3, OASIS Standard incorporating Approved Errata 01, 25 April 2012.WS-Trust 1.4	Uses WS-Security base mechanisms and defines additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. Extends WS-Trust to allow federation of different security realms. Used to describe what aspects of the federation framework are required/supported by federation participants and that this information is used to determine the appropriate communication options.

ID: Service/Purpose	Standards	Implementation Guidance
10: Transforming XML documents into other XML documents	• Mandatory: XSL Transformations (XSLT) Version 2.0, W3C Recommendation, 23 January 2007. • Note that XSLT 2.0 is a revised version of the XSLT 1.0 Recommendation published on 16 November 1999	Developer best practice for the translation of XML based documents into other formats or schemas.
11: Configuration management of structured data standards, service descriptions and other structured metadata.	• Mandatory: ebXML v3.0: Electronic business XML Version 3.0, • Mandatory: Registry Information Model (ebRIM), OASIS Standard, 2 May 2005, • Mandatory: Registry Services and Protocols (ebRS) • Mandatory: OASIS Standard, Universal Description, Discovery, and Integration Specification (UDDI v2.0). • Emerging: OASIS Standard, Universal Description, Discovery, and Integration Specification (UDDI v3.0).	Used as foundation for setup, maintenance and interaction with a (AMN) Metadata Registry and Repository for sharing and configuration management of XML metadata. Also enables federation among metadata registries/ repositories.
12: Exchanging structured information in a decentralized, distributed environment via web services	• Mandatory: W3C SOAP 1.1, Simple Object Access Protocol v1.1 (SOAP) 1.1, W3C Note, 8 May 2000 • Mandatory: WSDL v1.1: Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001. • Conditional: Representational State Transfer (REST) in accordance with:	The preferred method for implementing web-services are SOAP, however, there are many use cases (mash-ups etc.) where a REST based interface is easier to implement and sufficient to meet the IERs. Restful services support HTTP caching, if the data the Web service returns is not altered frequently and not dynamic in nature. REST is particularly useful for restricted-profile devices

ID: Service/Purpose	Standards	Implementation Guidance
	• University of California, Roy Thomas Fielding, Architectural Styles and the Design of Network-based Software Architectures: 2000, Irvine, CA. • Emerging (2014): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation, 27 April 2007. • Emerging (2014): SOAP Version 1.2 Part 2: Adjuncts (Second Edition), W3C Recommendation, 27 April 2007. • Emerging (2014): SOAP Version 1.2 Part 3: One-Way MEP, W3C Working Group Note, 2 July 2007	such as mobile phones and tablets for which the overhead of additional parameters like headers and other SOAP elements are less.
13: Secure exchange of data objects and documents across multiple security domains	The Draft X-Labels syntax definition is called the "NATO Profile for the XML “Confidentiality Label Syntax" and is based on version 1.0 of the RTG-031 proposed XML confidentiality label syntax, see "Sharing of information across communities of interest and across security domains with object level protection" below.	
14: Topic based publish / subscribe web services communication	• Mandatory: OASIS, Web Services Brokered Notification 1.3 (WS-BrokeredNotification), OASIS Standard, 1 October 2006	Enable topic based subscriptions for web service notifications, with extensible filter mechanism and support for message brokers.

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: OASIS, Web Services Base Notification 1.3 (WS-BaseNotification), OASIS Standard, 1 October 2006 • Mandatory: OASIS, Web Services Topics 1.3 (WS-Topics), OASIS Standard, 1 October 2006	
15: Providing transport-neutral mechanisms to address web services	• Mandatory: Web Services Addressing 1.0 – Core, W3C Recommendation, 9 May 2006	Provides transport-neutral mechanisms to address Web services and messages which is crucial in providing end-to- message level security, reliable messaging or publish / subscribe based web services end.
16: Reliable messaging for web services	• Mandatory: OASIS Standard, Web Services Reliable Messaging (WS-Reliable Messaging) Version 1.2, February 2009.	Describes a protocol that allows messages to be transferred reliably between nodes implementing this protocol in the presence of software component, system, or network failures.

[a]This specification is subject to the following copyright: (c) 2001-2006 BEA Systems, Inc., BMC Software, CA, Inc., International Business Machines Corporation, Layer 7 Technologies, Microsoft Corporation, Inc., Novell, Inc. and VeriSign, Inc. All rights reserve.

1.3.3. Enterprise Support Services

036. **Definition**: *Enterprise Support Services are a set of Community Of Interest (COI) independent services that must be available to all members within the AMN. Enterprise Support Services facilitate other service and data providers on the federated networks by providing and managing underlying capabilities to facilitate collaboration and information management for end-users.*

037. For the purposes of this Volume, Enterprise Support Services will be broken up further into:

- Unified Communication and Collaboration Services
- Information Management Services
- Geospatial Services

1.3.3.1. Unified Communication and Collaboration Services

038. **Definition**: *Unified Communication and Collaboration Services provide users with a range of interoperable collaboration capabilities, based on standards that fulfill operational requirements. They will enable real-time situational updates to time-critical planning activities between coalition partners, communities of interest (e.g. the Intel community or the Logistics community), and other agencies. Levels of collaboration include awareness, shared information, coordination and joint product development.*

039. Different use cases require different levels of protection of these communication and collaboration services. For voice or audio-based collaboration services, the AMN profile can provide interoperability standards for two different scenarios:

- A. Voice over Secure IP (VoSIP) network services
- B. Network agnostic Secure Voice Services (such as 3G, IP/4G, ISDN)

040. On AMN, VoSIP is mandatory. If however network agnostic Secure Voice services are required in addition to VoSIP[2], then Secure Communications Interoperability Protocol (SCIP) specifications as defined for audio-based collaboration services (end-to-end protected voice) over any network should be used[3]. [Note this has been included due to the emerging requirements regarding Operation Resolute Support (i.e. from Jan 2015, post ISAF)]

041. For text-based collaboration there is also a basic profile sufficient for operating this service with reduced protection requirements as well as an enhanced XMPP profile that includes additional security mechanisms.

1.3.3.1.1. Standards

042. To provide federated services the standards listed in Table 1.8 should be adhered to.

Table 1.8. Unified Communication and Collaboration Services and Data Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Video-based Collaboration Services (VTC)	• Mandatory (VTCoIP Signalling): ITU-T H.323 v7 (12/2009) Packet-based multimedia communications systems;	AMN VTC over IP is based on a QoS-Enabled Net- work Infrastructure (QENI) using Diffserve. The AMN-Wide allowed interconnections are:

[2]The only scenario where this would apply would be in the case that crypto devices cannot be supplied, protected and managed on site and physical access to the AMN is hence not available at that location.

[3]If SCIP is used, then access to the AMN can only be possible if a gateway for SCIP multi-conferencing and interconnection to VoSIP networks is provided. AMN. Additionally to achieve this there would need to be agreement to re-use a Key Management system that is already deployed in ISAF (for example that used for the OMLTs).

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory (VTCoIP Audio encoding): ITU-T G.722.1c (2005) Corrigendum 1 (06/2008) Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss; • Mandatory (VTCoIP Video encoding): ITU-T H.263 (01/2005) Video coding for low bit rate communication	A) Peer to Peer, B) Peer to MCU and C) Peer to MCU to MCU to Peer
2: Audio-based Collaboration Services	• Mandatory (VoIP numbering): STANAG 4705 Ed. 1 Ratification Draft, International Network Numbering for Communications Systems in use in NATO. • Mandatory (VoIP): IETF RFC 3261: 2002, SIP: Session Initiation Protocol. • Mandatory (Subscriber Number): STANAG 5046 Ed.3 (1995) The NATO Military Communications Directory System • Mandatory (VoIP Audio data encoding): ITU-T Recommendation G.729 Annex A (11/96), Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP). [a]	VoSIP refers to non-protected voice service running on a classified IP network (as in the case of the AMN). All numbers (calling and called) passed over the NIP consist of 13 digits irrespective of the networks involved. The 13-digits consist of a 6 digit prefix and a 7-digit subscriber number. A TCN must be prepared to pass these 13 digits over the NIP. By default the subscriber number should be taken from STANAG 5046 Voice Sampling Interval between Voice packets: 40ms RTP protocol ports 16384 and/or 16385 See also detailed Interface Control Document for "Voice over Secure IP (VoSIP) Network Service" [THALES ICD 61935771-558 A Jul 2009].
3: Audio-based Collaboration Services (end-to-end	• Emerging: ITU-T V.150.1 (03/2004), Modem-over-IP	Secure voice services over any network.

