ÚŘAD PRO OBRANNOU STANDARDIZACI,
KATALOGIZACI A STÁTNÍ OVĚŘOVÁNÍ JAKOSTI

ČESKÝ OBRANNÝ STANDARD

589502 **1. vydání**	**SPECIFIKACE DEFINUJÍCÍ INTEROPERABILNÍ SÍŤ SPOLEČNÉHO SYSTÉMU SESEDNUTÉHO VOJÁKA – BEZPEČNOST**

ZAVÁDÍ	STANAG 4677, Ed. 1 DISMOUNTED SOLDIER SYSTEMS STANDARDS AND PROTOCOLS FOR COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS (C4) INTEROPERABILITY (DSS C4 INTEROPERABILITY) Standardy a protokoly systémů sesednutého vojáka (DSS) pro interoperabilitu velení, řízení, spojení a výpočetní techniky (C4) (DSS C4 interoperabilita) AEP-76(A), VOL. 1 SPECIFICATIONS DEFINING THE JOINT DISMOUNTED SOLDIER SYSTEM INTEROPERABILITY NETWORK (JDSSIN) – SECURITY Specifikace definující interoperabilní síť společného systému sesednutého vojáka – bezpečnost
NAHRAZUJE	Nenahrazuje žádnou normu nebo standard

Praha 2019

(VOLNÁ STRANA)

ČESKÝ OBRANNÝ STANDARD

SPECIFIKACE DEFINUJÍCÍ INTEROPERABILNÍ SÍŤ SPOLEČNÉHO SYSTÉMU SESEDNUTÉHO VOJÁKA – BEZPEČNOST

Základem pro tvorbu tohoto standardu byly originály následujících dokumentů

STANAG 4677, Ed. 1	DISMOUNTED SOLDIER SYSTEMS STANDARDS AND PROTOCOLS FOR COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS (C4) INTEROPERABILITY (DSS C4 INTEROPERABILITY) Standardy a protokoly systémů sesednutého vojáka (DSS) pro interoperabilitu velení, řízení, spojení a výpočetní techniky (C4) (DSS C4 interoperabilita)
AEP-76, VOL. 1, Ed. A	SPECIFICATIONS DEFINING THE JOINT DISMOUNTED SOLDIER SYSTEM INTEROPERABILITY NETWORK (JDSSIN) – SECURITY Specifikace definující interoperabilní síť společného systému sesednutého vojáka – bezpečnost

Praha 2019

OBSAH

1 Předmět standardu

ČOS 589502, 1. vydání zavádí STANAG 4677, Ed. 1 a AEP-76, VOL. 1, Ed. A do prostředí ČR. Specifikuje interoperabilní síť systému sesednutého vojáka se zaměřením na bezpečnost.

2 Nahrazení standardů (norem)

ČOS nenahrazuje žádnou normu nebo standard.

3 Související dokumenty

V tomto ČOS jsou normativní odkazy na následující citované dokumenty (celé nebo jejich části), které jsou nezbytné pro jeho použití. U odkazů na datované citované dokumenty platí tento dokument bez ohledu na to, zda existují novější vydání/edice tohoto dokumentu. U odkazů na nedatované dokumenty se používá pouze nejnovější vydání/edice dokumentu (včetně všech změn).

ČOS 589501	-	SPECIFIKACE DEFINUJÍCÍ INTEROPERABILNÍ SÍŤ SPOLEČNÉHO SYSTÉMU SESEDNUTÉHO VOJÁKA
ČOS 589503	-	SPECIFIKACE DEFINUJÍCÍ INTEROPERABILNÍ SÍŤ SPOLEČNÉHO SYSTÉMU SESEDNUTÉHO VOJÁKA – DATOVÝ MODEL
ČOS 589504	-	SPECIFIKACE DEFINUJÍCÍ INTEROPERABILNÍ SÍŤ SPOLEČNÉHO SYSTÉMU SESEDNUTÉHO VOJÁKA – ZAPŮJČENÁ RADIOSTANICE
ČOS 589506	-	SPECIFIKACE DEFINUJÍCÍ INTEROPERABILNÍ SÍŤ SPOLEČNÉHO SYSTÉMU SESEDNUTÉHO VOJÁKA – PŘÍSTUP K SÍTI
NIAG STUDY SG123 ANNEX B	-	WHITE PAPER ON SECURITY IN JOINT DISMOUNTED SOLDIER SYSTEMS INFORMATION HANDLING AND EXCHANGE Bílá kniha o bezpečnosti při manipulací a výměně informací ve společných systémech sesednutého vojáka
AC/35-D/1034	-	SUPPORTING DOCUMENT ON THE SECURITY PROTECTION OF NATO RESTRICTED INFORMATION Dokument bezpečnostní ochrany NATO Restricted informací
AC/35-D/2001	-	DIRECTIVE ON PHYSICAL SECURITY Směrnice fyzické bezpečnosti
AC/35-D/2002	-	DIRECTIVE ON THE SECURITY OF INFORMATION Směrnice bezpečnosti informací
AC/35-D/1014	-	GUIDELINES FOR THE STRUCTURE AND CONTENT OF SECURITY OPERATING PROCEDURES FOR CIS Pokyny pro strukturu a obsah bezpečnostních provozních postupů pro CIS

