PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část
ÚVOD

Dokument obsahuje:	Krycí list, manažerské shrnutí a seznam zkratek
Verze:	5.1
Schválil za Dodavatele:	Tomáš Paško
Datum aktualizace:	30/10/2013

Obsah

01. Krycí list dokumentu 3
02. Manažerské shrnutí 4
03. Ekonomika - investice 5
04. Seznam zkratek a pojmů NIS IZS 6
05. Příloha Č.1 7
06. Příloha Č.2 10

01. Krycí list dokumentu

Základní údaje o dokumentu

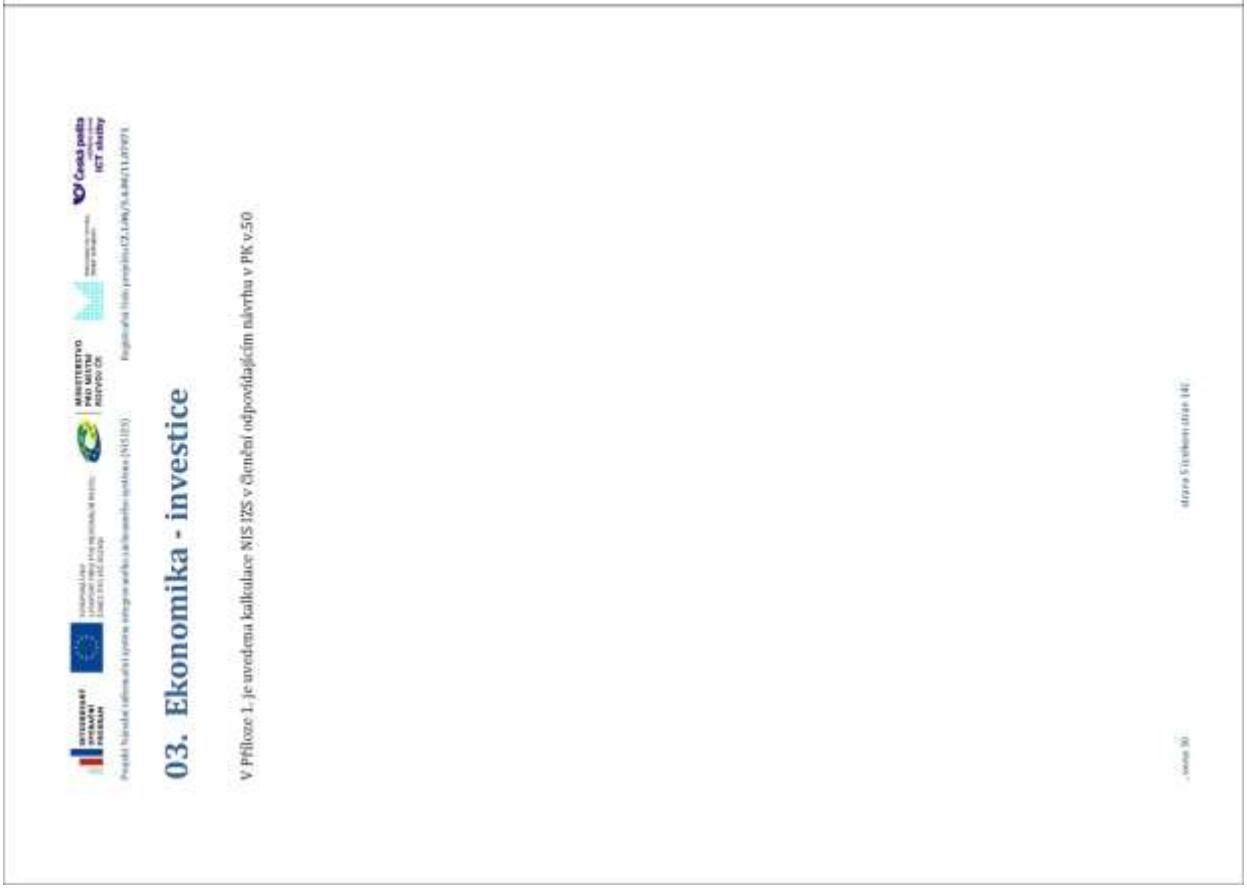
Název dokumentu	PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ
Zkrácený název dokumentu	PK
Forma předání dokumentu	elektronická (DVD), formáty DOC, XLS, MPP, PDF, EA, ADB
Název projektu	Národní informační systém integrovaného záchranného systému
Zkrácený název projektu	NIS IZS
Registrační číslo projektu	CZ.1.06/3.4.00/11.07071
Dotační titul projektu	Integrovaný operační program
Zadavatel	MINISTERSTVO VNITRA - generální ředitelství Hasičského záchranného sboru České republiky Kloknerova 2295/26, 148 01 Praha 414
Věcný gestor projektu	plk. Ladislav Prudil
Dodavatel	Česká pošta, s.p., Odštěpný závod ICT služby Olšanská 4, 130 00 Praha 3
Gestor projektu za dodavatele	Ing. Tomáš Fadko

Verze dokumentu

VERZE	ÚČEL	DNE	DOKUMENT
1.0	k akceptaci, nebyl akceptován	14/06/2013	předávací protokol
2.0	pracovní	průběžně	
3.0	pracovní k připomínkám	20/8/2013	
4.0	k připomínkám	4/10/2013	předávací protokol
5.0	k akceptaci, nebyl akceptován	21/10/2013	předávací protokol
5.1	k akceptaci	30/10/2013	předávací protokol

02. Manažerské shrnutí

Účel PK	Účelem dokumentu je: - detailně popsat dodávaný IS NIS IZS - specifikovat nároky na součinnost Zadavatele při instalaci a oživení IS NIS IZS - specifikovat harmonogram dodávek IS NIS IZS - specifikovat požadavky na síťové přenosy ITS pro pokrytí funkcionality IS NIS IZS včetně definování požadované formy zajištění (VPN, QoS) - specifikace dekompozice IS NIS IZS - specifikace požadavků na telefonní operátory z hlediska primárního a záložních připojení - vyčíslení nákladů na provoz (vč. podpory, údržby, reportingu a monitoringu IS NIS IZS) - popis zajištění systémové i objektové bezpečnosti - specifikace možných případů havárie IS NIS IZS a způsob jejich řešení - definice testů (vč. harmonogram a způsob zajištění) - plán školení.
Vstupní dokumentace	Rámcový koncept SW řešení (RK), připomínky k PKv40, schválený návrh změny architektury NIS ISZ na AAA (active – active – active).
Navazující dokument	Funkční prototyp (FP)
Členění PK	Jednotlivé kapitoly jsou vzhledem k rozsahu zpracovány v těchto samostatných dokumentech: A. Dodávaný HW B. Dodávaný SW C. Síťová infrastruktura D. Harmonogram dodávek E. Specifikace provozu F. Bezpečnostní projekt G. Výpočet spolehlivosti H. Testování I. Školení J. Telefonie.



03. Ekonomika - investice

V Příloze 1. je uvedena kalkulace NIS IZS v členění odpovídajícím návrhu v PK v.50

04. Seznam zkratek a pojmů NIS IZS

V Příloze 2. je uveden seznam zkratek a pojmů.

05. Příloha č.1

Struktura ceny projektu
(investice)
verze 51 ze 30.10.2013

Níže uvedená tabulka struktury ceny je informativní a není pro Dodavatele závazná. Byla kalkulována na základě aktuálního návrhu technického řešení. Skutečná cena jednotlivých částí dodávek je závislá na výsledcích cenových jednání v rámci obchodního zajištění. Dodavatel je limitován celkovou cenou za projekt NIS IZS jako nepřekročitelnou.

Ozn.	Položka	ks	cena/ks tis. Kč bez DPH	cena celkem tis. Kč bez DPH
HW01	CDC Servery	3	5 000	15 000
HW02	CDC Storage (diskové pole)	3	3 500	10 500
HW03	CDC Systémový SW	3	2 040	6 120
HW04	CDC - 10 GE Infrastruktura (router, FW, switch, LB)	3	12 000	36 000
HW05	CDC Archivace a zálohování	3	7 000	21 000
HW06	KDC Servery	13	600	7 800
HW07	KDC Storage (diskové pole) pro kraje	1	13 200	13 200
HW08	KDC Systémový SW pro kraje	1	14 500	14 500
HW09	Infrastruktura krajských lokalit s KDC	1	35 708	35 708
HW10	Infrastruktura krajských lokalit bez KDC	1	39 900	39 900
HW11	Telefonie KDC - HW pro kraje (vč. hlasových bran)	1	25 200	25 200
HW12	Pracoviště NSPTV	62	100	6 200
HW13	Hybridní pracoviště typu 1 (HZS)	29	94	2 726
HW14	Hybridní pracoviště typu 2 (PČR)	66	70	4 620
HW15	Hybridní pracoviště typu 3 (ZZS-a)	54	116	6 264
HW16	Hybridní pracoviště typu 3 (ZZS-b)	61	68	4 148
HW17	Multifunkce A4, laser color	41	38	1 558
HW	**Celkem HW**			**250 444**
GISSW01	GIS server CDC	3	2 920	8 760
GISSW02	GIS server KDC	13	1 570	20 410
GISSW03	GIS klient NSPTV runtime (krabicový-COTS SW)	300	0	0
GISSW04	GIS maintenance a support (1 rok)	0,5	7 668	3 834
GISSW05	GIS mapové podklady	1	3 500	3 500
GISSW06	GIS mapové podklady (maintenance/rok)	1	875	875
GISSW	Celkem GIS SW			37 379
SWIPL01	SW nahrávání pro kraje (záznamové jednotky, řízení záznamu, replikace, archivace)	1	15 200	15 200
SWIPL02	SW CTI a záznam IP telefonie pro kraje	618	8	4 944
SWIPL03	Telefonie KDC - SW pro kraje	1	7 000	7 000
SWIPL	Celkem IPL SW			27 144
SW	**Celkem SW**			**64 523**
SWA01	Solution Architect (ManDays)	120	12	1 440
SWA02	IT Architect (ManDays)	108	12	1 296
SWA03	Vedoucí vývojář (ManDays)	120	11	1 320
SWA04	Specialista bezpečnost (ManDays)	40	12	480
SWA05	Specialista provoz (ManDays)	15	11	165
SWA06	Specialista DC/networking (ManDays)	8	10	80
SWA07	Specialista ITS (ManDays)	15	10	150
SWA08	Analytik APL (ManDays)	240	12	2 880
SWA09	Architekt APL (ManDays)	120	10	1 200
SWA10	Architekt IPL (ManDays)	20	10	200
SWA11	Architekt TLF (ManDays)	40	10	400
SWA12	Architekt GIS (ManDays)	40	10	400
SWA13	Architekt infrastruktura (ManDays)	5	10	50
SWA14	Metodik vývoje (ManDays)	10	10	100
SWA15	Programátor GIS (ManDays)	120	8	960
SWA16	Programátor IPL (ManDays)	120	8	960
SWA17	Programátor TLF (ManDays)	30	8	240
SWA18	Programátor UI (ManDays)	240	8	1 920
SWA19	Tester (ManDays)	30	5	150
SWA20	Technolog analytik (ManDays)	20	5	100
SWA21	Systémový inženýr (ManDays)	20	5	100
SWA22	Specialista datových sítí (ManDays)	5	8	40
SWA23	Technik VT (ManDays)	60	4	240
SWA24	Vedoucí projektu (ManDays)	540	15	8 100
SWA25	Dokumentátor (ManDays)	230	12	2 760
SWA26	Back Office podpora (ManDays)	540	8	4 320
SWA	**Celkem vývoj aplikačního SW (multilicence)**			**30 051**
SW	**Celkem SW**			**94 574**
NIS01	**NIS celkem (bez Prahy)**			**345 018**