ID: Service/Purpose	Standards	Implementation Guidance
protected voice) (Secure Communications Interoperability Protocol. SCIP)	networks: Procedures for the end-to-end connection of V-series DCEs, incorporating changes introduced by Corrigendum 1 and 2. • Emerging: National Security Agency (NSA), SCIP-210. SCIP signalling plan. 2007. • Emerging: NSA, SCIP-214, Interface requirements for SCIP devices to circuit switched networks. • Emerging: NSA, SCIP-215, Interface requirements for SCIP devices to IP networks. • Emerging: NSA, SCIP-216: Minimum Essential Requirements (MER) for V.150.1 recommendation. • Emerging: NSA, SCIP-220: Requirements for SCIP. • Emerging: NSA, SCIP-221: SCIP Minimum Implementation Profile (MIP). • Emerging: NSA, SCIP-233: NATO interim cryptographic suite (NATO and coalition).	V.150.1 support must be end-to-end supported by unclassified voice network SCIP-214 only applies to gateways Note that SCIP-216 requires universal implementation.
4: Informal messaging services (e-mail)	• Mandatory: IETF RFC 2821:2001, Simple Mail Transfer Protocol (SMTP). • Mandatory: IETF RFC 1870:1995, SMTP Service Extension for Message Size Declaration.	Conditional: messages must be labelled in the message header field “Keywords” (RFC 2822) according to the following convention: • [MMM] [CLASSIFICATION], Releasable to [MISSION]

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: IETF RFC 2822:2001, Simple Internet Messages. • Emerging (2016): IETF RFC 5321: 2008, Simple Mail Transfer Protocol which obsoletes: IETF RFC 2821: 2001 • Emerging (2017): IETF RFC 6477: 2012, Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail	Where: • CLASSIFICATION is the classification {SECRET, CONFIDENTIAL, RESTRICTED, UNCLASSIFIED} • MMM is the alpha-3 country code e.g. DEU, GBR, as defined in Table 11.ID2 with the exception that NATO will be identified by the four letter acronym “NATO”. • Example: • Keywords: ITA UNCLASSIFIED, Releasable to XFOR
5: Content encapsulation within bodies of internet messages	Multipurpose Internet Mail Extensions (MIME) specification: • Mandatory: IETF RFC 2045:1996, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. • Mandatory: IETF RFC 2046: 1996, Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. • Mandatory: IETF RFC 2047: 1996, MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text. • Mandatory: IETF RFC 2049: 1996, Multipurpose Internet Mail Extensions (MIME) Part	10 MB max message size limit Minimum Content-Transfer-Encoding: • 7bit • base64 • binary BINARYMIME SMTP extension [IETF RFC 3030] Minimum set of media and content-types: • text/plain [IETF RFC1521] • text/enriched [IETF RFC1896] • text/html IETF [RFC1866]

ID: Service/Purpose	Standards	Implementation Guidance
	Five: Conformance Criteria and Examples. • Mandatory: IETF RFC 4288 : 2005, Media Type Specifications and Registration Procedures.	• multipart/mixed [IETF RFC 2046] • multipart/signed
6: text-based collaboration services	• Mandatory: Basic XMPP profile (see ID 6.1 below) • Recommended: Enhanced XMPP profile (see ID 6.2)	Near-real time text-based group collaboration capability for time critical reporting and decision making in military operations.

6.1: text-based collaboration services (basic XMPP profile)	• Mandatory: IETF RFC 6120: 2011, Extensible Messaging and Presence Protocol (XMPP): Core
	
	• Mandatory: IETF RFC 6121: 2011, Extensible Messaging and Presence Protocol (XMPP) extensions for: Instant Messaging and Presence.
	
	• Mandatory: The following XMPP Extension Protocols (XEP) defined by the XMPP Standards Foundation shall also be supported:
	
	  • XEP-0004: Data Forms, August 2007.
	
	  • XEP-0030: Service Discovery, February 2007
	
	  • XEP-0045: Multi-User Chat (MUC), July 2008
	
	  • XEP-0049: Private XML Storage, March 2004
	
	  • XEP-0050: Ad Hoc Commands, June 2005
		IETF RFC 6120 supersedes IETF RFC 3920
		
		IETF RFC 6121 XMPP IM supersedes IETF RFC 3921

ID: Service/Purpose	Standards	Implementation Guidance
	• XEP-0054: vCard Profiles, March 2003 • XEP-0065: SOCKS5 Byte streams, April 2011 • XEP-0092: Software Version, February 2007 • XEP-0096: SI File Transfer, April 2004. • XEP-0114: Jabber Component Protocol, March 2005 • XEP-0115: Entity Capabilities, February 2008. • XEP-0203: Delayed Delivery, September 2009 • XEP-0220: Server Dialback, December 2007 • XEP-0288: Bidirectional Server-to-Server Connections, October 2010 • Fading: • XEP-0078: Non-SASL Authentication, October 2008. (for support of older clients) • XEP-0091: Legacy Delayed Delivery, May 2009	
6.2: text-based collaboration services (enhanced XMPP profile).	• Recommended: The enhanced profile requires compliance with the basic profile as defined above plus:	Developers are also advised to consult the following IETF RFCs:

ID: Service/Purpose	Standards	Implementation Guidance
	• XEP-0033: Extended Stanza Addressing, September 2004 • XEP-0079: Advanced Message Processing, November 2005. • XEP-0122: Data Forms Validation. September 2005. • XEP-0199: XMPP Ping, June 2009. • XEP-0249: Direct MUC Invitation, September 2011. • XEP-0258: Security Labels in XMPP, March 2009 • Emerging: • XEP-0311(MUC Fast Reconnect, January 2012	• IETF RFC 6122: 2011, Extensible Messaging and Presence Protocol (XMPP): Address Format • IETF RFC 6125: 2011, Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS) • IETF RFC 3923: 2004, End-to-end signing and object encryption for XMPP • IETF RFC 4854: 2007,XMPP URN A uniform Resource Name (URN) Namespace for Extensions to the Extensible Messaging and Presence Protocol (XMPP). • IETF RFC 4979: 2007, IANA registration of an Enumservice for XMPP (see IETF RFC 3761: 2004, The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)). • IETF RFC 5122: 2008, A Internationalized Resource Identifiers (IRIs) and Uniform Resource Identifier (URI) for the Extensible Mes-

ID: Service/Purpose	Standards	Implementation Guidance
		saging and Presence Protocol (XMPP)

[a]The use of G.729 may require a license fee and/ or royalty fee. DiffServ, PHB and DSCP defined by *IETF RFC 2474: 1998, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.* Please also see Table 1.3 ID 3 (IP Quality of Service).

1.3.3.2. Information Management Services

043. **Definition**: *Information Management Services provide technical services "...to direct and support the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organization." These services support organizations, groups, individuals and other technical services with capabilities to organize, store and retrieve information (in any format, structured or unstructured) through services and managed processes, governed by policies, directives, standards, profiles and guidelines.*

1.3.3.2.1. Standards

044. To provide federated services the standards listed in Table 1.9 should be adhered to. Additionally all information should be labelled with the minimum metadata set by ISAF

Table 1.9. Information Management Services and Data Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Enterprise Search Services: Automated information resource discover, information extraction and interchange of metadata	• Mandatory: ISO 15836:2009, Information and documentation - The Dublin Core metadata element set.” • Mandatory: TIDE Information Discovery (v2.3.0, Allied Command Transformation Specification, 30 October 2009.) • Emerging: TIDE Transformational Baseline 3.0 – Annex C: TIDE Service Discovery (v.2.2.0, Allied Command Transformation Specification) December 2009. • Emerging: SPARQL 1.1 Query Language, W3C Re-	ISO 15836:2009 does not define implementation detail. This profile requires a subset of metadata with UTF8 character encoding as defined in the NATO Discovery Metadata Specification (NDMS) – see The technical implementation specifications are part of the TIDE Transformational Baseline v3.0, however, Query-by-Example (QBE), has been deprecated with the TIDE Information Discovery specs v2.3.0 and replaced by SPARQL. The TIDE community is evaluating OpenSearch for potential