AC/35-D/1020	-	REVIEW OF THE NATURE AND EXTENT OF THE THREATS TO, AND VULNERABILITIES OF, CIS Přehled základních hrozeb a slabých míst CIS (Utajovaný dokument NATO RESTRICTED)
AC/322-D(2005) 0040	-	INFOSEC TECHNICAL & IMPLEMENTATION GUIDANCE FOR THE INTERCONNECTION OF COMMUNICATION AND INFORMATION SYSTEMS (CIS) INFOSEC technické a prováděcí pokyny k propojení komunikačních a informačních systémů (CIS)
AC/322-D(2005) 0044	-	INFOSEC TECHNICAL & IMPLEMENTATION GUIDANCE ON IDENTIFICATION AND AUTHENTICATION INFOSEC technické a prováděcí pokyny pro identifikaci a ověřování (Utajovaný dokument NATO RESTRICTED)

4 Zpracovatel ČOS

Vojenský technický ústav, s.p., odštěpný závod VTÚVM, Ing. Martin Matějka.

5 Použité zkratky a definice

5.1 Zkratky

Zkratka	Název v originálu	Český název
AEP	Allied Engineering Publication	spojenecká technická publikace
BMS	Battle Management System	systém řízení boje
C4	Command, Control, Communications and Computers	velení, řízení, spojení a výpočetní technika
C4I	Command, Control, Communications, Computers and Intelligence	velení, řízení, spojení, výpočetní technika a inteligence
CIS	Communication and Information Systems	spojovací a informační systémy
COMPUSEC	Computer Security	počítačová bezpečnost
COMSEC	Communication Security	bezpečnost spojení
ČOS		český obranný standard
ČR		Česká republika
DoS	Denial of service	odmítnutí služby
DSS	Dismounted Soldier System	systém sesednutého vojáka
IA	Information Assurance	zajištění informací
INFOSEC	Information Security	bezpečnost informací
IP	Internet Protocol	internetový protokol
JDSS	Joint Dismounted Soldier System	společný systém sesednutého vojáka

Zkratka	Název v originálu	Český název
JDSSDM	Joint Dismounted Soldier System Data Model	datový model společného systému sesednutého vojáka
JDSSIEM	Joint Dismounted Soldier System Information Exchange Mechanism	mechanismus výměny informací společného systému sesednutého vojáka
JDSSIN	Joint Dismounted Soldier System Interoperability Network	interoperabilní síť společného systému sesednutého vojáka
LAN	Local Area Network	lokální síť
LCG/1	Land Capability Group 1	skupina pro pozemní schopnosti
NAC	North Atlantic Council	Severoatlantická rada
NATO	North Atlantic Treaty Organization	Organizace Severoatlantické smlouvy
OSI	Open System Interconnection	propojení otevřených systémů
PfP	Partnership for Peace	partnerství pro mír
RF	Radio Frequency	rádiový kmitočet
STANAG	NATO Standardization Agreement	standardizační dohoda NATO
TRANSEC	Transmission Security	bezpečnost přenosu
UDP	User Datagram Protocol	standard sady protokolů TCP/IP

5.2 Definice

Pro účely tohoto standardu se používají následující termíny a definice obsažené v tomto ČOS.

COMPUSEC Pravidlo ochrany neoprávněných přístupů a narušení výpočetních systémů.

COMSEC Pravidlo zabraňující neoprávněným odposlechům ve srozumitelné podobě z telekomunikačních linek při současném proudu informací určeným příjemcům.

IA Soubor opatření k dosažení určité úrovně důvěry v ochraně spojení, informačních a jiných elektronických systémů, neelektronických systémů a informací, které jsou uloženy, zpracovávány nebo přenášeny v těchto systémech s ohledem na důvěrnost, neporušenost, nepopiratelnost a autentizaci.