Dodávka pro OS základních složek IZS hl. města Prahy

HW18	KDC Server a Storage	1	1 488	1 488
HW12	Pracoviště NSPTV	10	100	1 000
HW13	Hybridní pracoviště typu 1 (HZS)	5	94	470
HW14	Hybridní pracoviště typu 2 (PČR)	12	70	840
HW15	Hybridní pracoviště typu 3 (ZZS-a)	10	116	1 160

HW16	Hybridní pracoviště typu 3 (ZZS-b)	0	68	0
HW17	Multifunkce A4, laser color	3	38	114
GISSW02	GIS server KDC	1	1 570	1 570
PHA01	**Celkem**			**6 642**

06. Příloha č.2

NIS IZS

Seznam zkratek a pojmů

Zkratka	Vysvětlení
Add-Drop Multiplex	Optický filtr, který vyděluje jenom část optického spektra
AIS	Agendový informační systém
API	Aplication Programing Interface, rozhraní pro programování aplikací
APV	Aplikační programové vybavení, aplikační SW
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol - dynamický směrovací protokol
BPMN 2.0	Business Process Management Notation, verze 2.0
BR	Business Rule
BT	Bezpečnostní testy
CAL	Client Access Licence - Licence pro přístup ke specifikovaným službám softwaru Microsoft
CC	směrování hovorů
CDC	Centrální datové centrum – celkem 3 instance, v různých lokalitách
CERT	Computer Emergency Response Team
CMS	Centrální místo služeb
CoS	Class of Service
CPE	Customer premises equipment
CRR	Centrum pro regionální rozvoj ČR
CTI	Computer – Telephony Integration
CUCM	Cisco Unified Communications Manager
ČD1	1. přípojné místo do páteřní sítě ČDT
ČD2	2. přípojné místo do páteřní sítě ČDT
ČDT	ČD - Telematika a.s.
ČP OZ	Česká pošta, s.p. odštěpný závod ICT služby
ČSN	Česká státní norma
DB	Databáze
DC	Data centrum, Datové Centrum
DDL	Data Definiton Language
DMZ	demilitarized zone - fyzická nebo logická podsíť, která je z bezpečnostních důvodů oddělena od ostatních zařízení v síti
Dodavatel	Česká pošta, s.p. odštěpný závod ICT služby

DWDM	Dense wavelength division multiplexing - Hustý vlnový multiplex - představuje v optických sítích technologii, kterou se při přenosu multiplexuje více optických signálů v jednom optickém vlákně s použitím rozdílných vlnových délek (barev) LED nebo laserů.
EoL	End of Life (Konec životnosti/podpory zařízení)
ESB	Enterprise Service Bus
ETL	Extract, Transfer, Load - přenášení a transformace dat z jedné báze do druhé
EU	Evropská unie
FHQ	Ohrožení základních životních funkcí
FP	Funkční prototyp, Prototyp
FT	Funkční testy
GB	gigabytes, gigabajtů = 1.000.000.000 bajtů
GD, GD ČP	Generální dodavatel ČP, s.p., Odštěpný závod ICT služby
GDB	Geodatabáze
GiB	gibibyte = 1024x1024x1024 bajtů = 1.073.741.824 bajtů
GIS	Geografický informační systém
GUI	Graphical User Interface
HA	Hlavní architekt
HTTP	Hypertext Transfer Protocol - webový protokol
HTTPS	Hypertext Transfer Protocol Secure - Zabezpečený webový protokol pomocí SSL
HW	Počítačový Hardware
Hybridní pracoviště	Koncové pracoviště (KP), které je určeno pro účely operačního řízení nebo pro příjem NSPTV
HZS, HZS ČR	Hasičský záchranný sbor ČR
ICT	Informační a telekomunikační technologie
IDM	Identity Management
IEC	International Electrotechnical Commission
IOP	Integrovaný operační program
IP	Internet protokol
IPL	Integrační platforma, softwarové řešení pro integraci externích systémů pro NIS IZS
IPT	IP Telefonie, hlasové služby provozované nad IP protokolem
IS	Informační systém
IS IZS	Jednotná úroveň informačních systémů operačního řízení a modernizace technologií pro příjem tísňového volání základních složek integrovaného záchranného systému
IS NIS IZS	Informační systém NIS IZS
IS OŘ	Informační systém operačního řízení
ISMS	Information Security Management System
ISO	International Organization for Standardization

ISO OSI	International Standards Organization / Open System Interconnection - referenční komunikační model rozdělující vzájemnou komunikaci mezi počítači do sedmi souvisejících vrstev.
ISP	Internet service provider
ISVS	Informační systémy veřejné správy
IT	Integrační testy
ITS MV	Integrovaná telekomunikační síť Ministerstva vnitra
ITS NGN	Integrovaná telekomunikační síť nové generace pro Policii České republiky, složky integrovaného záchranného systému a územní orgány státní správy. Též ve významu projekt „Zajištění infrastruktury pro operační střediska základních složek IZS".
IZS	Integrovaný záchranný systém
JSDI	Jednotný systém doprovázných informací
JTAPI	Java Telephony API
JTS	Jednotná telefonní síť
JVM	Java Virtual Machine, provozní prostředí všech Java programů
KDC	Krajské datové centrum – jedno v každém kraji (umístěno u HZS ČR), celkem 14 instancí
KGIS	Krajský GIS
KIVS	Komunikační infrastruktura veřejné správy
KP NSPTV	koncové pracoviště operátora NSPTV
KP OŘ	koncové pracoviště operátora OŘ
KP, koncové pracoviště	HW a SW pracoviště operátora, obsahuje hlavně miniPC, monitory, IP telefon, klávesnici, myš, aj.
KS	Komunikační systém
KSP	Krajský Standardizovaný Projekt, také někdy "noha"
KVM	Keyboard, Video, Mouse - Hardwarové zařízení, které umožňuje uživateli ovládat více počítačů z jedné klávesnice, monitoru, myši atd.
LAN	Local area network - lokální počítačová síť
LDAP	Lightweight Directory Access Protocol - Systém ověřování v síti
miniPC	osobní počítač (PC) malých rozměrů (CPU, RAM, nebíhučná diková jednotka), s pasivním chlazením (bez větráků), se 3 výstupy na monitor, určený pro koncové pracoviště
MPLS	Multiprotocol Label Switching
MST	Místopisný helper
MV, MV ČR, MVČR	Ministerstvo vnitra ČR
MV-GŘ HZS ČR	Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru České republiky
NBÚ	Národní bezpečnostní úřad
NIS IZS	Národní informační systém integrovaného záchranného systému
NSPTV	Národní systém příjmu tísňového volání
ODF	Optický propojovací panel
OoB	Out of Band
ORP	Obec s rozšířenou působností

OR	Operační řízení - proces nasazování sítí a prostředků (SaP) u HZS, PČR a ZZS
OS	Operační středisko - samostatné pro každou složku v každém kraji + GŘ HZS a FP PČR, operační středisko zahrnuje a) technologickou místnost pro umístění síťových technologií a b) vlastní operační síť, ve kterém budou provozovány komcové stanice NIS IZS, celkem 44 instancí
OSS	Organizační složka státu
OVM	Orgán veřejné moci
OZ ICT	Česká pošta, s.p. odštěpný závod ICT služby
PČR	Policie ČR
PČR/ITS	Objekt PČR s technologií ITS
PE	Provider Edge (MPLS PE)
PK, PTP	Prováděcí koncept SW řešení
PKv40	PK verze 40
PKv50	PK verze 50
PM	Projektový manažer
PoE, POE	Power over Ethernet, Napájení přes ethernetový kabel
POI	Point of Interest
PoP	Point-of-presence - přípojné místo přítomnosti páteřní sítě
PoP OPS P ČR	Hierarchická architektura přípojných míst páteřní sítě
PT	Projektový tým
PTV	Příjem Tísňového Volání
PVS	Portál veřejné správy
QoS	Quality of Service
RAIN	Redundant Array of Independent Nodes
REC	nahrávání hovorů
RK, RTP	Rámcový koncept SW řešení
RPO	recovery point objective, maximální doba, během které mohou být ztracena data některé IT služby z důvodu havárie
RTO	recovery time objective, doba trvání (vč. úrovně služby), během které musí být byznys proces obnoven po havárii
RTP	Real Time Protocol
RUIAN	Základní registr
SaP	Síla a Prostředky - Aktuální poloha nebo stav vysílání sil a prostředků
SBC	Session Border Controller
SDK	Software Development Kit, vývojové prostředí
SF EU	Strukturální fondy Evropské unie
SIP	Session initiation protocol
SLA	Service level agreement
SLA	Service Level Agreement (smlouva na poskytnutí služby s definovanými vlastnostmi)
SNMP	Simple Network Management Protocol
SOA	Servisně Orientovaná Architektura

SOAP	Simple Object Access Protocol je protokolem pro výměnu zpráv založených na XML, přes síť, hlavně pomocí HTTP
SRV	Server
ST	Systémové testy
STM1	Synchronous Transport Module level-1
STM4	Synchronous Transport Module level-4
SW	Software/Aplikační software
TB	terabytes, terabajtů = 1.000.000.000.000 bajtů
TCTV	Telefonické centrum tísňového volání
TDM	Time-division multiplexing
TiB	tibibyte = 1024x1024x1024x1024 bajtů = 1.099.511.627.776 bajtů
TKU	Tranzitní komunikační uzel
TV	Tísňové volání, příjem tísňových volání
VD	Vývojová dokumentace
VOIP	Voice over IP
VPN	Virtual private network
VRF	Virtual Routing and Forwarding - oddělení jednotlivých uživatelských sítí a nezávislé směrovací tabulky jsou udržovány pro každou síť odděleně.
WAN	Wide area network - rozlehlá počítačová síť
WDM	Wavelength-division multiplexing - vlnový multiplex
ZDTP	Změny detailů technického projektu
ZT	Záložové testy
ZZS	Zdravotnická záchranná služba krajů

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu

Národní informační systém integrovaného záchranného systému (NIS IZS)

Část

A. Dodávaný HW

Dokument obsahuje:	Seznam a specifikaci dodávaného HW a požadavky na jeho umístění (vyjma síťové infrastruktury a telefonie, které jsou specifikovány v částech C a J).
Verze:	5.1b
Schválil za Dodavatele:	Petr Rektorys
Datum:	2/5/2014
Registrační číslo projektu	CZ.1.06/3.4.00/11.07071

Česká pošta ICT služby

Obsah

1. Systémová architektura 4
1. 1.1 ..... Diskrétní systémových služeb 4
2. 1.2 ..... Virtualizace systémových prostředí 6
1.2.1 VIII infrastruktura 8
3. 1.3 ..... Archivace 9
1.3.1 Význam Archivace 9
1.3.2 Archivovaná data 9
1.3.3 Postup archivace 9
1.3.4 Přístupy archivovaných dat/ke 10
1.3.5 Struktura archivačního tvůrce 10
1.3.6 Parametry archivačního systému 11
1.3.7 Způsob ukládání archivu 12
1.3.8 Archivované data v manažeru Fileset 12
4. 1.4 ..... Zálohování 12
1.4.1 Význam zálohování 12
1.4.2 Parametry zálohovacího systému 13
1.4.3 Ukládání záloh 13
1.4.4 Zálohované data 14
1.4.5 Postup zálohování 15
1.4.6 Obnova záloh 15
2 Technická specifikace HW komponent 16
5. 2.1 ..... HW komponenty dodávané do CDC 16
2.1.1 CDC - blade server farma 17
2.1.2 CDC - diskové pole 19
2.1.3 CDC - archivační jednotka 20
6. 2.2 ..... HW komponenty dodávané do KDC 21
2.2.1 KDC - rack server 22
2.2.2 KDC - diskové pole 22
2.2.3 VIII infrastruktury pro IZS a PČR 24
7. 2.3 ..... Alokace výpočetního výkonu a diskových prostorů 24
2.3.1 Alokace pro CDC komponenty 24
2.3.2 Alokace pro KDC komponenty 25
8. 2.4 ..... Technologie do NSPTV 25
2.4.1 MonPC (součástí NSPTV) 25
2.4.2 Displej 26
2.4.3 Klávesnice 26
2.4.4 Myš 27