ID: Service/Purpose	Standards	Implementation Guidance
	commendation, 21 March 2013. • Emerging: OWL 2 Web Ontology Language Document Overview (Second Edition), W3C Recommendation, 11 December 2012. • Emerging (2014): OpenSearch 1.1 Draft 5.	inclusion into the TIDE Information Discovery specifications. On the AMN CORE a commercial product called FAST ESP is being used to generate search indexes. This product could act as an OpenSearch "slave", but requires adaptation to this Open Standard but only using HTTP. For automated information discovery across the AMN all potential information sources must provide this standard search interface in order to allow tools like FAST ESP to discover relevant information.
2: Enterprise Search Services: manual information resource discovery, classification marking and file naming conventions	• Recommended: AC322-N(2010)0025 – Guidance On File Naming	
3: Enterprise Support Guard Services: General definition of Security and confidentiality metadata	• Mandatory: NO-FFI-rapport 00961:2010, XML Confidentiality Label Syntax - a proposal for a NATO specification. • Mandatory: NO-FFI-rapport 00962: 2010, Binding of Metadata to Data Objects - a proposal for a NATO specification. • Mandatory: NCIA TN-1455-REV1, NATO Profile for the Binding of Metadata to Data Objects, Vers 1.1, December 2012.[a] • Mandatory: NCIA TN-1456-REV1, NATO Profile for the XML Confidentiality Label	Services and applications shall implement object level labelling in order to support cross-domain information exchange using common enterprise Support Guard Services (e.g. Cross-Domain Solutions or Information Exchange Gateways)

ID: Service/Purpose	Standards	Implementation Guidance
	Syntax, Vers 1.1, January 2013.[b]	

[a]NC3A TN-1455 is the NATO profile of NO-FFI 00962.

[b]NC3A TN-1456 is the NATO profile of NO-FFI 00961.

1.3.3.3. Geospatial Services

045. **Definition**: *Geospatial Services deliver network-based access to quality raster, vector and terrain data, available in varying degrees of format and complexity. Geospatial Services form a distinct class of information services through their unique requirements for collecting, converting, storing, retrieving, processing, analyzing, creating, and displaying geographic data. The generic nature of Geospatial Services - "organizing information by location" - is interdisciplinary and not specific to any Community of Interest (COI) or application.*

1.3.3.3.1. Standards

046. To provide federated services the standards listed in Table 1.10 should be adhered to.

Table 1.10. Enterprise Support Geospatial Services and Data Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Geospatial Coordinate Services: identifying Coordinate Reference Systems (CRS)	• Fading: "DGIWG Geodetic Codes and Parameters Registry", https://portal.dgiwg.org/files/?artifact_id=3071 Last updated, Sept 2000 • Recommended: EPSG registry http://www.epsg-registry.org/ , current version 8.2, dated 29 November 2013	The European Petrol Survey Group maintains the most comprehensive and accurate register of international geodetic codes and parameters for CRS. To identify the CRS for the exchange of geospatial data a standard naming convention and reference repository is required.
2: GeoWeb Service Interface to GIS Servers	• Recommended: Open Esri GeoServices REST specification Version 1.0, September 2010	There are implementations of the Open Esri GeoServices REST specification from various other vendors. The REST API may be used for an easier to implement and rich interface to the server side GIS capabilities. Functional Services that support this interface may take advantage of this interface.

ID: Service/Purpose	Standards	Implementation Guidance
3: Geo-Analytical Functionality as a Service	• Emerging (2014): Open Esri GeoServices REST specification Version 1.0, September 2010 • Emerging (2014): OGC 05-007r7 Web Processing Service 1.0.0	Instead of retrieving all required spatial data in order to analyze it in a fat client, clients are encouraged to invoke the analytical processes where the data resides so that only the analytic result needs to be transmitted from the server to the client.
4: 3D Perspective Viewer as a GeoWeb-Service	• Recommended: KML network link as part of OGC OGC 07-147r2 KM	Nil
5: Geodetic and geophysical model of the Earth.	• Mandatory: NIMA Technical Report 8350.2 Third Edition incorporating Amendments 1 and 2: 23 June 2004, Department of Defense World Geodetic System 1984 Its Definition and Relationships with Local Geodetic Systems.	
6: Electronic format for medium resolution terrain elevation data.	• Mandatory: MIL-PRF-89020 Rev. B, Performance Specification: Digital Terrain Elevation Data (DTED), 23 May 2000.	Used to support line-of-sight analyzes, terrain profiling, 3D terrain visualization, mission planning/rehearsal, and modelling and simulation.
7: Services to publish geospatial data as maps rendered in raster image formats	• Mandatory: ISO 19128:2005, Geographic information - Web map server interface (WMS v.1.3.0). • Mandatory: OGC 02-070 OpenGIS Styled Layer Descriptor (SLD) Implementation Specification v 1.0 • Fading (Dec 2012): OGC WMS v1.0.0, v1.1.0, and v1.1.1 • Emerging: OGC 05-078r4, OpenGIS Styled Layer Descriptor (SLD) Profile of the Web Map Service	WMTS are to be provided as a complimentary service to WMS to ease access to users operating in bandwidth constraint environments. WMTS trades the flexibility of custom map rendering for the scalability possible by serving of static data (base maps) where the bounding box and scales have been constrained to discrete tiles which enables the use of standard network mechanisms for scalability such as distributed cache systems to cache images between the client and the server, reducing latency and bandwidth use.

ID: Service/Purpose	Standards	Implementation Guidance
	Implementation Specification v.1.1.0, June 2007. • Emerging (2018): OGC 07-057r7, OpenGIS Web Map Tile Service Implementation Standard (WMTS) v.1.0.0, April 2010.	
8: Services to publish vector-based geospatial feature data to applications	• Mandatory: OGC 04-094, Web Feature Service (WFS) v.1.1. • Mandatory: OGC 04-095, Filter Encoding v.1.1 • Emerging: OGC 10-100r3 Geography Markup Language (GML) simple features profile (with Corrigendum) v 2.0 including OGC 11-044 Geography Markup Language (GML) simple features profile Technical Note v 2.0	
9: Electronic interchange of geospatial data as coverage, that is, digital geospatial information representing space varying phenomena	• Mandatory: OGC 07-067r2, Web Coverage Service (WCS) v.1.1.1. • Fading (Dec 2011): v1.0.0 and v1.1.0 • Emerging (2014): OGC 09-110r4, Web Coverage Service (WCS) v2.0, October 2010.	Web Coverage Service v.1.1.1 is limited to describing and requesting grid (or "simple") coverage. OGC Web Coverage Service (WCS) Standard Guidance Implementation Specification 1.0
10: File based storage and exchange of digital geospatial mapping (raster) data where services based access is not possible	• Mandatory: GeoTIFF format specification: GeoTIFF Revision 1, Version 1.8.2, December 2000.[a] • Mandatory: OGC 05-047r3: OpenGIS GML in JPEG 2000 for Geographic Imagery (GMLJP2) Encoding	This is provided for legacy systems, implementers are encouraged to upgrade their systems to consume OGC Web Services. In practice, the exchange of large geospatial(raster) data sets between Geo organizations of different TCN’s is conducted

ID: Service/Purpose	Standards	Implementation Guidance
	Specification 1.0.0, January 2006. • Recommended: MIL-PRF-89038, Performance Specification Compressed ARC Digitized Raster Graphics (CADRG). October 1994 • Recommended: MIL-STD-2411 (NOTICE 3), Department of Defense Interface Standard: Raster Product Format (31 Mar 2004).	in the proprietary[b] Multi-resolution seamless image database format (MrSID Generation 3). Data in MrSID format could be transformed to GeoTIFF.
11: File based storage and exchange of non-topological geometry and attribute information or digital geospatial feature (vector) data	• Mandatory: OGC 07-147r2, Keyhole Markup Language (KML) 2.2.0, April 2008. • Fading: ESRI White Paper, ESRI Shapefile Technical Description, July 1998. • Emerging (2014): File Geodatabase (.gdb directories). (Note: The current version of the gdb file format is defined via the application programming interface File Geodatabase API 1.3, which is used in several GIS implementations including the open source Geospatial Data Abstraction Library (GDAL)).	ESRI Shapefiles are used by legacy systems and as file based interchange format. Implementers are encouraged to upgrade their systems based on OGC Web Services. File geodatabases store datasets as folders in a file system with each file capable of storing more than 1 TB of information. Each file geodatabase can hold any number of these large, individual datasets. File geodatabases can be used across all platforms and can be compressed. They support the complete geodatabase information model and are faster than using shapefiles for large datasets. Users are rapidly adopting the file geodatabase in place of using shapefiles.
12: Geospatial Coordinate Services: general positioning, coordinate systems, and coordinate transformations	• Recommended: OGC 01-009, OpenGIS Coordinate Transformation Service Implementation Specification Revision 1.00, January 2001.	