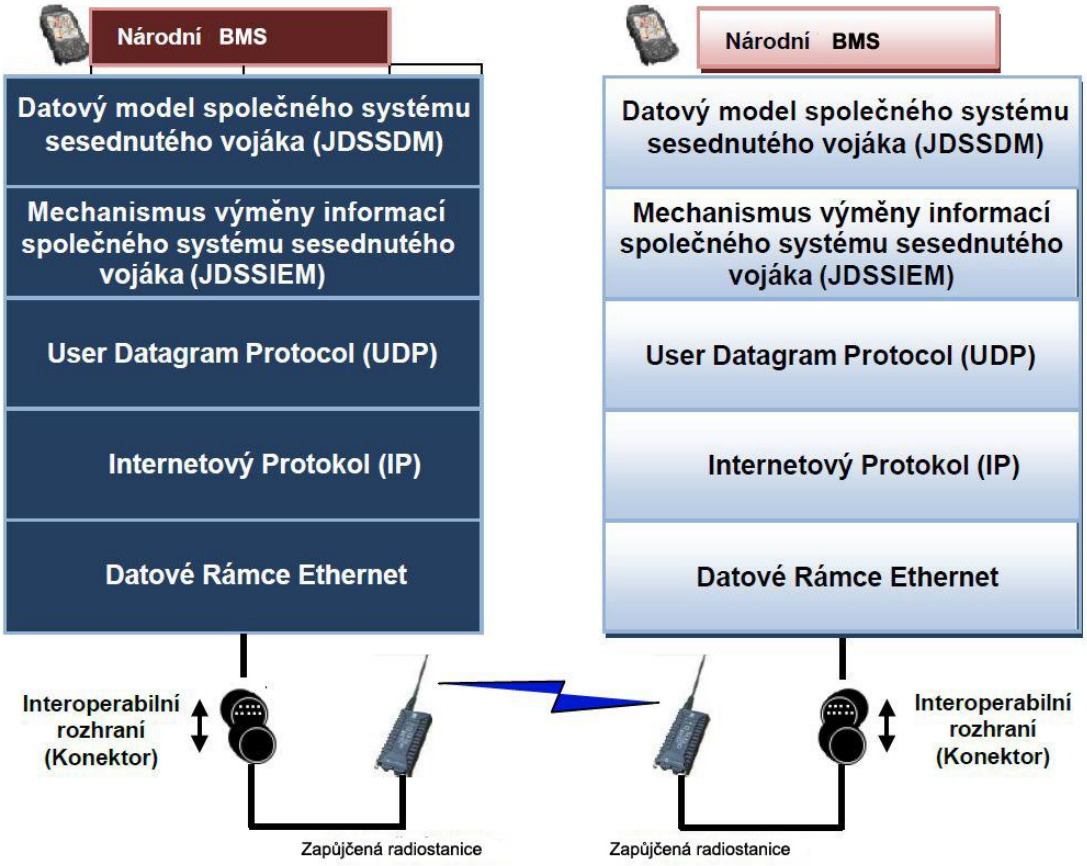
INFOSEC Pravidlo ochrany informací a informačních systémů před neoprávněným přístupem, použitím, zveřejněním, narušením, pozměněním, prostudováním, kontrolováním, nahráváním nebo zničením.

Internetový Protokol (IP) Nespojovaný síťový protokol, který poskytuje datagramovou službu s „nejvyšším výkonem“ (tzn. nezaručí doručení paketů).

Land Group One (LG/1) LCG/1	Pracovní skupina vytvořena pro sesednutého vojáka. Vzhledem k zvyšující se odpovědnosti TG/1, vytvořila Poradní skupina pro pozemní výzbroj v rámci NSA s označením NAAG plně oprávněnou skupinu LG/1. V roce 2006 NAAG přejmenoval „Land Group One“ na „ Land Capability Group One“ (LCG/1).
Podsystém	Skupina modulů, které zajišťují dané funkce nebo schopnosti. Architektura systému sesednutého vojáka, zahrnující definice podsystémů, je národní odpovědností.
Systém sesednutého vojáka (DSS)	Všechno co voják nosí, přenáší nebo využívá pro vlastní potřebu na bojišti v taktickém prostředí.
TEMPEST	Vztahuje se na vyzrazující vyzařování související s nežádoucími signály, které mohou obsahovat zpravodajskou informaci a pokud budou zachyceny a analyzovány, mohou prozradit informace s možným negativním dopadem. TEMPEST signály přicházejí ze zařízení informační techniky, která zpracovává data a informace ve vojenském prostředí. Vyzařování může pocházet z elektrické, mechanické a akustické energie, které mohou vést k získání prostého textu a tím kompromitovat (prozradit) konkrétní systém.
TG/1 Topical Group One	Skupina pro interoperabilitu vojáka. Původní skupina pod Work Group 3 pro definování standardů systémů sesednutého vojáka.
TRANSEC	Pravidlo zabraňující neoprávněným stranám detekovat a narušovat přenos informací.
UDP	Jeden ze základních protokolů internetové sady protokolů. UDP neposkytuje spolehlivost a řazení (tj. pakety mohou být přijímány mimo pořadí nebo mohou být ztraceny bez oznámení), což je efektivnější pro využití méně významných nebo rádiových přenosů. UDP používá datagramy (paket může obsahovat několik datagramů).