2.4.3 Tiskárna 27
2.4.6 RACR 27
2.4.7 Hlasový [illegible] 27
2.4.8 Zapojení pracovišť NSPTV 29
2.4.9 Vybavení pracovišť a grafická jednotlivých úloh 29
3 Umístění HW komponent 35
9. 3.1 ..... Metodika řízení dodávky 35
10. 3.2 ..... Koncepce pro jednoznačnou identifikaci lokalit 35
11. 3.3 ..... Koncepce pro jednoznačnou identifikaci komponent 35
12. 3.4 ..... Požadavky na technologické zajištění lokalit 36
3.4.1 CDC 36
3.4.2 KDC 37
3.4.3 NSPTV - Technologická místnost 39
3.4.4 NSPTV - Operační síť 39
Přílohy 40
13. Příloha č. 1 - Identifikace lokalit 40
14. Příloha č. 2 - Identifikace dodávaných komponent 43
15. Příloha č. 3 - Podrobný seznam dodávek 44
16. Seznam zkratek 57
17. Seznam obrázků 58
18. Seznam tabulek 58

1 Systémová architektura

Model architektury nastíněný v Rámcovém konceptu SW řešení, který předcházel tomuto Prováděcímu konceptu, doznal po konzultacích se zákazníkem úprav a zpřesnění. V rámci paralelního vývoje prototypu aplikace NSPTV nebylo prokázáno požadované chování tenkého klienta (virtuálního desktopu), respektive technologie pro přenos obrazu, která umožňuje přenos virtuálního desktopu z centrálního datového centra na pracoviště operátora. Během procesu průběžného schvalování technického řešení (resp. změn detailů technického řešení, jak je popsáno ve vývojích k jednání) rozhodl zákazník o využití miniPC s instalovanou aplikací NSPTV namísto konceptu virtuálního desktopu. S tímto rozhodnutím jsou spojeny zejména následující logické dopady na systémovou architekturu:

1) realizovat replikaci dvou centrálních DC na úrovni diskových polí není nákladově ani technicky efektivní, tato technologie byla uvažována zejména k vytvoření transparentního prostředí pro virtuální desktopy,
2) geografické služby pro potřeby lokálně běžících operátorských aplikací je možné čerpat z příslušné lokality krajského datového centra, výhody takového postupu pramení zejména v nižší latenci (poddlouhé umístění na KDC jsou od operátorů zpravidla geograficky blíže než na CDC) a nižší zátěže sítě ITS, datové objemné dlaždice z GIS budou významně zatěžovat infrastrukturu krajských trojúhelníků, ale nikoli páteřní síť,
3) vzhledem k odchýlení od uvažované replikace dvou CDC na úrovni diskových polí, neexistují již tak zásadní omezení pro volbu lokalit těchto CDC (geografická vzdálenost do 30 km), z rozhodnutí zákazníka byla pro jedno z těchto CDC namísto lokality Praha, Sazečská, zvolena lokalita Plzeň, Kapitánova 2726/9.

V prováděcím konceptu SW řešení jsou tedy všechny centrální lokality považovány za rovnocenné z hlediska provozovaných služeb a mohou být tedy v prostředním prostředí provozovány paralelně vedle sebe, přičemž synchronizace těchto tří logických instancí bude řešena pro každou SW komponentu zvlášť dále popsanými mechanismy a následně také v částech B – SW a I - telefonie.

1.1 Dislokace systémových služeb

Na základě provedených konzultací se zákazníkem byla provedena identifikace 3 kategorií služeb z pohledu potřeby jejich centralizace, resp. distribuce v datových centrech NIS IZS:

- centralizované – služby poskytované výhradně na úrovni tří CDC (tyto služby na KDC nefungují bez dostupného CDC),
- hybridní – služby poskytované na úrovni CDC a zároveň na všech KDC (služby mohou být v KDC lokalitách poskytovány nezávisle na tom, jestli je dostupné CDC a naopak),
- distribuované - služby poskytované výhradně z úrovně KDC (tyto služby na CDC nefungují bez dostupného KDC, resp. více KDC).

K připojení externích systémů (BIS/LAN, ISIM) a přístupu ke službám vystaveným ve veřejném internetu bude využito služeb CMS 2.0 (resp. služeb CMS než dojde k dodávce projektu CMS 2.0). Analogicky budou služby poskytované projektem NIS IZS pro externí systémy (zejména záchrnní koordinátora dle IPL) vystaveny také v CMS, resp. CMS 2.0.

1.2 Virtualizace systémových prostředí

HW vrstva fyzických serverů, jak rackových (využívaných na KDC), tak blade serverů (využívaných na CDC), bude překrytá virtualizační vrstvou (tzv. Hypervizorem), která dokáže efektivně využít výkon systémových prostředků a zvýšit dostupnost a odolnost proti výpadku jednotlivých částí HW vrstvy. Hypervizor umožňuje alokovat části výkonu (zejména CPU, RAM, LAN, VGA) fyzických serverů do virtuálních strojů (tzv. VM – virtual machine).

Každé diskové pole bude podporovat virtualizační vrstvu a bude napojeno do správce virtualizační vrstvy, která alokuje jednotlivé části diskového prostoru pomocí technologie iSCSI (Target-LUN) pro virtuální stroje (VM).

Pro síť se virtualizační vrstva tváří jako sada virtuálních switchů, které propojují fyzické porty serverů s VM. Virtuální switche umožňují nastavení rychlosti linky, agregace linek, QoS, VLAN, VPN nebo představit virtualizovaný firewall. To umožňuje vytvořit samostatnou nebo virtuálně oddělenou síť v rámci existující sítě, resp. mimo komunikační síťovou infrastrukturu. Toho lze efektivně využít pro oddělené testování a vývoj, školení a vlastní produkční prostředí tak, aby se tato prostředí vzájemně neovlivňovala.

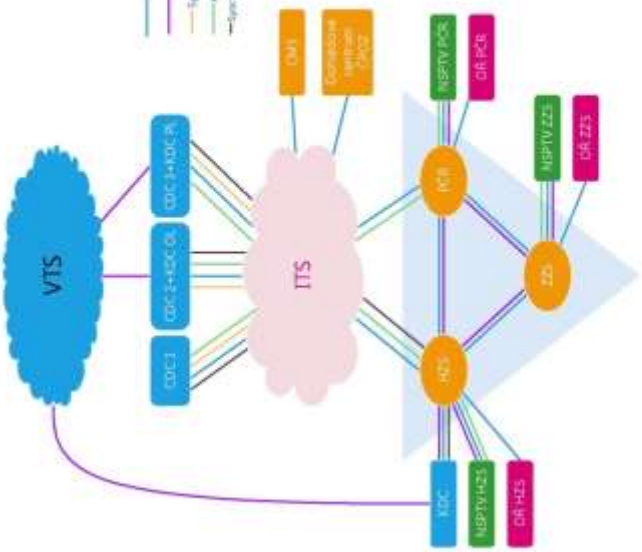
VM je ve své podstatě plnohodnotný počítač/server, který má přidělené prostředky z fyzické vrstvy a tváří se v síťovém prostředí jako fyzický server a tudíž dokáže poskytovat stejné přesvědčivé služby. Hypervizor umožňuje dynamicky alokovat prostředky z fyzické vrstvy bez nutnosti odstavení nebo změny systémové vrstvy instalované ve VM.

Hypervizor umožňuje vytvářet obrazy VM (Snapshot VM), které se používají pět změnách nastavení v instalovaném systému VM a v případě chyby je možné se v krátkém čase vrátit k vytvořenému obrazu a tudíž k návratu do funkčního stavu. Tuto technologii zde použít i k zálohování výchozích stavů. Dále umožňuje vytváření kopií VM (Clone VM), které umožňuje vývojářům pracovat v reálnému kopií produkčního prostředí tak, že pobězí paralelně vedle produkčního prostředí, ale není možné ovlivňovat provoz na původním VM ze strany kopie nebo naopak. Tuto technologii lze využít i k vytváření šablon systémových komponent aplikační vrstvy pro testování, vývoj a školení.

Všechny Hypervizory ze všech serverů jsou napojeny na Centrální správu, která dokáže spravovat, monitorovat a automaticky řešit krizové scénáře v případě pádu jednotlivých částí systému. Celá virtualizace bude spravována z této centrální komponenty. Tato komponenta umožňuje v reálném čase migrovat jednotlivé či celé skupiny VM mezi fyzickými servery v rámci CDC nebo KDC. Dále umožňuje prioritizovat výkon VM v celém prostředí. Toho lze efektivně využít v případě havárii HW části systému, kdy je automaticky utlumen výkon nepotřebné části systému na úkor kritických systémů.

Obrázek 1 - Úroveň centralizace/distribuce služeb

Z výše uvedeného schématu je zřejmé, které služby mohou být dostupné i při případném výpadku ITS na úrovni KDC. Hybridní služby GIS a SW pro nahrávky budou primárně poskytovány z KDC, pouze při nedostupnosti příslušného KDC budou poskytovány z úrovně CDC. Hybridní služba IPL bude naopak primárně poskytována z úrovně CDC, pouze při nedostupnosti centrální úrovně bude poskytována záložně z KDC.

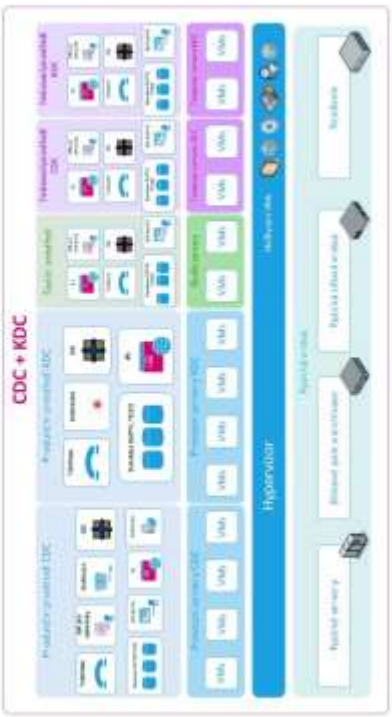


Obrázek 2 - Poskytovatelé a příjemci služeb z pohledu centrálních a krajských lokalit složek IZS

Na následujících schématech je vyobrazeno, jak budou uspořádány jednotlivé systémové vrstvy z hlediska virtualizace v CDC a KDC. Pro všechny centrální lokality bude dodáván výkonný HW v podobě blade serverové farmy a diskového pole, přičemž v lokalitách CDC2 a CDC3 bude navýšen výkon serverové farmy kvůli potřebě souběžného provozu místně příslušných KDC. Vzhledem k tomu, že HW umístěný do lokalit CDC je dimenzován tak, aby dokázal samostatně obsloužit veškerý provoz NIS IZS, bude při souběžném provozu DL ale i dvou lokalit CDC k dispozici dostatečný výkon pro školící a testovací prostředí. Pouze v případě, že by došlo k nedostupnosti dvou lokalit CDC, došlo by k automatické realokaci prostředků pouze na produkční prostředí skrz mechanismy popsanými v části G – Spolehlivost. V takové situaci by byl automatizovaně zcela potlačen provoz testovacího a školicího prostředí.