[a]GeoTIFF 1.8.2 is public domain metadata standard embedding geo-referencing information within a TIFF revision 6.0 file.

[b]Requires LizardTech's (lizardtech.com) decoding software development kit (DSDK). The MrSID file format is a proprietary technology that provides tools for the rapid compression, viewing, and manipulation of geospatial raster and LiDAR data.

1.4. COMMUNITIES OF INTEREST SERVICES

047. **Definition**: *Communities of Interest (COI) Services support one or many collaborative groups of users with shared goals, interests, missions or business processes.*

048. COI Service will be broken up further into:

- COI Enabling Services
- COI Specific Services

1.4.1. Communities of Interest Enabling Services

049. **Definition**: *COI-Enabling Services provide COI-dependant functionality required by more than one communities of interest. They are similar to Enterprise Support Services in that they provide building blocks for domain-specific service development. The distinction between the two is that Enterprise Support Services provide generic COI-independent capabilities for the entire enterprise (e.g. collaboration and information management services) and COI-Enabling Services provide those COI-dependant services that are typically shared by a larger group of COIs (e.g. operational planning and situational awareness capabilities).*

050. For the purposes of this Volume, COI-Enabling Services will be broken up further into:

- General COI-Enabling Data Formats and Standards
- Situational Awareness Services
- Biometric Services

1.4.1.1. General COI-Enabling Data Formats and Standards

1.4.1.1.1. Standards

051. Common standards that apply to all COI Enabling Service are listed in Table 1.11. These should be adhered to if federated services are to be achieved.

Table 1.11. General Data Format Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: General definition for the Representation of Dates and Times.	• Mandatory: ISO 8601:2004, Data elements and inter-change formats - Information	Implementation of the W3C profile of ISO 8601:2004 (W3CDTF profile) is recom-mended.

ID: Service/Purpose	Standards	Implementation Guidance
	interchange - Representation of dates and times	Note: See also guidance on storage and use of time given in Table 6. IDs 1 and 4
2: General definition of letter codes for Geographical Entities	• Undetermined .	Alpha-3 codes “XXA”, “XXB”, “XXC”, “XXX” shall not be used to avoid potential conflicts with ISO/IEC 7501-1.
3: General definition of letter codes for identifying Nationality of a person	• Conditional: ISO/IEC 7501-1:2008, Identification cards -- Machine readable travel documents - Part 1: Machine readable passport.	When 3-letter codes are being used for identifying nationality, code extensions such as XXA, XXB, XXC, XXX as defined in ISO/IEC 7501-1 are to be used.
4: General definition of geospatial coverage areas in discovery metadata	• Mandatory: NIMA Technical Report 8350.2 Third Edition Amendment 1+2: 23 June 2004, Department of Defense World Geodetic System 1984 Its Definition and Relationships with Local Geodetic Systems. • Mandatory: ISO 19115:2003, Geographic information – Metadata. • Mandatory: ISO 19115:2003/ Cor 1:2006. • Mandatory: ISO 19136:2007, Geographic Information -- Geography Markup Language (GML). • Recommended: STANAG 2586 NATO Geospatial Metadata Profile	ISO 19139 provides encoding guidance for ISO 19115 STANAG 2586 includes the mandatory ISO standards, but concretizes and extends it to cope with the NATO geospatial policy. It provides a conceptual schema and an XML encoding for geospatial metadata elements that extend ISO 19115

1.4.1.2. Situational Awareness Services

052. **Definition**: *Situational Awareness (SA) Services provide the situational knowledge required by a military commander to plan operations and exercise command and control. This is the result of the processing and presentation of information comprehending the operational environment - the status and dispositions of friendly, adversary, and non-aligned actors, as*

well as the impacts of physical, cultural, social, political, and economic factors on military operations.

1.4.1.2.1. Standards

053. To provide federated services the standards listed in Table 1.12 should be adhered to.

Table 1.12. Battlespace Management Interoperability Protocols and Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Expressing digital geographic annotation and visualization on, two-dimensional maps and three dimensional globes	• Mandatory: TIDE Transformational Baseline Vers. 3.0, Annex A: NATO Vector Graphics (NVG) v1.5, Allied Command Transformation Specification, December 2009. • Fading: NVG 1.4 • Retired: NVG 0.3 • Mandatory: Open Geospatial Consortium 07-147r2, Keyhole Markup Language (KML) 2.2, April 2008.	NVG shall be used as the standard Protocol and Data Format for encoding and sharing of information layers. NVG and KML are both XML based language schemas for expressing geographic annotations.
2: Formatted military message exchange in support of: • SOA Platform Services/ Message-oriented Middleware Services • Enterprise Support Services/ Unified Communication and Collaboration Services/ Text-based Collaboration Services	• Mandatory: STANAG 5500 Ed.7:2010, Concept of NATO Message Text Formatting System (CONFORMETS) / ADatP-03 Ed. (A) Ver. 1: December 2009.	ADatP-03(A) contains two different equivalent presentations of data: one as "classic" message or alternatively as XML-MTF instance. A) Automated processing of XML-files in static facilities/systems is much easier and thus preferred for the exchange between national AMN extensions and the AMN Core. B) At the tactical edge of the AMN the "classic" message format is the preferred option as this format is "leaner" and easier

ID: Service/Purpose	Standards	Implementation Guidance
		to transmit via tactical radio systems.
3: Message formats for exchanging information in low bandwidth environments	• Mandatory: STANAG 7149 Ed. 5 NATO Message Catalogue APP-11(C) Change 1. Minimum set of messages supported by the AMN Core Network (cited in the form: MTF Name (MTF Identifier, MTF Index Ref Number)): • PRESENCE REPORT (PRESENCE, A009) • CASUALTY EVACUATION REQUEST (CASEVACREQ, A015) • ENEMY CONTACT REPORT (ENEMY CONTACT REP, A023) • INCIDENT REPORT (INCREP, A078) • MINEFIELD CLEARING RECONNAISSANCE ORDER (MINCLRRECCEORD, A095) • AIRSPACE CONTROL ORDER (ACO, F011) • AIR TASKING ORDER (ATO, F058) • KILLBOX MESSAGE (KILLBOX, F083) • AIR SUPPORT REQUEST (AIRSUPREQ, F091) • INCIDENT SPOT REPORT (INCSPOTREP, J006)	The following messages that are not compliant with STANAG 7149 Ed.5 could be accepted by the AMN Core Network: • Joint Tactical Air Strike Request (JTAR) US DD Form 1972 • SALUTE (Size, Activity, Location, Unit/Uniform, Time, Equipment) Change request proposals reflecting the requirements for those non-standard messages should be submitted within the configuration management process of ADatP-3 by those nations that are the primary originators of those messages Note: the KILLBOX MESSAGE (KILLBOX, F083) is also promulgated/referred to in Theatre as a ROZ Status message [Note that compliance of the ROZ Status use of F083 with STANAG 7149 Ed 5 has to be confirmed by AMN AWG] Notes for Emerging: • A011: Only for ISAF use • A012: Formatted message for 9-liner • J025: Formatted message to replace the NFFI format

ID: Service/Purpose	Standards	Implementation Guidance
	• SEARCH AND RESCUE INCIDENT REPORT (SARIR, J012) • EOD INCIDENT REPORT (EODINCREP, J069) • EVENTS REPORT (EVENTREP, J092) • SITUATION REPORT (SITREP, J095) Emerging (2015)[a]: • OPSITREP IRREGULAR ACTOR (OPSITREP IA, A011) • MEDICAL EVACUATION REQUEST (MEDEVAC, A012) • TROOPS IN CONTACT SALTA FORMAT (SALTATIC, A073) • FRIENDLY FORCE INFORMATION (FFI, J025) • UXO IED REPORT 10-LINER (UXOIED, A075)	• A075: Formatted message for 10-liner
4: Exchange of digital Friendly Force Information such as positional tracking information between systems hosted on a Mission Network and mobile tactical systems	• Mandatory: AC/322-D(2006)0066 Interim NATO Friendly Force Information (FFI) Standard for Interoperability of Force Tracking Systems (FFTS) • Emerging (2015): STANAG 5527 Ed. 1 / ADatP-36(A)(1), Friendly Force Tracking Systems (FFTS) Interoperability.	All positional information of friendly ground forces (e.g. ground forces of Troop Contributing Nations or commercial transport companies working in support of ISAF Forces) shall be as a minimum made available in a format that can be translated into the NFFI V1.3 format (as specified in AC/322-D(2006)0066)