6 Cíl

ČOS 589502 a jeho související dokumenty popisuje standardy a protokoly systémů sesednutého vojáka (DSS) pro interoperabilitu (interoperabilita DSS C4) velení, řízení, spojení a výpočetní techniky (C4) a má za cíl umožnit interoperabilitu standardizované výměny informací mezi systémy C4 používanými sesednutými vojáky celé Organizace Severoatlantické smlouvy (NATO) nebo partnery pro mír (PfP). Toto řešení je znázorněno na obrázku 1.



OBRÁZEK 1 – Řešení interoperability C4 systému sesednutého vojáka

Řešení interoperability C4 systému sesednutého vojáka obsahuje:

- Bránu společného systému sesednutého vojáka (JDSS), zajišťující překlad zpráv, která bude přidána ke každému podsystému C4 národního DSS. Brána JDSS se skládá z:
  - Datového modelu společného systému sesednutého vojáka (JDSSDM);
  - Mechanismu výměny informací společného systému sesednutého vojáka (JDSSIEM);
  - Standardu sady protokolů TCP/IP (UDP);
  - Internetového protokolu IP;
  - Ethernetu.
- Fyzické spojení mezi bránou JDSS a společným rádiem;
- Zapůjčenou radiostanici.

7 Účel

Standard stanovuje stupeň utajení NATO, který bude nezbytný pro ochranu a zacházení s informacemi předávanými v koaliční operaci mezi sesednutými vojáky ze dvou nebo více zemí.

Stanovený stupeň utajení je **NATO Restricted**. Stupeň utajení je založen na:

- možných bezpečnostních hrozbách pro takovéto sdílení informací;

- závažnostech dopadů hrozeb pro takovéto sdílení informací;
- stupni utajení států NATO a států PfP, který se nejpravděpodobněji bude používat v jejich vlastních národních systémech velení, řízení, spojení, výpočetní techniky a zpravodajství (C4I) vojáka.

Dalším cílem tohoto standardu je specifikovat pokyny, které bezpečnostní dokumenty NATO se týkají zavedení a používání systémů v určeném stupni utajení NATO. A konečně poskytnout množinu požadavků souvisejících s bezpečností, které mají být splněny k přijetí národních bran JDSS a kandidátů na zapůjčené radiostanice.

8 Rozsah

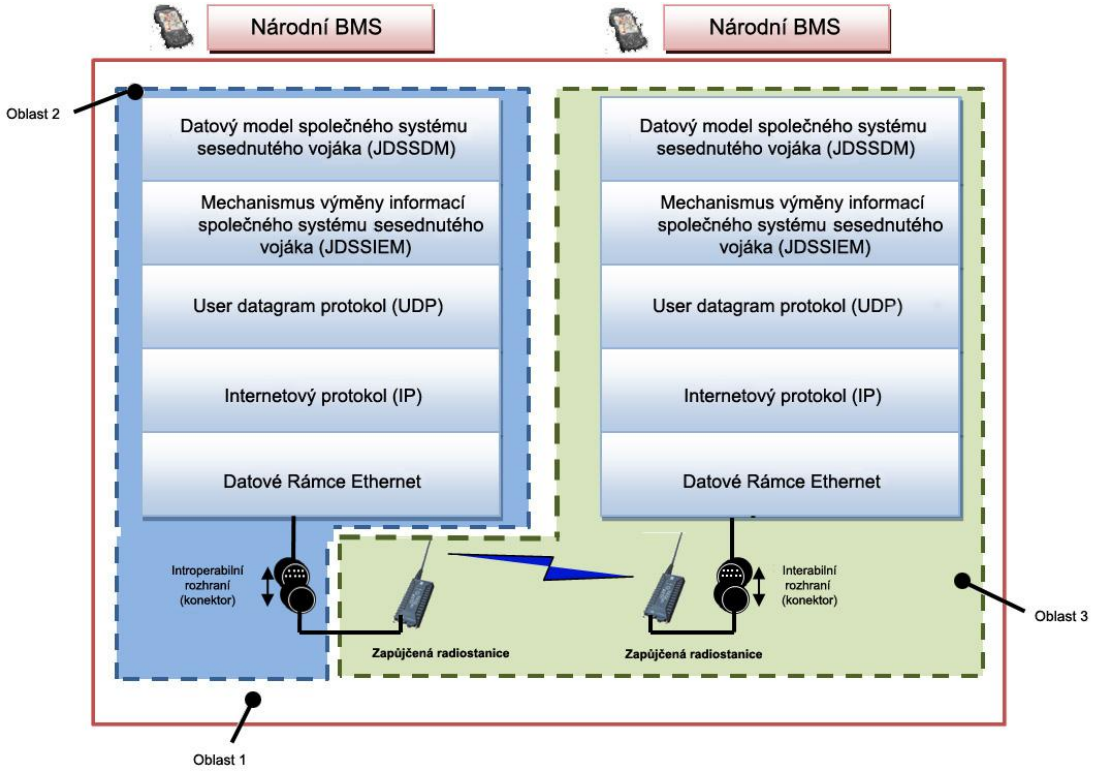
Ochrana informací na nejnižší taktické úrovni má řadu charakteristických vlastností:

