Allied Data Publication 34

(ADatP-34(J))

NATO Interoperability Standards and Profiles

Volume 3

Minimum Interoperability Profile

DECEMBER 2016

NCI Agency

Table of Contents

This page is intentionally left blank

List of Figures

This page is intentionally left blank

1. MINIMUM INTEROPERABILITY PROFILE

1.1. INTRODUCTION

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 NATO nations are engaged, they participate together with a wide variety of other organizations on the ground. Such organizations include coalition partners from non-NATO nations, Non-Governmental Organization (NGOs - e.g. Aid Agencies) and industrial partners. It is clear that the overall military and humanitarian objectives of an operation could usefully be supported if a basic level of system interoperability existed to enhance the exchange of information.

002. To support the goal of widespread interoperability this section defines a minimum profile of services and standards that are sufficient to provide a useful level of interoperability. This profile uses only those services and standards that are already part of the NISP, however it presents them as a simple and easy to follow, yet comprehensive protocol and service stack.

1.1.1. Architectural Assumptions

003. This document assumes that all participants are using IP v4 or IP v6 packet-switched, routed networks (at least at the boundaries to their networks) and that interoperability will be supported through tightly controlled boundaries between component networks and systems; these may be connected directly or via a third-party WAN (see Figure 1.1 below). A limited set of services will be supported at the boundary, these requiring server-to-server interactions only. Each nation/organization will be responsible for the security of information exchanged.

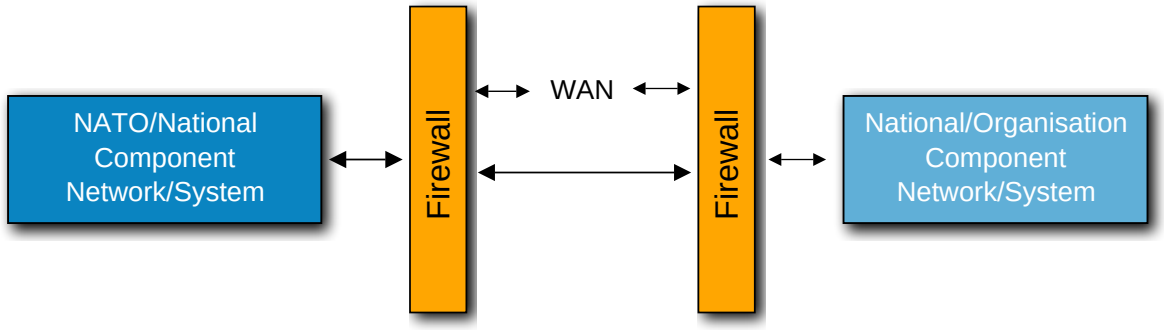

Figure 1.1. NATO to National Connectivity

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

1.1.2. Shared Services

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

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

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

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

1.1.3. Minimum Architecture

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

Table 1.1. NISP Lite

Service Area	Class	Mandatory Standard	Comments
NNEC Application Services			
COI Services			

Service Area	Class	Mandatory Standard	Comments
NNEC Core Enterprise Services			
	Messaging	SMTP (RFC 1870:1995, 2821:2001, 5321:2008)	
	Application	FTP (IETF STD 9, RFC 959:1985 updated by 2228:1997, 2640:1999, 2773:2000, 3659:2007)	
		HTTP v1.1 (RFC 2616:1999 updated by 2817:2000), URL (RFC 4248:2005, 4266:2005), URI (RFC 3938:2005)	
		Network News Transfer Protocol NNTP (RFC 3977:2006)	
		MPEG-1 (ISO 11172:1993)	
		MPEG-2 (ISO 13818:2000)	
		MP3 (MPEG1 - Layer 3)	The audio compression format used in MPEG1
	Translator	7-bit Coded Character-set for Info Exchange (ASCII) (ISO 646:1991)	
		8-bit Single-Byte Coded Graphic Char Sets (ISO/IEC 8859-1-4-9:98/98/99)	
		Universal Multiple Octet Coded Char Set (UCS) - Part 1 (ISO 10646-1:2003)	
		Representation of Dates and Times (ISO 8601:2004)	
	Data encoding	UUENCODE (UNIX 98), MIME (RFC 2045:1996 updated by 2231:1997, 5335:2008: 2046:1996, updated by 3676:2004, 3798:2004, 5147:2008, 5337:2008; 2047:1996, updated by	Base64 is used by some email products to encode attachments. It is part of the MIME std.

Service Area	Class	Mandatory Standard	Comments
		2231:1997; 2049:1996, 4288:2005, 4289:2005)	
	Mediation	Scalable Vector Graphics (SVG) 1.1 20030114, W3C	
		JPEG (ISO 10918:1994)	
		PNG vers. 1.0 (RFC 2083:1997)	
		XML 1.0 3rd ed:2004, W3C	
		HTML 4.01 (RFC 2854:2000)	
		PDF (Adobe Specification 5.1)	
		Rich Text Format (RTF)	
		Comma Separated Variable (CSV)	For spreadsheets
		Zip	
Network and Information Infrastructure Services			
	Directory	DNS (IETF STD 13, RFC 1034:1987+1035:1987 updated by 1101:1989, 1183:1990, 1706:1994, 1876:1996, 1982:1996, 1995:1996, 1996:1996, 2136:1997, 2181:1997, 2308:1998, 2845:2000, 2931:2000, 3007:2000, 3425:2002, 3597:2003, 3645:2003, 4033:2005, 4034:2005, updated by 4470:2006; 4035:2005, updated by 4470:2006; 4566:2006, 4592:2006, 5395:2008, 5452:2009)	
	Transport	TCP (IETF STD 7, RFC 793:1981 updated by 1122: 1989, 3168:2001)	
		UDP (IETF STD 6, RFC 768:1980)	

Service Area	Class	Mandatory Standard	Comments
	Network	IPv4 (STD 5, RFC 791:1981, 792:1981, 894:1984, 919:1984, 922:1984, 1112:1989 updated by RFC 950:1985, 2474:1998, 3168:2001, 3260:2002, 3376:2002, 4604:2006, 4884:2007)	Boundary/advertised addresses must be valid public addresses (i.e. no private addresses to be routed across boundary)
		Border Gateway Protocol (BGP4) (RFC 4271:2006)	

This page is intentionally left blank