ID: Service/Purpose	Standards	Implementation Guidance
5: Mediation Services: Mediate between the TDL and MN to provide weapon delivery assets with Situational Awareness on friendly forces.	• Emerging (2016): STANAG 5528 Ed: 1/ ADatP-37 Ed. A, Services to forward Friendly Force Information to weapon delivery assets.	
6: Real time automated data exchange between TDL networks.	• Mandatory: STANAG 5518, Ed.1 - Interoperability Standard for the Joint Range Extension Applications Protocol (JREAP).; see also US MIL-STD 3011 In combination with: • Mandatory: STANAG 5516, Ed.4:2008 - Tactical Data Exchange (Link16) • Mandatory: STANAG 5511, Ed.6:Feb 28, 2006 - Tactical Data Exchange (Link 11/11B); see also US MIL-STD 6011 • Mandatory: STANAG 5616 Ed.5:2011 - Standards for Data Forwarding between Tactical Data Systems employing Link 11/11B,Link 16, and Link 22.	Link-16 data is disseminated via JREAP and ad-hoc (i.e. NACT) protocols in ISAF. The transition to a full JREAP based dissemination needs to be implemented in close coordination with via the AMN Sec TMO.
7: Exchanging information on Incident and Event information to support information exploitation.	• Emerging (2014): Draft EVENTEXPLOITREP XML schema. • Recommended: NC3A JOCWatch Web Services Specification - Operational Incident Report (OIR) – 1.2, Sep 2011	This schema will be used to exchange rich and structured incident/ event information between C2 and Exploitation systems like JOCWatch and CIDNE. National capability developers are invited to contribute to the development of the final EVENTEXPLOITREP XML Schema[c]. Until the EVENTEXPLOITREP XML Schema

ID: Service/Purpose	Standards	Implementation Guidance
	• Recommended: U.S.PM Battle Command SIGACT Schema[b]	definition is finalised, it is recommended to continue to use the current draft schema also known as OIR (Operational Incident Report) and the SIGACT Schema. The SIGACT schema is used via PASS, webservices and XMPP to exchange SIGACT information at Regional Command level and below.
8: Military Symbology interoperability	• Mandatory: STANAG 2019, Ed.5:2008, Joint SmbologyAPP-6(B) • Recommended: MIL-STD-2525B (w/Change 2), Common Warfighting Symbology, Mar 2007.	Note that the different standards are not fully compatible with each other and require mapping services. A translation symbol service needs to be provided on the AMN Core Network.
9: Digital exchange of semantically rich information about Battlespace Objects	• Mandatory: MIP C2 Information Exchange data model (C2IEDM) [note: STANAG 5523 was cancelled] • Mandatory: MIP Data Exchange Mechanism (DEM) Block 2 • Mandatory: AMN MIP Implementation Profile (published in Annex A to NC3A AMN MIP Workshop Final Report). RD-3188	C2IEDM Business Rule F11.2 b is not applicable in the AMN scope. Implementations shall ensure that the use of CONTEXT-ASSOCIATION does not create circular references between CONTEXTs. AMN members implementing MIP have agreed to use C2IEDM (MIP-Block 2) due to lack of fielded MIP-Block 3.1 systems by the Nations and the limited information exchange requirements of AMN Mission Threads (i.e. no requirement for Operational planning)[d]. Any addition or expansion of this data model or data dictionaries that is deemed to be of general interest shall be submitted as a change proposal within the con-

ID: Service/Purpose	Standards	Implementation Guidance
		figuration control process to be considered for inclusion in the next version of the specification The AMN Integration Core uses Ground Tracks, Event Exploit Rep, Atom, KML, NVG and initial support for JC3IEDM as the basis for its canonical model schemas. Other Schemas of immediate interest to AMN include the US Publish and Subscribe Services (PASS) Schemas POSREP, SIGACT and GRAPHICS. Altogether allow the ingestion of Track, Unit, Object Associations (ORBAT/ TASKORG), Facilities, Control Features, Airspace Control measures, Routes[e]information and the transformation into formats that the AMN Integration Core canonical model support.

[a]APP-11(C) Change 2, which is satisfying urgent operational requirements and contains new message formats designed for ISAF and similar operations, was sadly not promulgated in 2012. Their promulgation is now forecasted for 2014 with APP-11(D) (1).

[b]It should be noted that this schema is subject to release by the US Army

[c]See http://tide.act.nato.int/tidepedia/index.php?title=TP_112:_Event_Exploitation_Reports_(EVENTEXPLOITREP)

[d]It should be noted that no further development is being pursued by the MIP community for MIP-Block 2. If AMN is to progress in line with direction of FMN, implementation needs to include MIP DEM Block 2.0 to 3.1 translation. If incorporated at the AMN Integration Core, translation of the information to other standards would also be also possible.

[e]See also https://tide.act.nato.int/tidepedia/index.php?title=C2_Integration_Cononical_Modeling.

1.4.1.3. Biometric Services

054. **Definition**: *Biometrics services record measurable biological (anatomical and physiological) and behavioural characteristics of personnel for use by automated recognition systems. Biometric enabled systems typically provide distinct services for Data Collection and for Matching/Identification.*

1.4.1.3.1. Standards

055. To provide federated services the standards listed in Table 1.13 should be adhered to. NATO is currently in the process of standardizing the exchange of biometric data under STANAG 4715 Ed 1 Biometrics Data, Interchange, Watchlisting and Reporting 3. Oct 2013,

covering AEDP-15 NATO Biometrics Data, Interchange, Watchlisting and Reporting, Ed A Vers 1, October 2013. Currently three out of 11 AMN TCNs (incl. the largest provider of biometric data for the operation), have ratified STANAG 4715 Ed 1 as "Ratifying Implementing".

Table 1.13. Biometric Data and System Interoperability Protocols and Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Interchange of Fingerprint (Type 4 and 14) data	• ANSI/NIST ITL 1-2000 • ANSI/NIST ITL 1-2007 Part 1 • EBTS 1.2 (references ANSI/NIST ITL 1-2000) • FBI EBTS v8.0/v8.1 (references ANSI/NIST ITL 1-2007) • DOD EBTS 2.0 • ISO/IEC 19794-2:2005, part 2	Use of the ISO standard over national standards is preferred.
2: Type 10 Facial	• EFTS v7.0, EFTS v7.1 • FBI EBTS v8.0/v8.1 • ANSI/NIST ITL 1-2000, 1-2007 Part 1 • EBTS 1.2 (references EFTS v7.0) • DOD EBTS v2.0 • ISO/IEC 19794-5 w/ Amd1:2007, part 5	Use of the ISO standard over national standards is preferred.
3: Type 16 Iris	• ANSI/NIST ITL 1-2000, 1-2007 Part 1 • EBTS 1.2 • ISO/IEC 19794-6	Use of the ISO standard over national standards is preferred.

ID: Service/Purpose	Standards	Implementation Guidance
4: Type 17 Iris	• ANSI/NIST ITL 1-2007 Part 1 • FBI EBTS v8.0/v8.1 (ref ANSI/NIST ITL 1-2007) • DOD EBTS v2.0 • ISO/IEC 19794-6	Use of the ISO standard over national standards is preferred.

1.4.2. Communities of Interest Specific Services

056. **Definition**: *Community of Interest (COI)-Specific Services provide specific functionality as required by particular C3 user communities in support of NATO operations, exercises and routine activities. These COI-Specific Services were previously also referred to as "functional services" or "functional area services".*

057. For the purposes of this Volume and the AMN, Standards and Implementation Instructions are currently only required for:

- Joint Intelligence, Surveillance and Reconnaissance (JISR or Joint ISR) Community of Interest (COI) Services.