- Informace jsou často krátkodobé a pomíjivé – platí pouze po krátkou dobu;
- Předávání informací je omezeno na malé geografické oblasti;
- Informace jsou uloženy na přenosných zařízeních, která jsou často v blízkosti možného fyzického ohrožení;
- Sítě na nižší taktické úrovni jsou často izolovány od rozlehlých sítí.

Aby byla zajištěna výměna informací přes rozhraní sil v mezinárodním prostředí interoperability, musí být výměna informací bezpečná a důvěryhodná. Stupeň bezpečnosti
a důvěry spojený s touto výměnou dat musí být stanoven na základě výše uvedeného kontextu. Tento bezpečnostní kontext je blíže popsán v NIAG Study SG123 Annex B.

V rámci přístupu DSS C4I popsaném v ČOS 589501, je potřeba zabezpečené oblasti realizovat a zpracovávat v souladu s tímto standardem, zahrnujícím veškerou funkcionalitu brány JDSS. Patří sem veškerý potřebný hardware a software, od rozhraní až po národní systém vojáka C4I, stejně jako interoperabilní síť JDSS (zobrazeno jako oblast 1 na obrázku 2). Bezpečnostní opatření mezi národním systémem vlastního vojáka C4I a národní bránou JDSS nejsou zahrnuty v tomto standardu.

Státy s vlastním systémem vojáka C4I, které používají zabezpečení na nižších úrovních než má brána JDSS, se nemohou v souladu s ČOS 589501 do systému zapojovat.



OBRÁZEK 2 – Pokrytí zabezpečené oblasti v rámci JDSS

V rámci bezpečnostní domény je každý stát odpovědný pouze za bezpečnost vlastní brány JDSS a kabelového připojení k zapůjčené radiostanici (zobrazeno jako oblast 2 v levé části obrázku 2). Kromě toho, stát poskytující zapůjčenou radiostanici, je rovněž odpovědný za bezpečnost bezdrátové interoperabilní sítě, skládající se ze zapůjčených radiostanic (zobrazeno jako oblast 3 v pravé části obrázku 2).

Interoperabilita (popsaná v ČOS 589501) je stanovena mezi národním BMS státu NATO nebo státu PfP a národním BMS jiného státu NATO nebo státu PfP.

Tento standard vychází z dokumentů NATO, které definují nezbytná bezpečnostní opatření včetně jejich zavedení, použití a správy. Bezpečnostní dokumenty NATO, které byly vyhodnoceny jako nejdůležitější vzhledem k rozsahu tohoto standardu, jsou popsány následně:

„Dokumenty vztahujících se k IA vydaných Severoatlantickou radou (NAC), Vojenským výborem NATO, Bezpečnostním výborem NATO (AC/322) C3 rady NATO (AC/322) a SECAN“

POZNÁMKA: Některé z těchto bezpečnostních dokumentů jsou utajovány stupněm NATO Restricted.

Tento standard nepřebírá informace obsažené v bezpečnostních dokumentech, ale uvádí příslušné dokumenty vůči každému požadavku. Mohou existovat i jiné relevantní publikace, které nejsou obsaženy v aktuálním seznamu NATO IA dokumentů.

9 Souhrn

Tento standard byl vypracován k formalizaci chování a způsobu zabezpečení a ochrany národní brány JDSS a interoperabilní sítě v terénu. Bezpečnostní otázky v tomto prostředí jsou v širším slova smyslu INFOSEC; což zahrnuje více než jen tradiční zabezpečení komunikace (COMSEC). INFOSEC zahrnuje taktéž systémový přístup pokrývající TRANSEC a COMPUSEC.

