NATO STANDARD

AEP-76
VOLUME I

SPECIFICATIONS DEFINING THE JOINT DISMOUNTED SOLDIER SYSTEM INTEROPERABILITY NETWORK (JDSSIN) – SECURITY

Edition A Version 3

MARCH 2023

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ENGINEERING PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

20 March 2023

1. The enclosed Allied Engineering Publication AEP-76, Volume I, Edition A, Version 2, SPECIFICATIONS DEFINING THE JOINT DISMOUNTED SOLDIER SYSTEM INTEROPERABILITY NETWORK (JDSSIN) - SECURITY which has been approved by the nations in the NATO ARMY ARMAMENTS GROUP, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4677.

2. AEP-76, Volume I, Edition A, Version 3 is effective upon receipt and supersedes AEP-76, Volume I, Edition A, Version 2, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

Dimitrios SIGOULAKIS
Lieutenant General, GRC (A)
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Documents Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Documents Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1 AIM

Standardization Agreement (STANAG) 4677 [1] on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability STANAG) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across North Atlantic Treaty Organization (NATO) or Partners for Peace (PfP) force boundaries. The DSS C4 Interoperability solution is depicted in Figure 1.

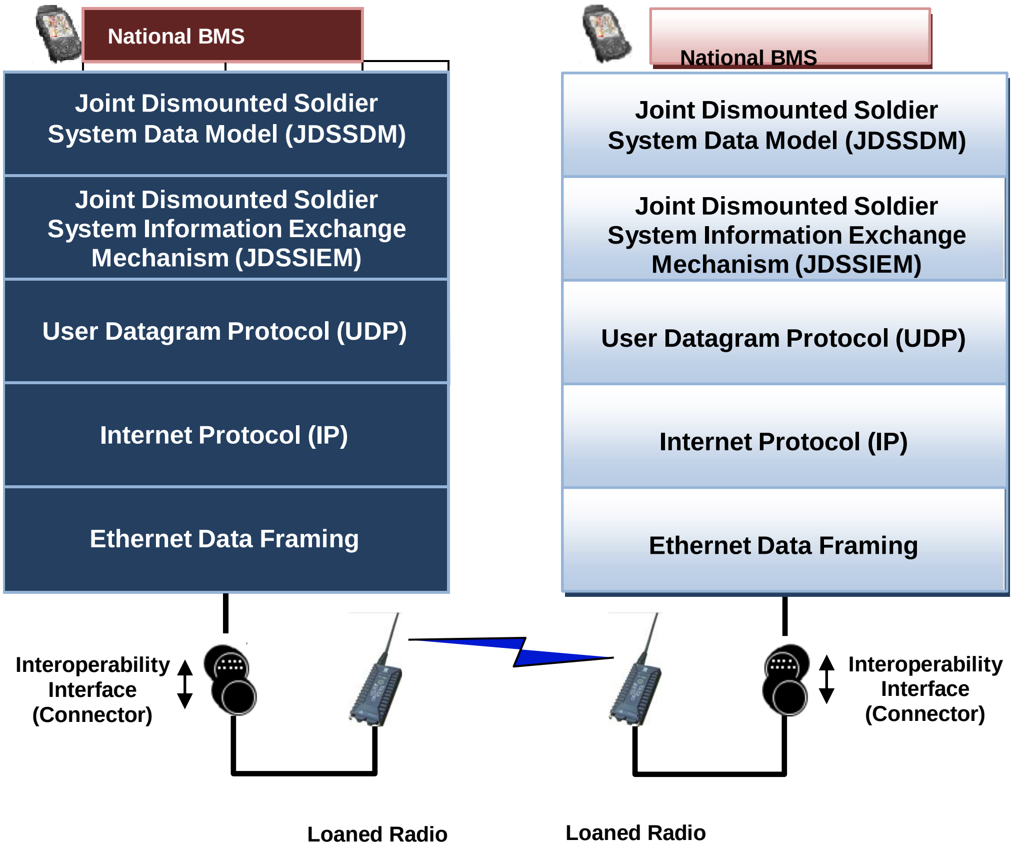
National BMS
Joint Dismounted Soldier System Data Model (JDSSDM)
Joint Dismounted Soldier System Information Exchange Mechanism (JDSSIEM)
User Datagram Protocol (UDP)
Internet Protocol (IP)
Ethernet Data Framing
National BMS
Joint Dismounted Soldier System Data Model (JDSSDM)
Joint Dismounted Soldier System Information Exchange Mechanism (JDSSIEM)
User Datagram Protocol (UDP)
Internet Protocol (IP)
Ethernet Data Framing
Interoperability Interface (Connector)
Interoperability Interface (Connector)
Loaned Radio
Loaned Radio