1.4.2.1. JISR COI Services

058. **Definition**: *Joint Intelligence, Surveillance and Reconnaissance (JISR or Joint ISR) Community of Interest (COI) Services provide unique computing and information services for intelligence support to operations. Intelligence Support is the set of military activities that are undertaken to receive commander's direction, proactively collect information, analyze it, produce useful predictive intelligence and disseminate it in a timely manner to those who need to know.*

1.4.2.1.1. Standards

059. The NATO Intelligence, Surveillance, and Reconnaissance Interoperability Architecture (NIIA) [AEDP-2, Ed.1:2005] provides the basis for the technical aspects of an architecture that provides interoperability between NATO nations' ISR systems. AEDP-2 provides the technical and management guidance for implementing the NIIA in ISR systems. These common standards are listed in Table 1.14. These should be adhered to if federated services are to be achieved.

Table 1.14. JISR Interoperability Protocols and Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Storing and exchanging of images and associated data	• Mandatory: STANAG 4545, Ed. Amendment 1:2000, NATO Secondary Imagery Format (NSIF)	AEDP-4, Ed. 1, NATO Secondary Imagery Format Implementation Guide, 15 Jun 07, NU.
2: Providing a standard software interface for searching and retrieving for ISR products.	• Mandatory: STANAG 4559, Ed. 3:2010 (starting Dec 2011). NATO Standard ISR Library Interface (NSILI). • Fading: STANAG 4559, Ed. 2:2007 (beginning July 2011)	AEDP-5, Ed. 1, NATO Standard Imagery Library Interface Implementation Guide, TBS, NU Note: STANAG 4559, Ed.2 and Ed.3 are NOT compatible with each other (**No backwards compatibility**). The NATO provided CSD on the AMN Core network only implements Ed.3:2010).
3: Exchange of ground moving target indicator radar data	• Mandatory: STANAG 4607, Ed. 2:2007 NATO Ground Moving Target Indicator (GMTI) Format. • Emerging: STANAG 4607, Ed.3:2010.	AEDP-7, Ed. 1, NATO Ground Moving Target Indication (GMTI) Format Implementation Guide, TBS, NU
4: Provision of common methods for exchanging of Motion Imagery (MI)across systems	• Mandatory: STANAG 4609, Ed. 2:2007 NATO Digital Motion Imagery Standard. • Emerging: STANAG 4609, Ed. 3:2009.	AEDP-8, Ed. 2, Implementation Guide For STANAG 4609NDMI , June 2007, NU
5: Exchange of unstructured data (documents, jpeg imagery)	• Recommended: IPIWIG V4 Metadata Specification: 2009, Intelligence Projects Integration Working Group (IPIWG), Definition of metadata for unstructured Intelligence.	
6: Providing a standard software interface for ex changing information about sensor planning, including information about capab-	• Emerging: OGC 09-000: OGC Sensor Planning Service Implementation Standard v2.0, March 2011.	For the AMN, Sensor Planning Service implementations shall adhere to the SOAP binding as defined in OGC 09-000.

ID: Service/Purpose	Standards	Implementation Guidance
ilities of sensors, tasking of a sensors and status of sensor-planning requests.		

1.5. USER FACING CAPABILITIES

060. **Definition**: *User-Facing Capabilities express the requirements for the interaction between end users and all CIS Capabilities, in order to process Information Products in support of Business Processes. User-Facing Capabilities incorporate the User Appliances, as well as the User Applications that run on those appliances.*

061. For the purposes of this Volume, only the standards for User Applications need to be cited.

1.5.1. User Applications

062. **Definition**: *User Applications, also known as application software, software applications, applications or apps, are computer software components designed to help a user perform singular or multiple related tasks and provide the logical interface between human and automated activities.*

1.5.1.1. Standards

063. To provide federated services the standards listed in Table 1.15 should be adhered to.

Table 1.15. User Application Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Displaying content within web browsers.	• Mandatory (for legacy): HyperText Markup Language (HTML) 4.01 Specification. W3C Recommendation 24 December 1999. • Mandatory (for legacy): Extensible Hypertext Markup Language (Second Edition) XHTML 1.0. A Reformulation of HTML 4 in XML 1.0. W3C Recommendation 26 January 2000, revised 1 August 2002 • Fading (for legacy): Cascading Style Sheets (CSS), Level	Applications must support the following browsers: Microsoft Internet Explorer v9.0 and newer, and Mozilla Firefox 12.0 and newer. When a supported browser is not true to the standard, choose to support the browser that is closest to the standard[a]. Some organizations or end-user devices do not allow the use of proprietary extensions such as Adobe Flash or Microsoft Silverlight. Those technologies shall be avoided. Implementers should use open standard based

ID: Service/Purpose	Standards	Implementation Guidance

	2 (CSS 2.0), W3C Recommendation, May 1998
	
	• Mandatory (for legacy): Cascading Style Sheets (CSS), Level 2 revision 1 (CSS 2.1), W3C Recommendation, September 2009.
	
	• Emerging (2014): HyperText Markup Language, Version 5 (HTML 5), W3C Candidate Recommendation, Dec 2012.
	
	• Emerging (2014): Cascading Style Sheets (CSS) Level 3:
	
	  • Cascading Style Sheets (CSS), Level 2 revision 1 (including errata) (CSS 2.1), W3C Recommendation, June 2011.
	
	  • CSS Style Attributes, W3C Candidate Recommendation, 12 October 2010
	
	  • Media Queries, W3C Recommendation, 19 June 2012.
	
	  • CSS Namespaces Module, W3C Recommendation, 29 September 2011.
	
	  • Selectors Level 3, W3C Recommendation, 29 September 2011.
	
	  • CSS Color Module Level 3, W3C Recommendation, 07 June 2011.
		solutions instead (e.g. move to HTML5 / CSS3).
		
		Some AMN members do not allow the use of ActiveX controls in the browser. Browser plug-ins will need to be approved by AMN Change Advisory Board (CAB).

ID: Service/Purpose	Standards	Implementation Guidance
	Browser plug-ins are not covered by a single specification.	
2: Visualize common operational symbology within C4ISR systems in order to convey information about objects in the battlespace.	• Mandatory: STANAG 2019, Ed.5:2008, Joint SmbologyAPP-6(B) • Mandatory: MIL-STD-2525B (w/Change 2), Common Warfighting Symbology, Mar 2007 • Mandatory: TIDE Transformational Baseline Vers. 3.0, Annex A: NATO Vector Graphics (NVG) v1.5, Allied Command Transformation Specification, December 2009. • Fading: NVG 1.4 • Retired: NVG 0.3	All presentation service shall render tracks, tactical graphics, and MOOTW objects using this standard except in the case where the object being rendered is not covered in the standard. In these exceptional cases, additional symbols shall be defined as extensions of existing symbol standards and must be backwards compatible. These extensions shall be submitted as a request for change within the configuration management process to be considered for inclusion in the next version of the specification.
3: Reliable messaging over XMPP	XMPP Clients must implement the following XMPP Extension Protocols (XEP): • Mandatory: XEP-0184 - Message Delivery Receipts, March 2011 (whereby the sender of a message can request notification that it has been received by the intended recipient). • XEP 0202 - Entity Time, September 2009 (for communicating the local time of an entity)	All XMPP Chat Clients used on the AMN shall implement these two protocol extensions {this section will be enhanced in the next version based on a detailed recently conducted requirements analyzis}.
4: Collaborative generation of spreadsheets, charts, presentations and word processing documents	Office Open XML: • Mandatory: Standard ECMA-376, Ed. 1: December	OASIS Open Document Format ODF 1.0 (ISO/IEC 26300) and Office Open XML (ISO/IEC 29500) are both open docu-

ID: Service/Purpose	Standards	Implementation Guidance

	2006, Office Open XML File Formats.
	
	• Emerging (2013): ISO/ IEC 29500:2012, Information technology -- Document description and processing languages -- Office Open XML File Formats
	
	  • Part 1: Fundamentals and Markup Language Reference.
	
	  • Part 2: Open Packaging Conventions.
	
	  • Part 3: Markup Compatibility and Extensibility.
	
	  • Part 4: Transitional Migration Features.
	
	Open Document Format:
	
	• Recommended: ISO/IEC 26300:2006, Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0.
	
	• Recommended: ISO/IEC 26300:2006/Cor 1:2010.
	
	• Recommended: ISO/IEC 26300:2006/Cor 2:2011.
	