Pokud budou všechny státy používat příslušné NATO pravidla a pokyny pro zacházení
a zavedení systémů s bezpečnostní klasifikací na úrovni NATO Restricted pro COMPUSEC, COMSEC a TRANSEC, bude dosažena dostatečná úroveň zabezpečení pro bránu JDSS a interoperabilní síť.

Brány JDSS a každý národní systém vojáka C4I bude mít k dispozici informace poskytované jinými státy. Tyto informace musí být chráněny před předáním do cizích rukou nebo musí být zkreslené/zfalšované při jejich předávání. Zabezpečovaný stát musí být odpovědný za to, že protivník nemůže získat informace poskytované jiným státem nebo vlastním státem z brány JDSS.

Brána JDSS může být cílem škodlivých útoků z kteréhokoliv připojeného systému. Je doporučeno, aby brány k řešení takových hrozeb obsahovaly detekční, neutralizační a preventivní prostředky.

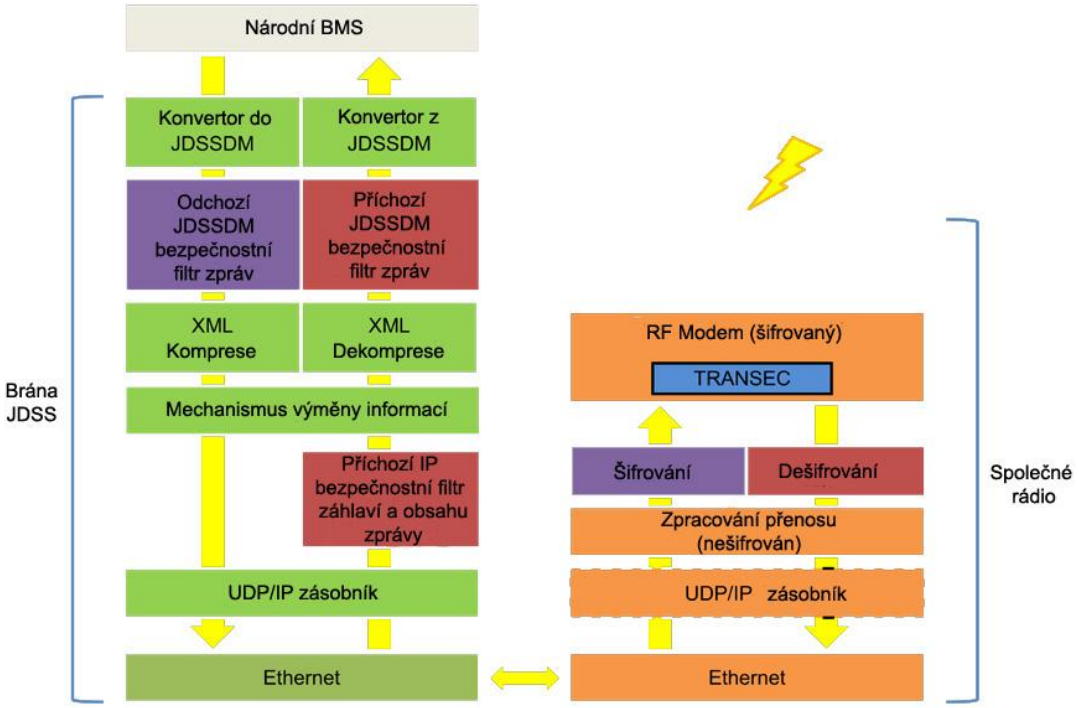
Zapůjčená radiostanice (popsána v ČOS 589504) bude splňovat požadavky týkající se ochrany přenosu informací uvedené v tomto dokumentu. Zabezpečující stát, poskytující zapůjčenou radiostanici, je zodpovědný za všechny aspekty bezpečnosti. Rozšiřování bezpečnosti a správa sítě se provádí před reálným nasazením, za podpory státu poskytujícího zapůjčenou radiostanici, pomocí vhodných postupů pro řízení, včetně pokynů bezpečnostních zásad a požadavků.

Může nastat problém, pokud některé státy nebudou mít národní bezpečnostní stupeň utajení rovnocenný se stupněm utajení NATO Restricted. Jednotlivé stupně utajení jsou popsány v AC/35-D/1034. V rámci stupňů utajení NATO jsou alternativou stupně NATO Confidential a NATO Unclassified. První z nich je považován pro tuto aplikaci za příliš silný a druhý za příliš slabý.

Státy s národními systémy vojáka na vyšší úrovni klasifikace budou řešit víceúrovňové zabezpečení odchozích informací. Státy s národními systémy vojáka používající nižší úroveň ochrany bezpečnosti než NATO Restricted, se mohou podílet na konceptu interoperability v souladu s ČOS 589501. V tomto případě musí před nasazením všechny státy zapojené do interoperabilní sítě vyhodnotit bezpečnostní rizika a strategie jejich případného zmírnění.