Figure 1 Dismounted Soldier System C4 Interoperability Solution

The DSS C4 Interoperability solution contains:

- A Joint Dismounted Soldier System (JDSS) Gateway, acting as a message translator, added to each C4 sub-system of a national DSS consisting of:
  - Joint Dismounted Soldier System Data Model (JDSSDM)
  - Joint Dismounted Soldier Information Exchange Mechanism (JDSSIEM)
  - User Datagram Protocol (UDP)
  - Internet Protocol (IP)
  - Ethernet
- A physical connection between the JDSS Gateway and the Loaned Radio based on STANAG 4619.
- A Loaned Radio.

1.2 OBJECTIVE

The objective of this Allied Engineering Publication (AEP) is to state the NATO Security Classification level deemed necessary to protect and handle the information exchange between the dismounted soldiers from two or several nations in a coalition operation as described in Ref [1].

This classification security level is NATO Restricted. The classification level is based on:

- the security threats possible for such information sharing
- threats consequences severity for such information sharing
- classification level NATO nations and PfP nations is most likely to use in their own national soldier Command, Control, Communications, Computers and Intelligence (C4I) systems

Further objective is to give guidance to which NATO security documents are relevant for implementing and using systems at the stated NATO Security Classification level. Finally to give a set of security related requirements to be met in order to accept the nation's JDSS Gateway and candidate Loaned Radio.

1.3 SCOPE

The protection of information at the lowest tactical level has a number of distinctive characteristics:

- information is often transient and perishable – it is only relevant for a short period of time
- transmission of information is confined to a small geographic area.
- information is held on portable devices which are often close to physical threats
- networks at the lower tactical are often isolated from the wider network.

In order to exchange information across force boundaries in international interoperability settings, exchange of information must be secure and trusted. The degree of security and trust associated with this exchange must be based on the above context. This security context is discussed further in Refs [3] and [15].

Within the DSS C4I approach described in Ref [1], the security domain to be implemented and handled in accordance with this AEP encompasses the entire JDSS Gateway functionality. This includes all necessary hardware and software, from the interface to the national soldier C4I system, as well as the JDSS Interoperability network (depicted in Region 1 in Figure 2). Security measures between the nations' own Soldier C4I system and the nations' JDSS Gateways are not covered within this AEP.

A nation with a national C4I soldier system with a security handling at lower levels than the JDSS Gateway cannot participate in accordance with the concept in Ref [1].