	• Recommended: ISO/IEC 26300:2006/Amd 1:2012, Open Document Format for Office Applications (OpenDocument) v1.1
		ment formats for saving and exchanging word processing documents, spreadsheets and presentations. Both formats are XML based but differ in design and scope.
		
		ISO/IEC TR 29166:2011, Information technology -- Document description and processing languages -- Guidelines for translation between ISO/IEC 26300 and ISO/IEC 29500 document formats.

ID: Service/Purpose	Standards	Implementation Guidance
5: Document exchange, storage and archiving	• Mandatory: ISO 19005-1:2005, Document management -Electronic document file format for long-term preservation –Part 1: Use of PDF 1.4 (PDF/A-1) • Emerging (2014): ISO 19005-2:2011, Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)	See Operational Record Retention Schedule and AMN JMEI Exit Instructions (Vol3) for further details.

6: Representation of Dates and Times	• Mandatory: W3C profile of ISO 8601 defined in:
	
	  • Date and Time Formats, W3C Note, 15 September 1997
	
	• Recommended: Working with Time Zones, W3C Working Group Note, July 2011.
	
	• Conditional (for military command and control systems):
	
	  • AAP-6:2013, NATO glossary of terms and definitions. Part 2-D-1, date-time group (DTG) format.
		See also Table 1.6 (ID 1 and 4) for time synchronization within and between systems
		
		When a DTG is expressed in local time, this must use the military time zone designator. For AFG this is D30.

7: Internationalization designing, developing content and (web) applications, in a way that ensures it will work well for, or can be easily adapted for, users from any culture, region, or language.	• Recommended: Internationalization of Web Design and Applications Current Status, http://www.w3.org/standards/ techs/i18nauthoring	Best practices and tutorials on internationalization can be found at: http://www.w3.org / International/articlelist

ID: Service/Purpose	Standards	Implementation Guidance
	• Recommended: Internationalization of Web Architecture Current Status, http://www.w3.org/standards/techs/i18nwebarch#w3c_all • Recommended: Internationalization of XML Current Status, http://www.w3.org/standards/techs/i18nxml • Recommended: Internationalization of Web Services Current Status, http://www.w3.org/standards / techs/i18nwebofservices	

[a]E.g. using http://html5test.com to compare features for HTML5.

1.6. HUMAN-TO-HUMAN COMMUNICATION

064. To work effectively in a federated mission networking environment, it is not sufficient to only standardise technical services. A key prerequisite is to also agree a common language, and terminology for force preparation, training material, user interfaces, common vocabularies etc.

1.6.1. Standards

065. To provide federated services the standards listed in Table 1.16 should be adhered to.

Table 1.16. Human-to-human interoperability Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Mutual understanding of terminology	• Recommended: General terminology: Concise Oxford English Dictionary. • Recommended: Specific military terminology: NSA AAP-6, NATO Glossary of terms and definitions.	
2: General language communication ability of staff working in a federated networking environment.	• Recommended: Standardised Language Profile (SLP) English 3222 in accordance with STANAG 6001 Version 4	As an addition to SLP Profiles the following proficiency description could also be considered[a]:

ID: Service/Purpose	Standards	Implementation Guidance
		For effective voice communications, a proficient speakers shall: 1. communicate effectively in voice-only (telephone/radio) and in face-to-face situations; 2. communicate on common, concrete and work-related topics with accuracy and clarity; 3. use appropriate communicative strategies to exchange messages and to recognize and resolve misunderstandings (e.g. to check, confirm, or clarify information) in a general or work-related context; 4. handle successfully and with relative ease the linguistic challenges presented by a complication or unexpected turn of events that occurs within the context of a routine mission situation or communicative task with which they are otherwise familiar; and 5. use a dialect or accent which is intelligible to the multinational mission community.

[a]Source: International Civil Aviation Organization (ICAO) Holistic Descriptors of operational language proficiency (adapted)

1.7. SERVICE MANAGEMENT AND CONTROL

066. **Definition**: *Service Management and Control (SMC) provides a collection of capabilities to coherently manage components in a federated service-enabled information technology infrastructure. SMC tools enable service providers to provide the desired quality of service as specified by the customer. In a federated environment such as the AMN, utilizing common process and data is a critical enabler to management of the network.*

1.7.1. Standards

067. To provide federated services the standards listed in Table 1.17 should be adhered to.

Table 1.17. Service Management and Control Interoperability Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Provide Service Management within the AMN.	• Mandatory: ITIL 2011 update / ISO/IEC 20000	See also AMN Service Management Framework CONOPS
2: Provide the Control (Governance) required to efficiently and effectively control the AMN.	• Recommended: ISACA, Control Objectives for Information and related Technology 5 Framework (COBIT 5). • Optional: TMForum Framework Business Process Framework (eTOM) Release 1.3.	COBIT is based on established frameworks, such as the Software Engineering Institute's Capability Maturity Model, ISO9000, ITIL, and ISO 17799 (standard security framework, now ISO 27001).
3: Network management	• Mandatory: IETF STD 62: 2002, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.	Details of Simple Network Management Protocol Version 3 (SNMPv3) are defined by IETF RFC 3411 - 3418:2002.
4: SOA Platform SMC Services	Web Services for Management: • Recommended: Distributed Management Task Force, WS-Management Specification Version 1.0.0 (DSP0226), 12 Feb 2008. • Recommended: Distributed Management Task Force, WS-Management CIM Binding Specification Version 1.0.0 (DSP0227), 19 June 2009.	WS-Management provides a common way for systems to access and exchange management information across the IT infrastructure.
5: Represent and share Configuration Items and details about the important attributes and relationships between them.	• Recommended: Distributed Management Task Force, CIM Schema version 2.30.0, 27 Sep 2011.	

ID: Service/Purpose	Standards	Implementation Guidance
	• Recommended: Distributed Management Task Force, CMDB Federation Specification V1.0.1, 22 Apr 2010.	

1.8. ABBREVIATIONS

068.

Table 1.18. Abbreviations

Acronym	Description
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ACO	Allied Command Operations
ACO	Air Operations... Airspace Control Order
ACP	Allied Communications Publication
ACS	Access Control Service
ACT	Allied Command Transformation
ADAMS	Allied Deployment and Movement System (FAS
ADSF®	Active Directory Federation Services
ADS®	Active Directory Services
ADS	Authoritative Data Sources/Stores (when in the context of Functional Services)
AEP	AMN European Point of Presence
AFPL	Approved Fielded Product List
AMCC	Allied Movement Coordination Cell
AMN	Afghanistan Mission Network
AMNOC	Afghanistan Mission Network Operations Centre
ANSF	Afghan National Security Forces
AOR	Area of Responsibility
APOD	Aerial Port Of Debarkation
ARCENT	Army Component of U.S. Central Command
ARRP	Alliance and Missions Requirements and Resources Plan
AS	autonomous system
ASCM	Airspace Control Measures

Acronym	Description
ATO	Air Tasking Order
AWCC	Afghan Wireless Communication Company
AWG	Architecture Working Group
BDA	Battle Damage Assessment
BE	Best Effort
Bi-SC	Bi- Strategic Command (ACO and ACT)
BGP	Border Gateway Protocol
C5ISR	Coalition Command, Control, Communications and Computers Intelligence, Surveillance, and Reconnaissance
CAB	Change Advisory Board
CBT	Computer Based Training
CDS	Cross Domain Solution
CCP	Configuration Change Proposal
CE	Crisis Establishment (manpower)
CES	Core Enterprise Services
CIAV	Coalition Interoperability Assurance and Validation
CIDNE®	Combined Information Data Network Exchange (FAS)
CIDR	Classless Inter-domain Routing
CIMIC	Civil-Military Co-operation
CIS	communication and information systems
CJMCC	Combined Joint Movement Coordination Centre
CMB	Change Management Board
CMDB	Configuration Management DataBase
CoI	Community of Interest
COIN	Counter Insurgency (Campaign)
COMIJC	Commander IJC
CONOP	Concept of Operation
COP	Common Operational Picture
COTS	Commercial Off The Shelf
CORSOM	Coalition Reception, Staging and Onward Movement (FAS)
CPU	Central Processing Unit
CPOF	Command Post of the Future (FAS)
CRCB	Crisis Response Coordination Board