Veškeré informace nacházející se uvnitř národních bran JDSS a kabelových částí zapůjčené radiostanice nevyžadují šifrování, jelikož tyto informace budou fyzicky chráněny.

Obrázek 3 znázorňuje architekturu zabezpečení, která byla přijata pro interoperabilitu JDSS. Nastiňuje hlavní opatření, která jsou nutná k ochraně interoperability ve vztahu k přenosu dat v otevřeném systému propojení (OSI), stanovená v rámci pracovní skupiny Land Capability Group 1 (LCG/1).



OBRÁZEK 3 – Architektura bezpečnostního filtru JDSS

Architektura obsahuje:

- COMPUSEC (bezpečnostní filtry zpráv JDSSDM a příchozí IP bezpečnostní filtr hlavičky a těla);
- COMSEC (šifrování a dešifrování);
- TRANSEC.

Požadavky uvedené v kapitole 10 odkazují na prvky v bezpečnostní architektuře zobrazené na obrázku 3. Požadavky na zabezpečení jsou organizovány takto:

- Kapitola 10.1 specifikuje celkové bezpečnostní opatření pro brány JDSS a interoperabilní síť;
- Kapitola 10.2 specifikuje bezpečnostní opatření pro brány JDSS;
- Kapitola 10.3 specifikuje bezpečnostní opatření pro zapůjčenou radiostanici.

10 Bezpečnostní požadavky

10.1 Celková bezpečnostní opatření

Požadavek 1

Provedení, informační obsah, zacházení s informacemi a používání národních bran JDSS a interoperabilních sítí založených na zapůjčených radiostanicích, musí být v souladu s příslušnými pravidly NATO Restricted.

Požadavek 2

Realizovaná bezpečnostní opatření a používané systémy mají být schopny čelit odpovídajícím bezpečnostním hrozbám a závažnostem těchto hrozeb. Přehled (předpokládaný) bezpečnostních hrozeb je uveden v ČOS 589501 a AC/35-D/1020.

Požadavek 3

Informační obsah a přístupy k národním branám JDSS včetně kabeláže zapůjčených radiostanic musí být zpracovány a fyzicky chráněny v souladu s příslušnými pravidly a pokyny NATO Restricted, viz AC/35-D/2001 a AC/35-D/2002.

10.2 Bezpečnostní opatření pro bránu JDSS interoperabilní sítě DSS

Požadavek 4

Bezpečnostní hrozby spojené s konverzí dat, jejich manipulací a skladováním musí být řešeny v národních branách JDSS v souladu s příslušnými pravidly NATO a pokyny pro NATO Restricted, viz AC/35-D/2001 a AC/35-D/2002.

Požadavek 5

Celková správa a bezpečnost řízení brány JDSS musí být v odpovědnosti zabezpečujícího státu, jelikož každý stát bude mít jedinečnou verzi brány JDSS přizpůsobenou národnímu DSS daného státu, viz AC/35-D/2001, AC/35-D/2002

a AC/35-D/1014.

Požadavek 6

Přístup k informacím nacházejícím se uvnitř národních bran JDSS může vyžadovat ověření a identifikaci uživatele, viz AC/322-D(2005)0044.

Požadavek 7

Brány JDSS musí být certifikovány pro práci s utajovanými informacemi na stupeň NATO Restricted nebo na odpovídající národní stupeň utajení, viz AC/35-D/1034.

Požadavek 8

Fyzické zařízení, které tvoří bránu JDSS, má mít prostředky k rychlému odstranění uložených operačních informací a důležitých parametrů filtru uživatelem, který je držitelem brány JDSS.

Požadavek 9

Fyzické zařízení, které tvoří bránu JDSS, má mít ochrannou funkci zajišťující smazání utajovaných informací, v případě fyzického narušení, viz AC/322-(2005)0040.

Požadavek 10

Fyzické zařízení, které tvoří bránu JDSS, má signalizovat, zda bylo zařízení fyzicky narušeno, viz AC/322-D(2005)0040.

Požadavek 11

Pokud je zavedena funkce hlídání fyzického narušení zařízení, musí být zajištěna tato funkce i při odpojení napájení.

Požadavek 12

Odchozí tok dat z národního systému vojáka C4I přes bránu JDSS má být po transformaci do formátu JDSSDM okamžitě zkontrolován na neporušenost formátu JDSSDM, viz ČOS 589503.

Požadavek 13

Extrahované a dekomprimované zprávy JDSS musí být kontrolovány ve shodě s pravidly obsahu formátu JDSSDM (viz ČOS 589503). Pokud nejsou vyhovující (dle bezpečnostního filtru příchozí zprávy JDSSDM znázorněného na obrázku 3), musí být vymazány.