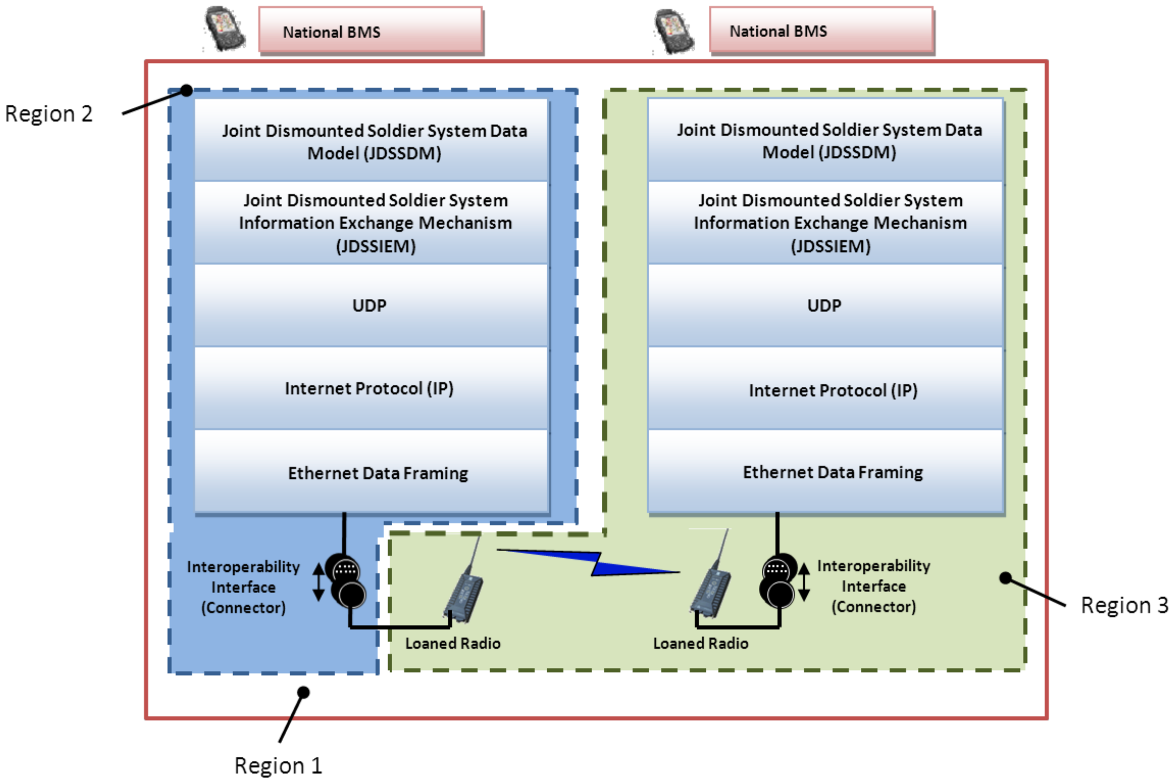
National BMS
National BMS
Region 2
Joint Dismounted Soldier System Data Model (JDSSDM)
Joint Dismounted Soldier System Information Exchange Mechanism (JDSSIEM)
UDP
Internet Protocol (IP)
Ethernet Data Framing
Joint Dismounted Soldier System Data Model (JDSSDM)
Joint Dismounted Soldier System Information Exchange Mechanism (JDSSIEM)
UDP
Internet Protocol (IP)
Ethernet Data Framing
Interoperability Interface (Connector)
Loaned Radio
Loaned Radio
Interoperability Interface (Connector)
Region 3
Region 1

Figure 2 Security Domain Coverage within JDSS

Within the security domain scope, each nation is only responsible for the security of their JDSS gateway and wired interface to the Loaned Radio (depicted by Region 2 towards the left of Figure 2). In addition, the supporting nation providing the Loaned Radio is also responsible for the security of the wireless interoperability network consisting of the Loaned Radios (depicted by the Region 3 towards the right of Figure 2).

The interoperability described in Ref [1] is between a National BMS of a NATO or PfP nation and the National BMS of another NATO or PfP nation.

This AEP relies on NATO guidance to define which security measures are necessary, how to implement these and how to use and manage the security. These references (Ref [6] - [28]) are a subset of the NATO security documents which have been identified as most relevant to the scope of this AEP. It is drawn from the NATO List of Current Information Assurance (IA) Documents. This is described as:

> *"The Section provides a list of the current documents related to Information Assurance published by the North Atlantic Council (NAC), the NATO Military Committee, the NATO Security Committee (AC/35), the NATO C3 Board (AC/322), and SECAN; noting that Information Assurance is described as follows:*

> *" the set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, non-electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, non-repudiation and authentication""*

NOTE: Some of the referenced documents are classified as NATO Restricted.

This AEP does not reproduce information held within these documents (Ref [6] - [28]), but identifies relevant documents against each requirement. There may be other relevant publications that are not contained on the NATO List of Current IA Documents.

A number of the NATO security documents provide an overview to the security processes and procedures that are related to this AEP: [6], [7], [8], [9], [11], [12], [16], [20] and [28].

1.4 REFERENCED DOCUMENTS

LCG/1 Documentation:

Ref	Document ID	Title	Revision
[1]	STANAG 4677 Edition A	Dismounted Soldier Systems Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability Standardisation Agreement (DSS C4 Interoperability STANAG)	Ed A
[2]	AEP-76, VOL. III	AEP-76, VOL.III Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – LOANED RADIO (STANAG 4677) Edition A	Ed A
[3]	NIAG Study SG123 Annex B	White Paper on Security in Joint Dismounted Soldier Systems Information Handling and Exchange	A
[4]	AEP-76, VOL. V	AEP-76, VOL.V Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Network Access (STANAG 4677) Edition A	Ed A
[5]	AEP-76, VOL. II	AEP-76, VOL.II Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) Data Model (STANAG 4677) Edition A	Ed A