Obrázek 3 - Rozdělení systémových prostředí provozovaných v lokalitě CDC1

Systémová prostředí budou oddělena nejen v úrovni virtuálních strojů, ale zejména z pohledu síťových rozsahů fyzické a virtuální LAN sítě. Tímto nastavením bude zajištěno, že tato prostředí se z technologické podstaty nemohou ovlivňovat. Aby při testování příjmu tísňových volání nemohlo dochazet k ovlivňování produkce, budou do lokality CDC1 dodány 2 ks fyzických hlasových bran určených pouze pro testování. Ve srovnání s běžnými hlasovými branami dodávanými na KDC se však bude jednat o mírně upravený HW.



Obrázek 4 - Rozdělení systémových prostředí provozovaných v lokalitách CDC2 a CDC3

Testovací prostředí KDC nebude provozováno na fyzické infrastruktuře KDC, ale v prostředí CDC. Takové zapojení vytvoří z technického pohledu srovnatelný obraz produkce a tedy provedené takovým způsobem budou věrohodné i vzhledem k produkci. Chování produkční sítě ITS mezi CDC a KDC bude emulováno SW nástrojem.

Obrázek 5 - Rozdělení systémových prostředí provozovaných v lokalitách KDC

1.2.1 VDI infrastruktura

V tomto případě se jedná o dodávku serverové infrastruktury, na které bude instalován operační systém, který umožní spouštění virtuálních pracovních stanic přímo na této infrastruktuře. Na virtuální pracovní stanici budou operátoři NIS IZS přistupovat pomocí „lenkého" klientského PC (tzv. thin PC) nebo klasického PC (architektury x86 popř. x 64b). Tato PC umožní ovládání periferií virtuálních pracovních stanic běžících na serverové infrastruktuře prostřednictvím fyzických periferií připojených k těmto PC.

1.3 Archivace

1.3.1 Význam Archivace

Představuje především dlouhodobé shromažďování informací pro případné pozdější použití například v soudním řízení. Součástí archivačního řešení bude i nasazení technologií pro rychlé vyhledávání a třídění výsledků archivace. Pro práci s archivem bude nejdůležitější jeho nepřerušení, dlouhodobá spolehlivost a vysoká životnost.

1.3.2 Archivovaná data

1. Nahrávky telefonních hovorů ve formátu mp3
2. Databáze událostí
3. Zprávy IPL

Při kalkulaci předpokládaných archivovaných dat bylo vycházeno z následujících podkladů:

Datový tok jednoho hovoru za vteřinu [WAV] [kb/s]	172
Datový tok jednoho hovoru za vteřinu [MP3] [kb/s]	32
Přijatá volání [počet/den] (Koncept TO-RE, str. 31, tabulka 7)	22100
Střední hodnota hovoru [min] (Koncept TO-RE, str. 137)	4
Počet uživatelů [uživatelé/den]	3500
Velikost události [KB]	200

Tabulka 1 - Předpoklady dlouhodobě ukládaných dat

Na základě analýz historických dat byly odhadnuty následující objemy ukládaných dat, zvýrazněny jsou údaje, které byly použity pro návrh diskového pole a archivační jednotky. Odhad ukládaných dat v archivační jednotce po dobu udržitelnosti projektu je 4,5 TB, s přibližně 20% rezervou je tedy tato jednotka navrhována s kapacitou 50 TB.

Ukládaná data	**Den [GB]**	**3 měsíce [TB]**	**1 rok [TB]**	**5 let [TB]**
Aktivně ukládané záznamy (WAV)	110,76	9,96	36,76	184,11
Archivované záznamy (MP3)	20,23	1,82	7,21	36,10
Archivované data IIS + zprávy IPL	2,87	0,23	0,92	4,59

Tabulka 2 - Předlohce uchovávaných dat na centrálním diskovém poli a v archivu

1.3.3 Postup archivace

- Nahrávky telefonních hovorů ve formátu mp3
  1. Ve chvíli vytvoření nahrávky je nahrávka ihned ošetřena pomocí hashe a digitálního razítka (popřípadě časového razítka) nahrávacím systémem
  2. Po ošetření nahrávky je nahrávka přesunuta z KDC do archivu CDC pro dlouhodobé zarchivování
- Databáze událostí
  1. Ve chvíli vytvoření transakčního logu je log okamžitě předán archivačnímu SW, který ho automaticky označí pomocí hashe a digitálního razítka (popřípadě časového razítka)
  2. Po ošetření transakčního logu je log automaticky přesunut do archivačního úložiště
- Zprávy IPL
  1. Ve chvíli přijetí zprávy na IPL nebo jejího odeslání je zpráva ve shodné podobě ihned předána archivačnímu SW, který ji automaticky označí pomocí hashe a digitálního razítka (popřípadě časového razítka)
  2. Po ošetření je tato zpráva automaticky přesunuta do archivačního úložiště

1.3.4 Přístup k archivovaným datům

- Pomocí NFS
- Pomocí webového rozhraní archivačního SW
- Prostřednictvím API nahrávacího systému v případě nahrávek
- Pomocí správy oprávnění bude možné oddělit přístup k jednotlivým částem archivu (např. k datům a nahrávkám jednotlivých složek)

1.3.5 Struktura archivačního řešení

- Archivační řešení bude složeno z HW části tvořené z modulárních serverů (zařízení s RAIN architekturou) a SW archivačního nástroje, který bude zajišťovat přístup k HW vrstvě.
- SW nástroj pro archivaci nahrávek bude popsáván v rámci výběrového řízení na subsystém telefonie a nahrávání. Cílem je sjednocení přístupu k nahrávkám bez ohledu na to, zda jsou v archivu nebo na diskovém poli a také plná kompatibilita s nahrávacím zařízením, čímž je zaručeno, že s nahrávkou nebylo manipulováno.
- Pro archivaci ostatních, pro důkazní řízení významných, dat (transakční logy a zprávy z IPL) bude soutěžen vlastní SW nástroj, který bude zajišťovat jejich archivaci.
- Synchronizace archivovaných dat mezi třemi lokalitami CDC bude řešena příslušným SW nástrojem, resp. nahrávacím systémem, který bude zajišťovat uložení shodných dat ve všech třech lokalitách.

13. Skartace dat zaručuje jejich neobnovitelnost, tzn. minimálně 7 přepisů mazaných dat
14. Nativní auditované smazání obsahu s důkazem o smazání (důvod smazání, kdo a kdy obsah smazal apod.) a to i včetně neautorizovaného smazání
15. Konfigurace výchozí skartační periody
16. Rozšíření o nastavení funkcionality pro ad-hoc vymazení „nevymazatelnosti" obsahu tzv. „Retention hold" a to i na jednotlivé soubory, celý archiv anebo jen část archivu
17. Automatické i ruční migrace archivovaných dat mezi různými druhy úložišť nebo lokalit (například do jiného datacentra)
18. Archivovaná data se určují:
    a. pomocí cesty k datům v síti nebo disku
    b. pomocí přípony souboru na úložišti
    c. zasláním pomocí https protokolu
19. Předarchivační příprava se skládá:
    a. vytvoření hash, ořezání časovým razítkem, opatření metadaty
    b. data musí být na tolik ošetřená tak, aby byla zaručená jejich jedinečnost
    c. předarchivační příprava může spolupracovat s telefonní ústřednou tak, aby byly uloženy veškeré požadavky na archivaci při archivaci telefonních hovorů z ústředny
20. Vyhledávání v archivovaných datech – grafické webové rozhraní pro vyhledávání (např. datum, událost, kde vznikla, či připojených informací apod.)

1.3.7 Fyzické uložení archivu

- Archiv bude uložen na úložném zařízení s RAIN architekturou, které bude dodáváno do každého CDC, detailní specifikace je uvedena v části Specifikace HW komponent.
- V každém CDC bude identická kopie archivu, synchronní stav všech archivů bude zajištěn nástrojem archivačního SW, resp. nahrávacím systémem v případě nahrávek.

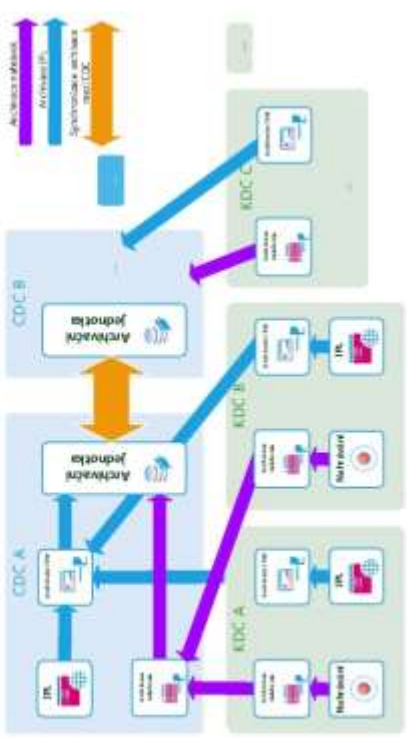
1.3.8 Archivovaná data v soudním řízení

Veškerá archivovaná data jsou plně přípustná v soudních řízeních, jelikož je zaručena jejich jedinečnost a pravost. Záruka jedinečnosti a pravosti dat je zaručena kombinací několika bezpečnostních prvků. A to tak, že archivovaná data jsou po celou dobu životnosti od okamžiku jejich vzniku ošetřena pomocí digitálního otisku, časového razítka nebo digitálního podpisu. A to tak, aby bylo možné kdykoliv důvěryhodně ověřit a zaručit jejich autenticitu.

1.4 Zálohování

1.4.1 Význam zálohování

Vytváření bezpečnostní kopie dat nebo celého operačního systému tak, aby bylo možné v případě havárie (a to jak SW, tak HW) velice rychle obnovit poškozená data nebo celý systém do stavu, který existoval těsně před vznikem poruchy a to i na nový HW nebo i do jiné lokality.