Požadavek 14

Příchozí tok dat z jiných národních bran JDSS přes zapůjčenou radiostanici (tvořící interoperabilní síť), musí být kontrolován na platný obsah záhlaví IP ve vztahu k dohodnuté konfiguraci sítě (viz ČOS 589506). Tento datový tok musí být smazán, pokud není kontrola vyhovující (dle příchozího IP bezpečnostního filtru záhlaví a obsahu zprávy na obrázku 3).

Požadavek 15

Brány JDSS musí být vybaveny indikací, která upozorní na příchozí IP pakety, které mají nedovolený nebo škodlivý obsah, viz AC/322-D(2005)0040.

Požadavek 16

Informace nacházející se v bráně JDSS mají být chráněny proti neúmyslnému radiofrekvenčnímu přenosu informací. Nejsou vyžadována žádná TEMPEST omezení pro zařízení zpracovávající NATO Restricted informace, viz AC/35-D/1034.

10.3 Bezpečnostní opatření pro zapůjčenou radiostanici interoperabilní sítě DSS

Obecně

Požadavek 17

Všechny bezdrátově přenášené informace ze zapůjčené radiostanice musí být chráněny proti předpokládaným bezpečnostním hrozbám v radiovém prostředí pomocí COMSEC a TRANSEC opatření, v souladu s pravidly a pokyny pro NATO Restricted.

Požadavek 18

Bezpečnostní hrozby související s bezdrátovým přenosem v interoperabilní síti musí být ošetřeny v zapůjčené radiostanici.

Požadavek 19

Zapůjčená radiostanice musí být pro manipulaci certifikována na utajovaný stupeň NATO Restricted nebo ekvivalentní národní klasifikační stupeň, viz AC/35-D/1034.

Požadavek 20

Zabezpečující stát poskytující zapůjčenou radiostanici, musí být odpovědný za nastavení
a správu těchto radiostanic. Při nasazení má být odpovědný za bezpečnost užívání radiostanice v interoperabilní síti JDSS rovněž zabezpečující stát, viz AC/35-D/2001, AC/35-D/2002 a AC/35-D/1014.

TRANSEC

Požadavek 21

Zapůjčená radiostanice má být odolná proti rušení, zamezit detekci a čelit DoS útokům.

Požadavek 22

Zapůjčená radiostanice má být vybavena funkcí radiový klid.

COMSEC

Požadavek 23

Zapůjčená radiostanice musí poskytovat ochranná opatření COMSEC k ochraně neporušenosti obsahu informací.

Požadavek 24

COMSEC opatření musí být založeny na šifrování radiového přenosu (na vysílací i přijímací straně).

Požadavek 25

Zapůjčená radiostanice musí mít mazací (nulovací) funkci, která odstraní šifrovací klíče a nastavené parametry rádiové sítě.

Požadavek 26

Zapůjčená radiostanice má být vybavena ochranou, která smaže šifrovací klíče a nastavené parametry radiové sítě při nedovolené fyzické manipulaci se zařízením, viz AC/322-D(2005)0040.

Požadavek 27

Zapůjčená radiostanice má mít schopnost indikace, pokud bylo se zařízením nedovoleně fyzicky manipulováno, viz AC/322-D(2005)0040.

Požadavek 28

Pokud je zařízení vybaveno funkcí, která hlídá nedovolenou fyzickou manipulaci se zařízením, musí být tato funkce v činnosti s i bez připojeného napájení.

TEMPEST

Informace nacházející se mimo šifrovanou sekci zapůjčené radiostanice mají být chráněny před nežádoucím radiovým přenosem informací. Nejsou stanovena žádná TEMPEST omezení pro zařízení zpracovávající NATO Restricted informace,

viz AC/35-D/1034.

(VOLNÁ STRANA)

(VOLNÁ STRANA)

(VOLNÁ STRANA)

Účinnost českého obranného standardu od: **13. prosince 2016**

Změny:

Změna číslo	Účinnost od	Změnu zapracoval	Datum zapracování	Poznámka

Upozornění: Oznámení o českých obranných standardech jsou uveřejňována měsíčně ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví v oddíle „Ostatní oznámení“ a Věstníku MO.

V případě zjištění nesrovnalostí v textu tohoto ČOS zasílejte připomínky na adresu distributora.

Rok vydání: 2019, obsahuje 10 listů
Distribuce: Odbor obranné standardizace Úř OSK SOJ, nám. Svobody 471/4, 160 01 Praha 6
Vydal: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti www.oos.army.cz