North Atlantic Council (NAC) – Council Memoranda (CM)

[6]	C-M(2002)49	Security Within the North Atlantic Treaty Organization NATO Unclassified	
[7]	C-M(2007)0118	NATO Information Management Policy NATO Unclassified	
[8]	C-M(2008)0113	The Primary Directive on Information Management NATO Unclassified	

NATO Security Committee Directives – AC/35 –D/2000 series

[9]	AC/35-D/2001-	Directive on Physical Security NATO Unclassified	REV2
[10]	AC/35-D/2002	Directive on the Security of Information NATO Unclassified	REV3
[11]	AC/35-D/2004	Primary Directive of INFOSEC NATO Restricted (Releasable to certified non-NATO nations and international organizations)	REV1
[12]	AC/35-D/2005	INFOSEC Management Directive for Communication and Information Systems (CIS) NATO Unclassified	REV1
[13]	AC/35-D/1014	Guidelines for the Structure and Content of Security Operating Procedures (Sec Ops) for CIS NATO Unclassified	REV2
[14]	AC/35-D/1017	Guidelines for Security Risk Assessment and Risk Management of Communication and Information Systems (CIS) NATO Unclassified	REV2
[15]	AC/35-D/1020	Review of the Nature and Extent of the Threats to, and Vulnerabilities of, CIS NATO Restricted	REV3
[16]	AC/35-D/1034	Supporting Document on the Security Protection of NATO RESTRICTED Information NATO Unclassified	

NATO C3 Board Directives / Documents – AC/322-D/…series

[17]	AC/322-D/0047	INFOSEC Technical & Implementation Directives on Cryptographic Security and Cryptographic Mechanisms NATO Restricted (Releasable to the General Secretariat of the Council of the European Union)	REV2 (INV)
[18]	AC/322-D/0048	INFOSEC Technical & Implementation Directive for Computer and Local Area Network (LAN) Security NATO Restricted	REV1
[19]	AC/322-D/0049	INFOSEC Technical & Implementation Directive for Transmission Security NATO Restricted	
[20]	AC/322-D(2005) 0031	INFOSEC Technical & Implementation Directive for the Protection of the Confidentiality of NATO Information within non-NATO Nation Systems NATO Restricted	

NATO C3 Board Guidelines / Supporting Documents – AC/322-D/…series

[21]	AC/322-D(2004) 0033	INFOSEC Technical & Implementation Guidance on Intrusion Detection NATO Restricted	

[22]	AC/322-D(2004) 0047	INFOSEC Technical & Implementation Guidance on Recommended Modes of Operation for the Medley and AES Cryptographic Algorithms NATO Restricted	
[23]	AC/322-D(2005) 0011	INFOSEC Technical & Implementation Guidance on Cryptographic Mechanisms in Support of Non-Confidentiality Services NATO Restricted	
[24]	AC/322-D(2005) 0040	INFOSEC Technical & Implementation Guidance for the Interconnection of Communication and Information Systems (CIS) NATO Unclassified	
[25]	AC/322-D(2005) 0044	INFOSEC Technical & Implementation Guidance on Identification and Authentication NATO Restricted	
[26]	AC/322-D(2006) 0009	INFOSEC Technical & Implementation Guidance on NATO Cryptographic Algorithms in Hardware and Software NATO Restricted	
[27]	AC/322-D(2006) 0069	INFOSEC Technical & Implementation Guidance on Key Management for Cryptographic Services NATO Restricted	
[28]	AC/322-D(2007) 0046	INFOSEC Technical & Implementation Guidance on Portable Computing and Communications Devices, Land Mobile Radio Systems and Associated Wireless Technologies NATO Restricted (Releasable to the Directorate General of European Commission)	

1.5 RELATED DOCUMENTS

Document ID	Title	Revision
NIAG Study SG103 Annex F	Radio Aspects	A
NIAG Study SG103 Annex D	Overall Interoperability Architecture	A
NIAG Study SG103 Annex I	Security	A

1.6 GLOSSARY

INFOSEC	The discipline of protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction
COMPUSEC	The discipline of protecting unauthorised parties from accessing and disrupting computer systems.
COMSEC	The discipline of preventing unauthorised interceptors from accessing telecommunications in an intelligible form, while still delivering content

	to the intended recipients.
TEMPEST	Refers to compromising emanations related to unintentional signals that can contain intelligence and if intercepted and analysed can disclose potentially damaging information. TEMPEST signals come from information technology equipment that processes data and information within a military-based environment. Emanations can come from electrical, mechanical and acoustical energy which can lead to the recovery of plaintext and compromise a particular system.
TRANSEC	The discipline of preventing unauthorised parties from detecting and disrupting the transfer of information.