Obrázek 6 - Schéma archivačních procesů

1.3.6 Parametry archivačního systému

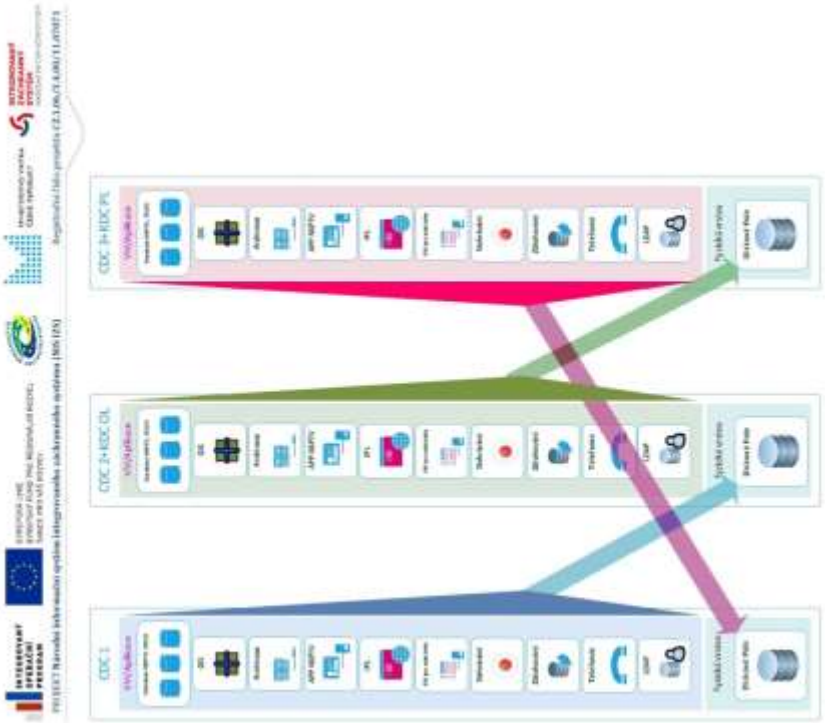
1. Archivace umožňuje uložení dat v plné shodě s odpovídajícími paragrafy následujících zákonů: zákon č. 499/2004 Sb., který je upraven zákonem č. 167/2012 Sb.
2. Archivační systém umožňuje nastavení minimální a maximální doby uložení dat zejména kvůli definici skartační doby a doby retence dat.
3. Garance nemožnosti uložených dat z důvodu autenticity takových dat při případném důkazním řízení
4. Garance jedinečnosti uložených dat z důvodu autenticity takových dat při případném důkazním řízení
5. Garance dlouhodobého uchování – nastavení politiky pro uchování dat (různé doby skartace až po neurčenou dobu uchování dat)
6. Garantovaná nemazatelnost uložených dat – možnost nastavení selektivně pro každý objekt příznak nemazatelnosti na definovanou libovolně dlouhou dobu (i neúsečně)
7. Vysoká bezpečnost (neexistuje nikdy natolik privilegovaný administrátor, který by mohl získat přístup k obsahu objektů, případně objekty mazat nebo manipulovat s podpisy a obsahem). To znamená například oddělené administrátorské role (např. systémový administrátor a aplikační administrátor nemůžou mít ta samá oprávnění)
8. Možnost asynchronní replikace celého zařízení nebo pouze vybraných částí zařízení do vzdálené lokality
9. Přístup k datům pomocí NFS, HTTPS
10. Archivace umožní vynucení skartační doby pro ukládaná data
11. Archivace umožní definici skartačních tříd podle druhu ukládaného obsahu
12. Archivace umožní elektronickou skartaci

1.4.2 Parametry zálohovacího systému

1. Podporované zálohování bvdli možnému vysoutěžení SW produktů, které budou dodávány spolu s vlastním systémem:
   a. MS Windows 2012 a novější (a to i souborové zálohování),
   b. Linux kernel 2.6 a novější - zejména Red Hat, SUSE (a to i souborové zálohování),
   c. Oracle DB,
   d. MS SQL server,
   e. IBM DB2,
   f. PostgreSQL,
   g. Virtuální stroje (běžící na platformách VMware 5.x, Citrixen Server 6.x a Microsoft Hyper-V 3.x),
   h. Vytváření kloně běžících serverů.
2. Veškerá zálohovaná data lze obnovovat po jednotlivých částech (tzv. item level recovery) souhory, data v DB
3. Obnovu dat lze provádět i do jiné destinace (důležité) než bylo původní
4. Podpora deduplikace na cíli
5. Podpora deduplikace a kompresu na zdroji
6. Automatické i ruční kopírování záloh mezi různými druhy úložišť (z nového úložiště lze i obnovovat data) nebo lokalit (například do jiného datacentra)
7. Automatická i ruční migrace záloh mezi různými druhy úložišť (z nového úložiště lze i obnovovat data) nebo lokalit (například do jiného datacentra)
8. Plné zálohování dat tzv. „full backup"
9. Inkrementální zálohování dat
10. Vytváření snapshotů serverů

1.4.3 Uložení záloh

1. Snapshoty budou uloženy vždy v lokalitě, kde budou vytvářeny z důvodu vysoké dostupnosti a menšího zatížení sítě
2. Zálohovaná data se budou vždy ukládat do jiné geografické lokality z důvodu bezpečnosti dat – nevztahuje se na snapshoty
3. Data z CDC1 do CDC2
4. Data z CDC2 do CDC3
5. Data z CDC3 do CDC1
6. Data budou uložena vždy na provozních diskových polích z důvodů vysoké dostupnosti a rychlosti obnovy
7. Data budou uložena na pomalé diskové vrstvě (tier) z důvodu ceny uložených dat



Obrázek 7 - Princip zálohování mezi centrálními lokalitami

1.4.4 Zálohovaná data

1. Databáze NSPTV
2. Databáze telefonie
3. Databáze archivace nahrávek
4. Databáze archivace událostí
5. GIS
6. SW archivace

7. SW NSPTV
8. SW IPL
9. SW nahrávání
10. SW telefonie
11. SW zálohování
12. LDAP
13. Veškeré virtuální stroje, nad nimiž poběží aplikace a databáze

1.4.5 Postup zálohování

1. Plné zálohy tzv. „full backup" se budou provádět každou neděli
2. Incrementální zálohy se budou provádět každý den od pondělí do neděle
3. Snapshoty na úrovni virtualizační vrstvy se budou provádět v případě updatu, změn konfigurací, instalací nových funkcionalit, aktualizací a nasazování nových systémů
4. Zálohy se budou držet 14 dní pro případ obnovy, poté se budou automaticky odmazávat
5. V každém CDC bude nainstalován zálohovací server, se zálohovacím SW pro správu a řízení zálohovacího řešení
6. Na každém serveru, který se bude zálohovat (viz. 1.4 Zálohovaná data) bude nainstalován zálohovací agent, který bude napojen na zálohovací server v CDC
7. Zálohovací agent podle nastavení zálohování na zálohovacím serveru provádí autonomně zálohování

1.4.6 Obnova záloh

- Celý systém NIS IZS funguje, ale je potřeba obnovit jen kmenové dílčí data
  a. Konkrétní data budou obnovena do původního umístění do předchozího datového stavu.
  b. Konkrétní data budou obnovena do jiného umístění/destinace pro další zpracování a analýzu datového stavu.
- Část systému NIS IZS nefunguje, je potřeba obnovit databázi, server nebo aplikaci
  a. Celá databáze, server nebo aplikace bude obnovena do původního umístění/destinace pro obnovení předchozího provozního stavu.
  b. Celá databáze, server nebo aplikace bude obnovena do jiného umístění/destinace pro obnovení předchozího provozního stavu, v případě, že nelze z provozních/havarijních důvodů obnovit do původního umístění/destinace.
- Celý systém NIS IZS včetně zálohovacího řešení nefunguje, je potřeba kompletní obnova celého řešení
  a. Nejdříve bude nainstalován nový zálohovací server, pomocí kterého bude obnovena původní konfigurace zálohovacího systému.
  b. Pomocí obnoveného zálohovacího serveru dojde k obnovení provozního stavu prostředí CDC.
  c. Po obnovení a zprovoznění CDC budou postupně obnovována a zprovozňována zbylá CDC jedno po druhém.

2 Technická specifikace HW komponent

Dodavatel jako řešitel zadavatel dosgělt k závěru, že při dodržení všech ustanovení smlouvy o dílo na dodávku pro projekt Národní informační systém integrovaného záchranného systému bude zajišťovat veškeré dodávky formou otevřených výběrových řízení. Jelikož tato výběrová řízení nejsou v době zpracování PK SW řešení dosud ukončena, je PK SW řešení dodáván jako produktové nezávislý se zohledněním technických specifikací (by jsou podkladem pro zadání příslušných výběrových řízení). Po ukončení výběrových řízení bude PK SW řešení aktualizován a předán zadavateli jako produktové závislý.

Z tohoto důvodu jsou ve specifikacích HW komponent uvedeny výhradně závazné parametry pro jednotlivá zařízení, která ději jejich podstatné vlastnosti. Tyto parametry budou plně zohledněny v zadávacích dokumentacích příslušných výběrových řízení na dodávky těchto komponent.

2.1 HW komponenty dodávané do CDC

Tato část provádícího konceptu SW řešení je podrobně věnována HW komponentám s výjimkou síťové infrastruktury a telefonie, tyto jsou podrobně specifikovány v částech C a E. Následující schéma ilustruje rozsah dodávky, jejíž specifikace je uvedena v rámci této části.

Obrázek 8 -Rozsah HW technologií dodávaných do CDC, resp. CDC + KDC, podrobně specifikovaných v části A - HW

2.1.1 CDC - blade server farma

2.1.1.1 Blade management

1. SW pro centrální správu, monitoring a reporting na úrovni Blade server systému, Blade server farmy a Blade server chassis. Tento SW spravuje celý blade server systém z jednoho centrálního místa
2. Podpora minimálně SNMP v 2
3. SW pro správu, monitoring a reporting umožní přístup ke správovskému rozhraní prostřednictvím WWW prohlížeče s podporou SSL a zároveň textového terminálového rozhraní CLI s podporou SSH
4. SW pro správu, monitoring a reporting musí umožnit řízení přístupových práv k řídicím modulům, KVM přepínačům a dalšímu částem správy systému prostřednictvím účtů v LDAP
5. Virtuální KVM podporuje textovou i grafickou konzoli serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače, včetně možnosti sdílení obrazu více uživateli současně a možnosti mapování vzdálených médií
6. SW pro správu, monitoring a reporting umožňuje členění přístupových uživatelských práv na základě členství v lokálních nebo LDAP skupinách
7. SW pro správu, monitoring a reporting poskytuje jednotné grafické rozhraní pro správu všech instalovaných komponent (farmy, chassis, blade server modulů, zdroje apod.) nevztahuje se na modulární konektivitu v chassis

2.1.1.2 Blade chassi

1. Plně osazené chassis redundantními zdroji
2. Plně osazené chassis redundantními ventilátory
3. Hot-plug ventilátory a zdroje
4. Podpora technologie hot plug Blade server
5. Minimálně 10 Gc Pass Thrum modul, který má porty v minimálně stejném počtu jako je počet možných instalovaných blade serverů dělitelných v poměr 1:4 a to celé redundantně nebo je povolena agregace v maximálním poměru 4:1
6. Řešení umožňuje nezávislý přístup pro OOB management po ethernetu. A to minimálně 100Mbps port, který bude redundantně

2.1.1.3 Blade server

1. Každý Blade server bude obsahovat ethernetové rozhraní minimálně 2x10Gb/s s podporou ISCSI
2. Podpora virtualizačních rozhraní, minimálně 4 virtuálních rozhraní ETH na interface
3. Plná podpora virtualizačních technologií a jejich fungování minimálně VMware 5.x, Citrix 6.x, Hyper-V 3.x
4. Blade server umožňuje bootování z různých zdrojů (Virtual CDROM/PXE/iSCSI/Flash paměť/USB CDROM/SAN/LAN)
5. Instalovaná minimálně jedna flash paměť 2GB (SD, USB flash disk a jiné) pro boot virtualizace
6. Podpora minimálně SNMP v 2
7. Podpora technologie hot plug Blade server
8. Blade server modul obsahuje minimálně 16 jader, x86, 64bit a zároveň s minimálním výkonem CPU podle benchmarku http://www.cpubenchmark.net/cpu_list.php 10000 bodů, a nebo CINT 2006 Rate minimálně 500
9. Blade server modul obsahuje minimálně DIMM sloty (2GB/4GB/8GB/16GB/32GB) DDR3 minimálně 1333MHz s podporou ECC
10. Blade server modul obsahuje minimálně 96 GB instalované paměti RAM s parametry DDR3, 1333MHz, podpora ECC

2.1.1.4 Výkonová varianta pro samostatné CDC

Počet serverových farem v jedné lokalitě	1
Počet lokalit celkem (1xCDC)	1

Pro lokalitu CDC1 bude dodavcha obsahovat následující počet blade serverů a příslušná chassi, jejich počet bude upřesněn na základě výsledků veřejné zakázky:

CDC - blade server farma	Počet
Blade server CDC	8

2.1.1.5 Výkonová varianta pro souběžně běžící CDC + KDC

Počet ks v jedné lokalitě: 1

Počet lokalit celkem (2xCDC+KDC): 2

Pro lokality CDC2 a CDC3 bude dodávka obsahovat následující počet blade serverů a příslušná chassi, jejich počet bude upřesněn na základě výsledků veřejné zakázky:

CDC+KDC - blade server farma	Počet
Blade server CDC	12

2.1.2 CDC - diskové pole

Počet ks v jedné lokalitě: 1

Počet lokalit celkem (1xCDC, 2xCDC+KDC): 3

2.1.2.1 Závazné parametry

1. Minimální požadovaná čistá, použitelná, formátovaná kapacita diskového pole je 25 TiB
2. Řešení poskytuje minimálně 2x 10Gbit/s ethernet port na řadič pro připojení serverové farmy
3. Minimální velikost cache 8 GB
4. Minimální rozložení kapacity diskového pole je:
   1) SSD - 5TiB (RAID 5)
   2) SAS 600GB - 10TiB (RAID 5)
   3) NL_SAS 3TB - 10TiB (RAID 6)
5. Diskové pole současně podporuje následující využitelné typy HW RAID bez omezení:
   1) RAID-1 a RAID-1/0
   2) RAID-5
   3) RAID-6
2. Diskové pole podporuje následující typy technologie hot spare (hot standby) a hot plug:
   1) globální a dynamický hotspare HDD – bez vazby na konkrétní pool (možnost aktivace pro libovolný disk v poli)
   2) proaktivní hotspare HDD - aktivace hotspare při detekci zhoršení parametrů disku ještě před samotným výpadkem
   3) hot plug ventilátory
   4) hot plug redundantní zdroje
6. Diskového pole bude možno rozšířit minimálně na 1,5 násobek kapacity
7. Diskové pole umožňuje současně následující typy alokace kapacit:
   1) provisioning s dopředným naformátováním všech bloků logického disku
   2) tenký provisioning bez dopředného formátování - tj. kapacita logického disku je alokována podle potřeby,

   3) možnost vyhrazení menší skupiny disků pro účely definice izolovaného logického disku s vlastní ochranou RAID
8. Architektura diskového pole splňuje minimálně následující parametry:
   1) redundantní řadiče (kontroléry)
   2) žádný Single Point Of Failure
   3) zajištění cache paměti proti neočekávanému výpadku napájení automatickým přepisem jejího obsahu na média nevyžadující napájení pro uložení dat
9. Diskové pole je vybaveno funkcionalitu pro CIFS a NFS datové sdílení po 10Gbit/s interface
10. Souborové služby diskového pole poskytují minimálně tyto funkce (všechny současně):
    1) schopnost integrace do systému Active Directory
    2) schopnost definice více CIFS serverů a „share" nad stejným datovým prostorem (diskovým svazkem)
    3) schopnost současného sdílení stejných dat protokolem CIFS i NFS
    4) deduplikace alespoň na úrovni single instancing
    5) možnost vyvažování zátěže dynamickým přesunem objektů
11. Řešení plně podporuje minimálně následující technologie pro virtualizaci: VMware 5.x, CitrixXen Server 6.x a Microsoft Hyper-V 3.x
12. Řešení zahrnuje nástroj pro detailní analýzu výkonnostních parametrů, v reálném čase i historicky
13. Navržená technologie podporuje heterogenní infrastrukturu pro vlastní uložení dat - běžná disková pole v SAN infrastruktuře, a to i různých výrobců současně
14. Zařízení dovoluje a plně podporuje zcela transparentní migrace dat i aplikací v rámci pole na běžící aplikace
15. Řešení poskytuje SNMP rozhraní minimálně ve verzi 2 pro monitorování centrálním dohledovým systémem
16. Řešení podporuje integraci na úrovni operací failover i failback pro virtualizační vrstvu
17. Součástí řešení je jednotný SW management systém – jediná konzole. Z tohoto jediného SW je možné spravovat všechna disková pole v CDC
18. Řešení umožňuje nezávislý přístup pro OOB management po ethernetu

2.1.3 CDC - archivační jednotka

Počet ks v jedné lokalitě: 1

Počet lokalit celkem (1xCDC, 2xCDC+KDC): 3

2.1.3.1 Závazné parametry

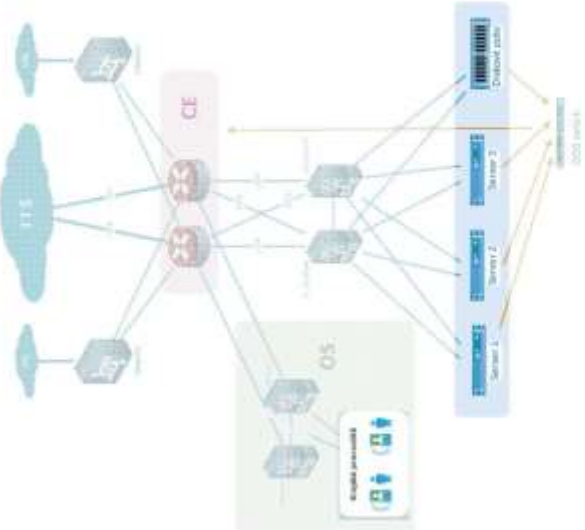
1. Minimální požadovaná čistá, použitelná, formátovaná kapacita Archivační jednotky je 50 TiB
2. Minimální rozšiřitelnost 200 TiB
3. Systém je založen na tzv. RAIN architektuře. Tedy na nezávislých modulech, které jsou schopny v případě výpadku některého z nich převzít jeho roli bez přerušení dostupnosti systému
4. Úložné zařízení má zabudován vysoký stupeň ochrany dat buď formou zrcadlení, nebo paritních kopií tak, aby např. havárie disku nebo modulů (nodu) nevedla ke ztrátě dat

Podpis/signature:.....

5. Úložné zařízení má zabudován samo zotavovací mechanismus, který je při selhání schopen bez zásahu administrátora některé z komponent obnovit nebo zpřístupnit dotčená data bez přerušení dostupnosti systému
6. Podpora SAN
7. Řešení poskytuje minimálně 2x 1Gbit/s ethernet port na modul připojení serverové farmy
8. Řešení poskytuje SNMP rozhraní minimálně ve verzi 2 pro monitorování centrálním dohledovým systémem
9. Součástí řešení je jednotný SW management systém – jediná konzole. Z tohoto jediného SW je možné spravovat všechny archivační jednotky v CDC
10. Řešení umožňuje nezávislý přístup pro OOB management po ethernetu

2.2 HW komponenty dodávané do KDC

Následující schéma ilustruje rozsah dodávky do KDC, jejíž specifikace je uvedena v rámci této části Prováděcího konceptu. Komponentám síťové infrastruktury a telefonie se podrobně věnují části C a J.



Obrázek 9 - Rozsah HW technologií dodávaných do jednotlivých KDC, podrobně specifikovaných v části A – HW

2.2.1 KDC – rack server

Počet ks v jedné lokalitě: 3

Počet lokalit celkem (12xKDC bez funkce CDC): 12

2.2.1.1 Závazné parametry

1. Redundantní napájecí zdroje
2. Redundantní ventilátory
3. Hot-plug ventilátory a zdroje
4. Server umožňuje bootování z různých zdrojů HDD/CD/DOM/Flash paměť/USB CD/DOM/LAN
5. Minimálně 100/1Gbps pro OBIB management
6. Diskový kontrolér s ochranou proti výpadku napětí
7. SW pro centrální správu, monitoring a reporting podporuje kompletní správu ve všech správcovských prostředích prostřednictvím WWW prohlížeče s podporou SSL a zároveň textového terminálového rozhraní CLI s podporou SSH
8. SW pro správu, monitoring a reporting umožňuje řízení přístupových práv k řídicím modulům, KVM přepínačům a dalším částem správy systému prostřednictvím účtů v LDAP
9. SW pro správu, monitoring a reporting umožňuje vzdálenou textovou i grafickou konzoli serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače), včetně možnosti sdílení více uživateli současně, možnost mapování vzdálených medií, souborů či adresářů
10. Virtuální KVM podporuje textovou i grafickou konzoli serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače), včetně možnosti sdílení více uživateli současně, možnost mapování vzdálených medií, souborů či adresářů
11. Podpora minimálně SNMP v 2
12. Blade server modul obsahuje minimálně 32 jader, x86, 64bit, a zároveň s minimálním výkonem CPU podle benchmarku http://www.cpubenchmark.net/cpu_list.php 10000 bodů a nebo CINT 2006 Rate minimálně 500
13. DOMM DDR3 minimálně 1333MHz, ECC
14. Minimálně 160 GB RAM 1333MHz
15. Server umožňuje bootování a zavedení systému po iSCSI
16. Instalovaná minimálně jedna flash paměť 2GB (například SD, USB flash disk a jiné) pro boot virtualizace
17. Minimálně 4x 1Gbps LAN
18. 2x 10Gbit/s iSCSI ethernet
19. Podporované OS: MS Windows 2012 a novější, Linux kernel 2.6 a novější, VMware ESX a ESXi 4.x a 5.x, Citrix, MS Hyper-V, Citrix Xen server
20. Provedení rack server maximálně 2U

2.2.2 KDC – diskové pole

Počet ks v jedné lokalitě: 1

Počet lokalit celkem (12xKDC bez funkce CDC): 12

2.2.2.1 Závazné parametry

1. Minimální požadovaná čistá, použitelná, formátovaná kapacita diskového pole je 10 TB v RAID 5 (do této kapacity se nezapočítává hotspare HDD)
2. Diskové pole bude obsahovat minimálně 1TB SSD v RAID 5
3. Podpora SAN
4. Řešení poskytuje minimálně 2x 10Gbit/s iSCSI ethernet port na pole pro připojení serverové farmy
5. Řešení poskytuje minimálně 2x 1Gbit/s iSCSI ethernet port na pole pro připojení serverové farmy
6. Diskové pole bude obsahovat minimálně 1 hotspare HDD až na 10 instalovaných HDD a pro každý typ disků
7. Diskové pole podporuje následující typy technologie hotspare (hot standby) a hot plug:
   1) globální a dynamicky hotspare HDD – bez vazby na konkrétní pool (možnost aktivace pro libovolný disk v poli)
   2) preaktivní hotspare HDD - aktivace hotspare při detekci zhoršení parametrů disku ještě před samotným výpadkem
   3) hot plug ventilátory
   4) hot plug redundantní zdroje
8. Diskového pole bude možno rozšířit minimálně na 1,5 násobek kapacity
9. Architektura diskového pole splňuje minimálně následující parametry:
   5) redundantní řadiče (kontroléry)
   6) žádný Single Point Of Failure
   7) zajištění cache paměti proti neočekávanému výpadku napájení automatickým přepsáním jejího obsahu na média nevyžadující napájení pro uložení dat
10. Diskové pole je vybaveno funkcionalitu pro CIFS a NFS datové sdílení po 10Gbit/s interface
11. Souhrnové úložiš diskového pole poskytují minimálně tyto funkce (všechny současně):
   8) schopnost integrace do systému Active Directory
   9) schopnost sdílení dat protokolem CIFS i NFS
12. Řešení plně podporuje minimálně následující technologie pro virtualizaci. VMware 5.x, Citrix Xen Server 6.x a Microsoft Hyper-V 3.x
13. Řešení zahrnuje nástroj pro detailní analýzu výkonnostních parametrů, v reálném čase i historicky
14. Navržená technologie podporuje heterogenní infrastrukturu pro vlastní uložení dat - běžná diková pole v SAN infrastruktuře, a to i různých výrobců současně
15. Řešení poskytuje SNMP rozhraní minimálně ve verzi 2 pro monitorování centrálním dohlížecím systémem
16. Řešení podporuje integraci na úrovni operací failover i fallback pro virtualizační vrstvu
17. Součástí řešení je jednotný SW management systém – jediná konzole. Z tohoto jediného SW je možné spravovat všechny diskové pole v KDC
18. Řešení umožňuje nezávislý přístup pro OOB management po ethernetu