Acronym	Description
CMRB	CRO Management Resource Board
CSD	Coalition Shared Database
CTE2	Coalition Test and Evaluation Environment
CUR	Crisis Response Operations Urgent Requirement
CX-I	CENTRIXS-ISAF
DCIS	Deployed CIS
DGI	Designated Geospatial Information
DML	Definitive Media Library
DNS`	Domain Name Service
DSCP	Differentiated Services Code Point
E2E	End to End (E2E)
eBGP	External BGP
ECM	Electronic Counter Measures
EG	AMN Executive Group
EVE	Effective Visible Execution Module (FAS)
FAS	Functional Area System
FDCM	Final Disconnection Coord Meeting
FMS	Foreign Military Sales
FP	Force Protection
FRAGO	Fragmentary Order
FS	Functional Service
FSC	Forward Schedule of Change
FTP	File Transfer Protocol
GAL	Global Address List
GeoMetOc	Geospatial Meteorological and Oceanographic
GIRoA	Government of the Islamic Republic of Afghanistan
HN	Host Nation
HPOV®	HP (Hewlett Packard) OpenView
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Number Authority
iBGP	internal BGP
ICC	Integrated Command and Control (FAS)
ICD	Interface Control Documentation

Acronym	Description
ICMP	Internet Control Message Protocol
IDC	Information Dominance Center (in IJC)
IEC	International Electrotechnical Commission
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
IER	Information Exchange Requirement
IETF	Internet Engineering Task Force
IFTS	ISAF Force Tracking System (FAS)
IJC	ISAF Joint Command
IKM	Information and Knowledge Management
IOC	Initial Operating Capability
IORRB	ISAF Operational Requirements Review Board
IP	Internet Protocol
IPM	Internet Performance Manager
IPS	Intrusion Prevention System
IPSLA	Internet Protocol Service Level Agreement
IPSLA-MA	IPSLA Management Agent
IPT	Integrated Planning Team
ISAB	ISAF Security Accreditation Board
ISAF	International Security Assistance Force
ISFCC	ISAF Strategic Flight Coordination Centre
ISO	International Organization for Standardization
ISR	Intelligence Surveillance and Reconnaissance
ITU	International Telecommunication Union
JALLC	Joint analyzis Lessons Learned Centre (Lisbon)
JFC	Joint Force Command
JFCBS	
JMEI	Joining, Membership and Exit Instructions
JOCWATCH	Joint Operations Centre Watchkeeper’s Log (FAS)
JOIIS	Joint Operations/Intelligence Information System (FAS)
JTS	Joint Targeting System (FAS)
KAIA-N	Kabul International Airport – North (the military portion of the Airport)

Acronym	Description
KPI	Key Performance Indicators
LAN	Local Area Network
LNO	Liaison Officer
LoA	Letter of Agreement
LogFAS	Logistics Functional Area System
LOS	Line of Sight
mBGP	Multi Protocol BGP
MAJIIC	Multi-Sensor Aerospace-Ground Joint Intelligence, Surveillance and Reconnaissance (ISR) interoperability coalition
MCI	Mission Critical Information
MEDEVAC	Medical Evacuation
MIP	Multilateral Interoperability Programme
MMR	minimum military requirement
MNDDP	Multinational Detailed (re)Deployment Plan
MOU	Memorandum of Understanding
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NATEX	National Expert
NC3B	NATO Consultation, Command And Control Board
NCI Agency	NATO Communications and Information Agency
NCIO	NATO Communications and Information Organisation
NCIRC TC	NATO Computer Incident Response Capability Technical Centre
NDSS	NATO Depot and Supply System (FAS)
NETOPS	Network Operations
NIMP	NATO Information Management Policy
NIMM	NATO Information Management Manual
NIP	Network Interconnection Point
NITB	NATO Intel Toolbox (FAS)
NRA	NATO Registration Authority
NOS	NATO Office of Security
NRT	Near Real Time
NSAB	NATO Security Accreditation Board
NTM-A	NATO Training Mission - Afghanistan

Acronym	Description
NU	NATO Unclassified
OAIS	Open Archival information System
OF-5	Officer Rank (Colonel or Equiv)
OPORDER	Operational Order
OPT	Operational Planning Team
OU	Organizational Unit
PDF/A	Portable Document Format used for digital preservation of electronic documents
PDIM	Primary Directive on Information Management
PE	Peacetime Establishment (manpower)
PKI	Public Key Infrastructure
PNG	Packet Network Gateways
POC	Point of Contact
PoP	Point of Presence
RFC	Request for Change (ITIL)
RFC	Request for Comments (Network Working Group, IETF)
PRT	Provincial Reconstruction Team
QoS	Quality of Service
RC	Regional Command
RAMNOC	Regional Afghanistan Mission Network Operations Centre
RFC	Request for Change
RIR	Regional Internet Registry
RLP	Recognised Logistics Picture
RT	Real Time
SACM	Service Asset and Configuration Management
SCCM	System Center Configuration Manager
SDD	Service Delivery Division (NCI Agency (Service Delivery))
SDE®	Service Desk Express (FAS)
SGI	Supplementary Geospatial Information (supplementary to DGI)
SHAPE	Supreme Headquarters Allied Powers Europe (i.e. HQ ACO)
SLA	Service Level Agreement
SME	Subject Matter Expert
SMF	Service Management Framework (Implementation of ITIL)

Acronym	Description
SMF	Single-mode optical fibre (Equipment)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNMP MIB	Simple Network Management Protocol Management information base
SoC	Statement of Compliance
SoF	Special Operations Forces
SOP	Standard Operating Procedure
SRTS	Service Requesting Tasking System
SSH	Secure Shell
SSL	Secure Sockets Layer
STD	Standard
SVT	Service Validation and Testing
TA	Technical Agreement
TACACS+	Terminal Access Controller Access Control System plus
TCN	Troop Contributing Nation
TDS	Trusted Data Sources
THoC	Theatre Head of Contracts
TMO	Technical Management Office (of the AMN Secretariat)
TNMA	Theatre Network Management Architect
TOA	Transfer of Authority
TPT	Technical Planning Team
TRN	Theatre Route Network
TSSB	Theatre Sustainment and Synchronisation Board
TTP	Tactics, Techniques and Procedures
UDP	User Datagram Protocol
VoIP	Voice over IP
VoSIP	Voice over Secure IP
VM	Virtual Machine
VTC	Video Tele Conference
WAN	Wide Area Network
WebTAS®	Web Enabled Temporal analyzis System (FAS)
WSUS®	Windows Server Update Services

Acronym	Description
XML	Extensible Mark-up Language

1.9. REFERENCES

069.

Table 1.19. References

Reference	Description
ADaTP-34(F)Vol4D Jan 2012	Allied Data Publication 34 (ADaTP-34(F)) STANAG 5524, NATO Interoperability Standards and Profiles (NISP), Volume 4 Interoperability Profiles and Guidance, Section D (page 93), The AMN Profile of NATO Interoperability Standards. 19 January 2012. NATO UNCLASSIFIED.
AC/322-N(2012)0092-AS1	NATO Consultation Command and Control Board. C3 Classification Taxonomy. AC/322- N(2012)0092-AS1. 19 June 2012. NATO UNCLASSIFIED.
MCM-0125-2012	Military Committee. Future Mission Network Concept MCM-0125-2012. 19 November 2012. NATO UNCLASSIFIED.
NC3A TN1417	NATO C3 Agency. Reference Document 2933, IP QoS Standardisation for the NII, RC 7, R.M. van Selm, G. Szabo, R. van Engelshoven, R. Goode, NATO C3 Agency, The Hague, The Netherlands, 15 June 2010 (Pre publication of Technical Note 1417, expected Q4 2010), NATO UNCLASSIFIED.
SHAPE CCD J6/CISO-PAMN/66/13	SHAPE CCD J6. Afghanistan Mission Network Governance Directive – Version 2. SH/CCD J6/CISOPAMN/66/13. 15 April 2013. NATO UNCLASSIFIED.
Thales ICD NIP Dec 2012	THALES Customer Service & Support, NATO SATCOM & FOC CIS for ISAF Interface Control Document (ICD) Between CISAF network and TCN networks. ICD NIP TCN_62543313_558_L. 13 December 2012, NATO UNCLASSIFIED. Made available to Troop Contributing Nations who have federated their Mission Networks to the AMN or who wish to commence the AMN joining process. Please contact the NCI Agency LNO in the AMN Secretariat Technical Management Office in SHAPE for details (NCN 254 2207/2259 or +32 6544 2207/2259).

This page is intentionally left blank