CHAPTER 2 OVERVIEW

This AEP has been developed to formalise the manner and way in which the nations' JDSS Gateways and the interoperability network are secured and protected in the field.

The security issues in this setting are Information Security (INFOSEC) in the widest sense; this encompasses more than just the traditional Communication Security (COMSEC). INFOSEC also includes a system approach covering Transmission Security (TRANSEC) and Computer Security (COMPUSEC).

When all nations are using relevant NATO Rules and Guidelines for handling and implementation of systems with NATO Restricted Security Classification level for COMPUSEC, COMSEC and TRANSEC, a sufficient level of assurance will be achieved for JDSS Gateways and the interoperability network (see Section1.3 SCOPE).

The JDSS Gateways and each nation's soldier C4I-system will contain information provided by another nation. This information has to be protected from falling into the wrong hands or to be distorted/falsified when transferred. The supported nation must be responsible for ensuring that a hostile opponent cannot retrieve information provided by another nation or own nation from the JDSS Gateway.

The JDSS Gateways may be subject to malicious attacks received by or residing on any connected system. It is recommended that gateway platforms need detection, neutralisation and prevention capabilities to address such threats.

It is assumed that the Loaned Radio (as described in Ref [2]) meets the requirements specified in this document regarding the protection of transfer of information. The supporting nation providing the Loaned Radio is responsible for all aspects of its security. Dissemination of security and network management information is performed prior to use, by the supporting nation providing the Loaned Radio, using appropriate management procedures including guidance on the security policies and requirements.

There is an issue that some NATO nations do not have a national equivalence security classification level to NATO Restricted. A guide to equivalence is provided in Ref [16]. Within the NATO Security Classification levels, the alternatives are NATO Confidential and NATO Unclassified. The first is deemed too severe and the latter too weak for this application.

Nations with national soldier systems at higher classification levels will have an outbound multi-level-security issue to deal with. Nations with national soldier systems which operate with a level of security protection lower than NATO Restricted may participate in the interoperability concept as described in Ref [1]. In this case, all nations participating in the interoperability network must evaluate the security risks and mitigation strategies prior to deployment (see Refs [13] and [14]).

All information residing inside the nations' JDSS Gateways and the wired side on the Loaned Radios do not require encryption as this information will be physically protected.

Figure 3 depicts the security architecture adopted for JDSS Interoperability. It outlines the major countermeasures required to protect interoperability in relation to the data transfer flow in the Open System Interconnection (OSI) type of stack defined by in this STANAG.