2.2.3 VDI infrastruktura pro ZZS a PČR

Počet ks v jedné lokalitě ZZS:	2
Počet ks v jedné lokalitě PČR (mimo PP PČR):	2

2.2.3.1 Závazné parametry

19. Terminálové RACK server řešení je plně redundantní, a to i na úrovni fyzických serverů(pokud je možné splnit výkonnostní požadavky pomocí 2 fyzických serverů, snižující dodávky budou dle zmíněné logiky 4 fyzické servery ve shodné konfiguraci).
20. Musí umožňovat správu bezpečnostních skupin, uživatelů, oprávnění přístupů do systémů a složek (LDAP)
21. Výkon každého serveru musí zajišsit provozování minimálně 30 terminálových/VDI instancí + 60 fyzických jader
22. Musí umět provozovat uživatelské terminály nebo VDI. A to minimálně pro 30 klientů optimalizovaných na přenos 3x 1920x1200
23. Musí podporovat hromadné nasazování SW
24. Minimálně 4x 1Gbit/s LAN s podporou iSCSI.
25. 2x optický 10Gbit/s ethernet s podporou iSCSI
26. 2x FC 4/8
27. 1000Mb/s pro OIIB management (tyto porty se nezapočítávají do konektivity iRack serveru)
28. Podpora minimálně SNMP v2
29. Řešení nesmí po dobu 5 let plánované přejít do režimu „End of support live" (EOSL)

2.3 Alokace výpočetního výkonu a diskových prostorů

Výkon HW komponent reflektuje identifikované potřeby SW produktů, které budou dodávány v rámci projektu. Kromě již zaškrtnutých SW produktů byl proveden průzkum trhu v oblastech:

- tiketové,
- nahrávání,
- GIS,
- archivační SW,
- zálohovací SW.

Pro tyto komponenty jsou uvedeny maximální parametry požadované u komerčních produktů. Takto dimenzovaný výkon bude potenciálním subdodavatelům poskytnut jako součinnost ve výběrovém řízení.

2.3.1 Alokace pro CDC komponenty

Následující tabulka sumarizuje alokace výpočetního výkonu a diskového prostoru pro SW komponenty provozované v rámci jednoho CDC. V případě lokalit CDC2 a CDC3 bude vzhledem k potřebě souběžného běhu CDC a KDC prostředí alokován součet potřeb CDC a KDC.

Server	Počet jader	RAM (GB)	SSD disk (TB)	SAS disk (TB)
GIS ETL/GIS Adm	2	16		0,5

DB GIS 1	4	32		0,1
DB GIS 2	4	32		0,1
Tiles GIS 1	4	16	0,5	
Tiles GIS 2	4	16	0,5	
DB IPL 1	4	32		2
DB IPL 1	4	32		2
IPL - proces 1	8	32		0,4
IPL - proces 2	8	32		0,4
Nahrávání	4	8		0,1
Telefonie 1	8	12		0,25
Telefonie 2	8	12		0,25
Telefonie 3	8	12		0,25
Telefonie 4	8	12		0,25
Archivace	8	32		0,1
Zálohování	4	16		0,1
LDAP	4	8		0,1
Součet	**94**	**320**	**1**	**6,90**

Tabulka 3 - Alokace HW prostředků pro SW komponenty provozované v rámci jednoho CDC

2.3.2 Alokace pro KDC komponenty

Následující tabulka sumarizuje alokace výpočetního výkonu a diskového prostoru pro SW komponenty

Server	Počet jader	RAM (GB)	SSD disky (TB)	SAS disky (TB)
GIS data	2	16		0,5
GIS/tiles 1	4	32	0,5	0,1
GIS/tiles 2	4	32	0,5	0,1
DB GIS 1	4	32		0,1
DB GIS 2	4	32		0,1
GC telco	2	16		0,2
IPL	4	32		0,4
Nahrávání	8	8		0,1
Telefonie 1	4	8		0,15
Telefonie 2	4	8		0,15
Archivace	4	16		0,1
LDAP	2	8		0,1
Součet	46	299	1	2,1

Tabulka 4 - Alokace HW prostředků pro SW komponenty provozované v rámci jednoho KDC

2.4 Technologie do NSPTV

2.4.1 MiniPC (stanice NSPTV)

Počet ks v jedné lokalitě: různé počty, detailně v příloze č. 3

Počet lokalit celkem (14x NSPTV HZS, 1xPP PČR, 1xGŘ HZS): 16

2.4.1.1 Závazné parametry

1. Technologie x86
2. Frekvence procesoru min. 1,5GHz
3. Operační paměť 4GB RAM
4. Obsahuje 3x výstup na displej DVI nebo DisplayPort
5. Podpora rozlišení na všech monitorech zároveň 1920 x 1200
6. Podpora protokolů MS Hyper-V, Citrix, VMWare View manager min. 4.0
7. Podpora MS RDP a PCoIP
8. Síťové rozhraní 100/1000Mbps UTP Ethernet
9. Integrovaná zvuková karta se samostatným vstupem 3,5mm jack výstupem 3,5mm jack
10. Obsahuje minimálně 4x USB 2.0 port
11. Chlazení pasivní a netočivé části
12. Splňuje Energy Star V. 5.0
13. Součástí dodávky bude také potřebná kabelá
14. Provedení miniPC v podobě RACK pro NSPTV HZS (do technologických místností) nebo standalone PC (pro lokality PP PČR a GŘ HZS)

2.4.2 Display

Počet ks v jedné lokalitě: různé počty, detailně v příloze č. 3

Počet lokalit celkem (14x NSPTV HZS, 14xNSPTV ZZS, 1xPP PČR, 1xGŘ HZS): 30

2.4.2.1 Závazné parametry

1. Úhlopříčka 24", max. šířka rámečku 1 cm
2. Rozlišení 1920 x 1200
3. Jas minimálně 300 cd/m²
4. Doba odezvy max. 8 ms
5. Dynamický kontrast 5000000:1
6. Pozorovací úhly H: 178 stupňů/ V: 178 stupňů
7. Technologie typu S-PVA,IPS,P-IPS,S-IPS s LED podsvícením
8. Konektory DVI, VGA, DisplayPort, USB, 3,5 mm audio
9. Integrované reproduktory
10. Délka kabelu bude upřesněna na základě místního šetření
11. Plně polohovatelný. Možnost umístění monitoru na držák typu VESA 100 (display disponuje standardními montážní otvory na zadní straně: 100x100 mm, resp. 2.95 x 2.95 palce nebo 3,94x3,94 palce, instalace za užití šroubů o průměru 4 mm)

2.4.3 Klávesnice

Počet ks v jedné lokalitě: různé počty, detailně v příloze č. 3

Počet lokalit celkem (14x NSPTV HZS, 14xNSPTV ZZS, 1xPP PČR, 1xGŘ HZS): 30

2.4.3.1 Závazné parametry

1. USB rozhraní, délka kabelu bude upřesněna na základě místního šetření
2. Bez programovatelných kláves
3. Bez multimediálních kláves
4. Český popis klávesnice
5. S numerickou klávesnicí

2.4.4 Myš

Počet ks v jedné lokalitě: různé počty, detailně v příloze č. 3

Počet lokalit celkem (14x NSPTV IZS, 14xNSPTV ZZS, 1xPP PČR, 1xGŘ HZS): 30

2.4.4.1 Závazné parametry

1. 3 tlačítka (levé a pravé tlačítko + středové kolečko tlačítkové jako prostřední tlačítko).
2. Připojení pomocí USB, délka kabelu bude upřesněna na základě místního šetření
3. Podpora OS Linux 2.6, MS Windows 2000, XP, Vista, 7
4. Univerzální provedení pro praváky i leváky
5. Typ optický/laser
6. Rozlišení 400 - 3200 CPI

2.4.5 Tiskárna

Počet ks v jedné lokalitě: 1

Počet lokalit celkem (14xNSPTV IZS, 14xNSPTV PČR, 14xNSPTV ZZS, 1xPP PČR, 1xGŘ HZS): 44

2.4.5.1 Závazné parametry

1. Laserová barevná síťová multifunkční tiskárna formátu A4
2. Umístění na stůl
3. Zatížení max. 5 tis. A4 měsíčně
4. Připojení pomocí LAN 100 Mb/s ethernet

2.4.6 RACK

Počet ks v jedné lokalitě: 1

Počet lokalit celkem: 14xNSPTV PČR

2.4.6.1 Závazné parametry

1. Kovové provedení
2. Formát stěžně 19"
3. Rozměr: 800mm x 1000mm
4. Výška minimálně 10U

2.4.7 Hlasový crossconnect

Počet lokalit celkem (14x NSPTV IZS): 14

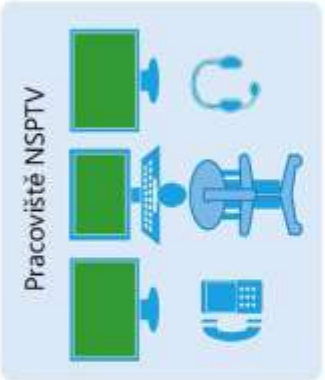
2.4.7.1 Závazné parametry

Tato komponenta a její parametry budou specifikovány v rámci Technického konceptu v projektu KSP IZS

2.4.8 Zapojení pracoviště NSPTV

2.4.8.1 Pracoviště NSPTV (dodávané do lokalit HZS, PP PČR, GŘ HZS)

MiniPC budou umístěna v technologické místnosti a kabeláž jsou přivedeny periferie přímo na operátorské stoly (operátorské stoly nejsou součástí dodávky). Pracoviště je vybaveno IP telefonem (technická specifikace v části J-Telefonie), klientskou stanicí se 3 displeji, klávesnicí a myší a náhlavní soupravou (technická specifikace v části J-Telefonie). Dodávka z NIS IZS zahrnuje také konfiguraci klienta, instalaci do technologické místnosti a propojení s periferiemi na sále operačního střediska. Počet dodávaných komponent pro pracoviště do jednotlivých lokalit je uveden v příloze č. 3.



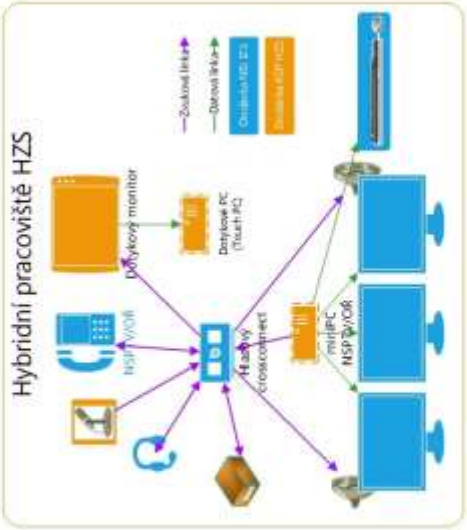
Obrázek 10 – Samostatné Pracoviště NSPTV z pohledu operátora

2.4.9 Hybridní pracoviště v prostředí jednotlivých složek

Hybridní pracoviště je rozšířením pracoviště NIS tak, aby je bylo možné využít buď v režimu pro příjem tísňových hovorů, nebo v režimu pro operační řízení, a to přepínáním veškerých periferií pracoviště pomocí křížového přepínače na příslušného klienta NIS nebo operačního řízení.