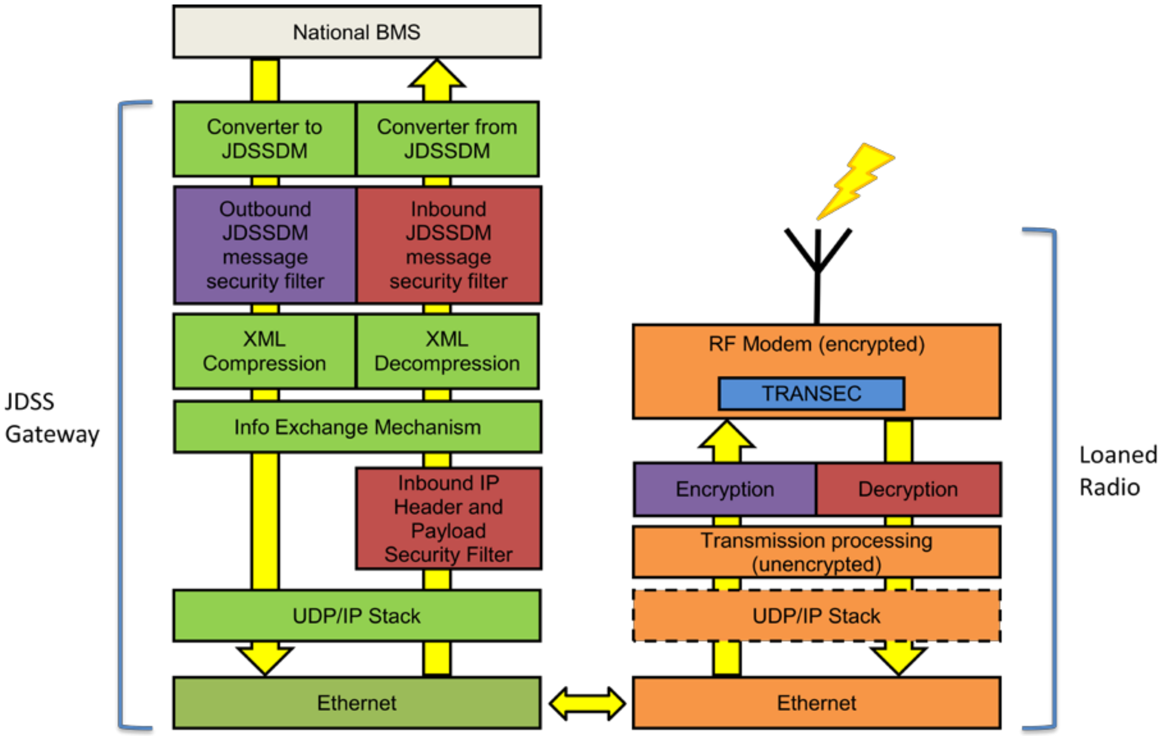

Figure 3 JDSS Security Filter Architecture

The architecture contains:

- COMPUSEC (JDSSDM Message Security Filters and an Inbound IP Header and Payload Security Filter)
- COMSEC (Encryption and Decryption)
- TRANSEC

The requirements in CHAPTER 3 SECURITY REQUIREMENTS, refer to the elements within the security architecture captured within

Figure 3. The security requirements are organised as follows:

- Section 3.1 specifies the overall security measures for the JDSS Gateways and the interoperability network.
- Section 3.2 specifies the security measures specific for the JDSS Gateways.
- Section 3.3 specifies the security measures specific for the Loaned Radio based interoperability network.

Throughout the requirements the words 'shall', 'should' and 'may' are used to state the nature of the requirements. Shall is used to identify mandatory requirements, while should is used to identify guidelines for the selection that are desirable but not mandatory. May is used to indicate a freedom of choice to be implemented on a bilateral basis between the participating nations.

CHAPTER 3 SECURITY REQUIREMENTS

3.1 OVERALL SECURITY MEASURES

Requirement 1. The implementation, the information content, the information handling and the use of the interoperating nations' JDSS Gateways and the interoperability network based on Loaned Radios (as defined in Ref [1]) shall comply with relevant rules of security level "NATO Restricted".

Requirement 2. The implemented security measures and the use of the systems should be able to counter the relevant security threats and the severity of these threats. An overview of (assumed) security threats is given in Refs [3] and [15].

Requirement 3. The information content and access to the nations' JDSS Gateways and the wired side on the Loaned Radios shall be handled and physically protected in accordance with relevant rules and guidelines of "NATO Restricted", see Refs [9] and [10].

3.2 SECURITY MEASURES FOR JDSS GATEWAY

Requirement 4. Security threats related to data conversion, handling and storage shall be dealt with in the nations' JDSS Gateways which comply with relevant NATO rules and guidelines for "NATO Restricted" (see Refs [9], [10] and [18]).

Requirement 5. The general management and security management of the JDSS Gateway shall be the responsibility of the supporting nation as each nation will have a unique version of a JDSS Gateway adapted to the nation's national soldier system (see Refs [9], [10] and [13]).

Requirement 6. Access to information residing inside the nations' JDSS Gateways may require authentication and identification of the user (see Ref [25]).

Requirement 7. The JDSS Gateways shall be certified for handling " NATO Restricted" classified information or equivalent national classification level (see Ref [16]).

Requirement 8. The physical unit containing the JDSS Gateway should have means of quickly deleting residing operational information and vital filter parameters by the user who possesses the JDSS Gateway.

Requirement 9. The physical unit containing the JDSS Gateway should have a tampering function deleting classified information when the equipment is physically tampered with (see Ref [24]).

Requirement 10. The physical unit containing the JDSS Gateway should indicate whether the equipment has been physically tampered with (see Ref [24]).

Requirement 11. The tampering function if implemented shall function both with and without connected power.

Requirement 12. The outbound data flow from the national soldier C4I-system and through the JDSS Gateway should, just after the transformation into the JDSSDM format, be checked for JDSSDM format consistency (as described in Ref [5]) (as per the Outbound JDSSDM Message Security Filter shown in Figure 3).

Requirement 13. The extracted and decompressed JDSS messages shall be checked for consistency with the content rules of JDSSDM format (as described in Ref [5]) and discarded if non-compliant (as per the Inbound JDSSDM Message Security Filter shown in Figure 3).

Requirement 14. The inbound data flow from other nations' JDSS Gateways via the Loaned Radio based interoperability network shall be checked for valid IP header content against the agreed network configuration (as described in Ref [4]) and be discarded if non-compliant (as per the Inbound IP Header and Payload Security Filter shown in Figure 3) (see Ref [21]).

Requirement 15. There shall be an indication in the equipment for the JDSS Gateway to notify if inbound IP packets contain positively detected illegal and malicious content (see Refs [18] and [24]).

Requirement 16. Information residing in the JDSS Gateway equipment should be protected to avoid unintentional radio frequency (RF) transmission of information. There are no TEMPEST restrictions on equipment processing NATO Restricted information (see Ref [16]).

3.3 SECURITY MEASURES FOR THE LOANED RADIO BASED INTEROPERABILITY NETWORK

3.3.1 General

Requirement 17. All information transmitted in a wireless manner from the Loaned Radios shall be protected against the assumed security threats on the air interface by means of COMSEC and TRANSEC measures in accordance with relevant rules and guidelines for NATO Restricted.

Requirement 18. Security threats related to the wireless transfer in the interoperability network shall be dealt with in the Loaned Radios.

Requirement 19. The Loaned Radio shall be certified for handling NATO Restricted classified information or equivalent national classification levels (for equivalence see Ref [16]).

Requirement 20. The supporting nation providing the Loaned Radios shall be responsible for setting-up and managing these radios. It seems reasonable that, from a deployment perspective, the supporting nation should be responsible for the security management of the radio when used in the JDSS interoperability network (see Refs [9], [10], [13], [20] and [27]).

3.3.2 TRANSEC

Requirement 21. The Loaned Radio should have the capability to deter jamming, avoid detection and prevent denial of service (see Ref [19]).

Requirement 22. The Loaned Radio should have a radio silence function (see Ref [19]).

3.3.3 COMSEC

Requirement 23. The Loaned Radio shall provide COMSEC measures to protect the integrity of the information content (see Refs [17], [22], [23], [26] and [27]).

Requirement 24. The COMSEC measures shall be based on encryption of the air interface transmission and reception (see Refs [17], [22], [23], [26] and [27]).

Requirement 25. The Loaned Radio shall have a zeroing function for the user to delete encryption keys and radio net parameters (see Ref [27]).

Requirement 26. The Loaned Radio should have a tampering function deleting encryption keys and radio net parameters when the equipment is physically tampered with (see Ref [24]).

Requirement 27. The Loaned Radio should have the ability to indicate if the equipment has been physically tampered with (see Ref [24]).

Requirement 28. The tampering function if implemented shall function both with and without connected power (see Ref [27]).

3.3.4 TEMPEST

Information residing in the non-encrypted section of the Loaned Radio should be protected to avoid unintentional RF transmission of information. There are no TEMPEST restrictions on equipment processing NATO Restricted information (see Ref [16]).

CHAPTER 4 MANAGEMENT PROCEDURES

The management procedures recommended for the JDSS Gateways and Loaned Radios are covered by Requirement 5 and Requirement 20: respectively.

ANNEX A ABBREVIATIONS

AEP	Allied Engineering Publication
C4	Command, Control, Communications and Computers
C4I	Command, Control, Communications, Computers and Intelligence
CIS	Communication and Information Systems
COMPUSEC	Computer Security
COMSEC	Communication Security
DSS	Dismounted Soldier System
IA	Information Assurance
INFOSEC	Information Security
IP	Internet Protocol
JDSSDM	Joint DSS Data Model
JDSSIEM	Joint DSS Information Exchange Mechanism
JDSS	Joint Dismounted Soldier System
LAN	Local Area Network
LCG/1	Land Capability Group 1
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
OSI	Open System Interconnection
PfP	Partners for Peace
RF	Radio Frequency
STANAG	Standardization Agreement
TRANSEC	Transmission Security

AEP-76 VOLI (A)(3)