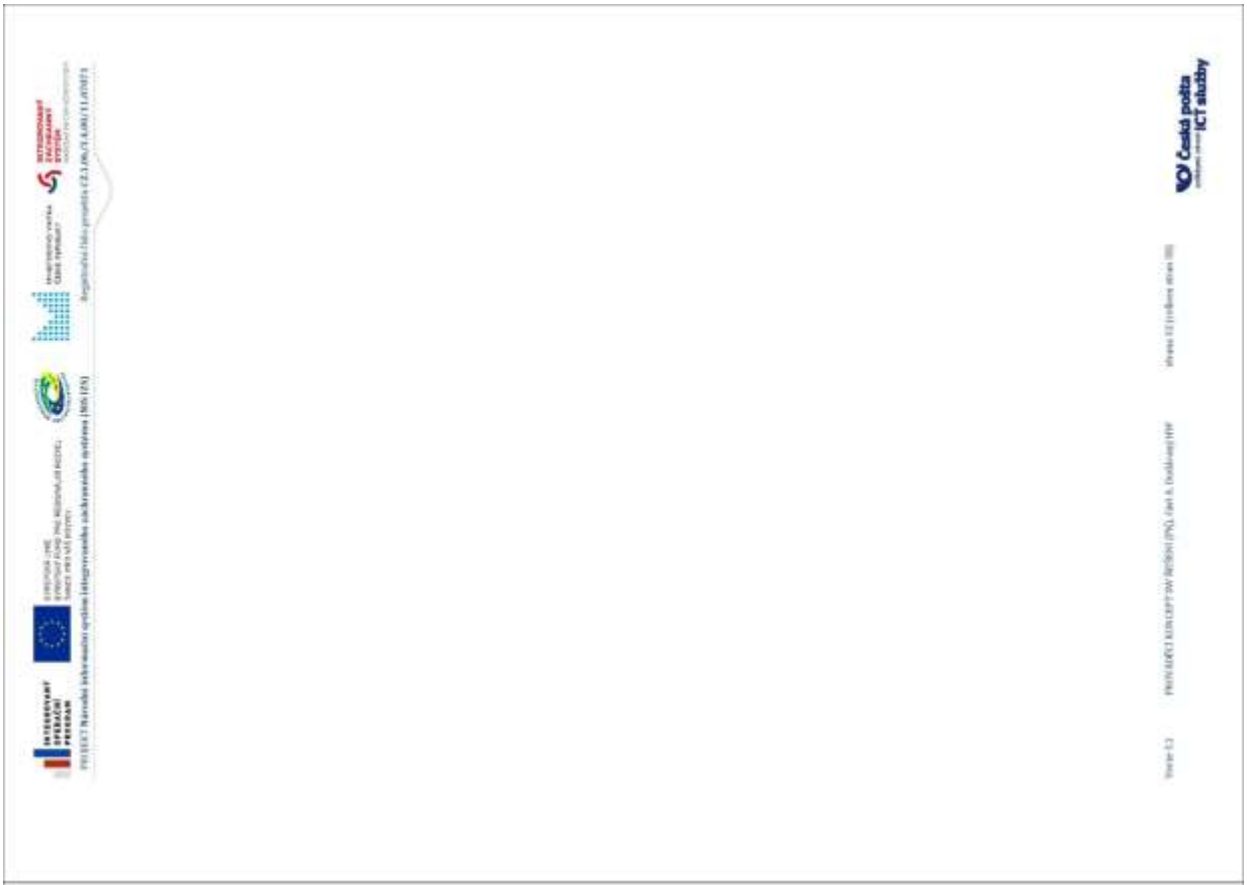
2.4.9.1 Hybridní pracoviště HZS

Pracoviště NSPTV bude realizováno instalací klientské části aplikace NSPTV na pracovní stanici OŘ (miniPC nebo PC) dodávaném z projektu HSP HZS. Pracovní stanice OŘ musí splňovat minimální výkonnostní a portové požadavky, jako „miniPC" dodávané pro samostatné pracoviště NSPTV. Pracovní stanice OŘ budou umístěny v technologických místnostech, které v součinnosti zajišťuje zadavatel. Délky kabelůže dodavatel upřesní na základě místního šetření. Dodávka hybridního pracoviště NSPTV pro HZS z projektu NIS IZS zahrnuje IP telefon (technická specifikace v části J-Telefonie), náhlavní soupravu (technická specifikace v části J-Telefonie), hlasový crosconnect). Financování je znázorněno na obrázku.



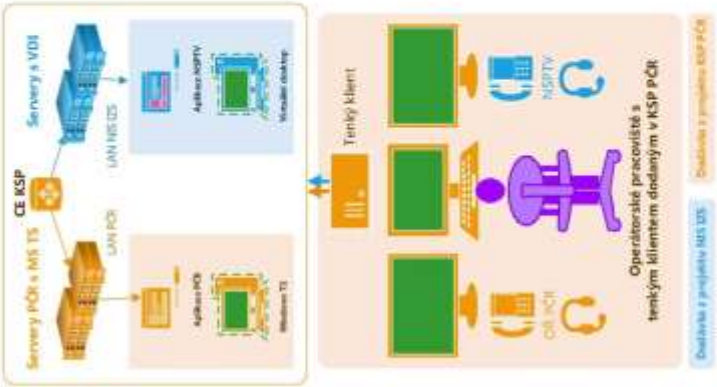
Obrázek 11 - Hybridní pracoviště HZS

Kasuistiky dodávek z projektu NIS IZS je uveden v příloze č. 3.



2.4.9.2 Hybridní pracoviště PČR

Dodávka hybridních pracovišť do lokalit PČR bude realizována pomocí VDI serverů s počtem licencí, který odpovídá minimálně počtu pracovišť PČR v daném kraji. Přepínání mezi virtuálními stanicemi NIS IZS a KSP PČR bude zajištěno pomocí virtuálního KVM. Dále budou v rámci těchto pracovišť dodávány IP telefony (technická specifikace v části J-Telefonie) s náhlavní soupravou (technická specifikace v části J-Telefonie). V koordinaci s paralelně probíhajícím projektem KSP PČR bude dodávka realizována doplněním ke stávající infrastruktuře v rozsahu, který je vyobrazen na následujícím schématu. Po projektu KSP PČR je požadován tenký klient (Thin PC) minimálně o parametrech definovaných v kapitole 2.4.1.



Obrázek 12 - Hybridní pracoviště PČR

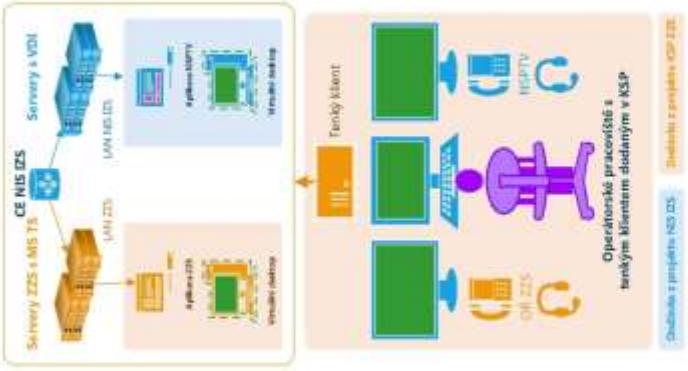
Konzovník dodávek z projektu NIS IZS je uveden v příloze č. 3. IP telefon bude umístěn na operátorský stůl OR PČR, kde bude v současnosti složky připravena LAN (RJ-45) zásuvka určená do serverovny. Do této serverovny bude dodávána serverová VDI infrastruktura.

2.4.9.3 Hybridní pracoviště ZZS

Dodávka Hybridního pracoviště NIS IZS (typ A)

Dodávka hybridních pracovišť do lokalit ZZS bude realizována pomocí VDI serverů s pohřbem licencí, který odpovídá minimálně počtu pracovišť ZZS v daném kraji. Přepínání mezi virtuálními stanicemi NIS IZS a KSP ZZS bude zajištěno pomocí virtuálního KVM. Dále budou v rámci těchto pracovišť dodávány IP telefony (technická specifikace v části J-Telefonie) s náhlavní soupravou (technická specifikace v části J-Telefonie). V koordinaci s paralelně probíhajícími projekty KSP ZZS budou dodávky realizovány doplněním k infrastruktuře pořizované v rámci projektů KSP ZZS v rozsahu, který je vyobrazen na následujícím schématu. Po projektech KSP ZZS je požadován tenký klient (Thin PC) minimálně o parametrech definovaných v kapitole 2.4.1.

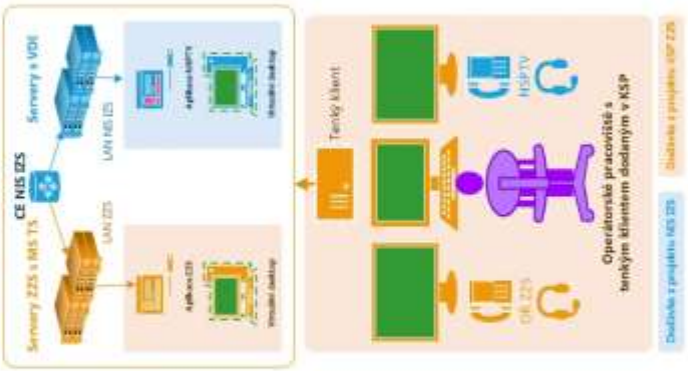
Kusovník dodávek z projektu NIS IZS je uveden v příloze č. 3. IP telefon bude umístěn na operátorský stůl OR ZZS, kde bude v součinnosti složky připraveno LAN (RJ-45) zásuvka ústící do serveroven. Do této serveroven bude v rámci projektu NIS IZS dodávána serverová VDI infrastruktura.



Obrázek 13 - Hybridní pracoviště ZZS typu A

Dodávka Hybridního pracoviště NIS IZS (typ B)

Filosofie hybridních pracovišť typu B je v principu shodná s typem A. Oproti dodávkám typu A však dodávky dle typu B neobsahují monitory. Rozsah dodávky ilustruje následující schéma, kusovník z projektu NIS IZS je uveden v příloze č. 3.



Obrázek 14 - Hybridní pracoviště ZZS typu B

3 Umístění HW komponent

3.1 Metodika členění dodávky

Pro popis dodávaného HW byla použita tato metodika pro členění dodávek:

- **Lokalita** – prostor, kde je umístěn příslušný systém. Přehled všech lokalit je uveden v příloze č. 1.
- **Komponenta** – uzavřená část zařízení tvořící logický funkční celek, fyzicky umístěná v jedné lokalitě. Komponenta je jednoznačně definována v technické specifikaci, pouze u jedné z komponent (Blade server farma) jsou uváděny dvě výkonové varianty pro lokalitu CDC1 a lokality CDC2 a 3.

V rámci projektu jsou definovány tyto logické kategorie lokalit:

- **CDC** – Centrální datové centrum – celkem 3 lokality (CDC1 s mírně výkonnou serverovou farmou než CDC2 a CDC3, přičemž tato dvě CDC budou zároveň zajišťovat i funkci místně příslušného KDC a OS IZS).
- **KDC** – Krajské datové centrum – 1 v každém kraji (umístěno u IZS) s umístěním krajských technologií a technologií místně příslušného operačního střediska IZS (zahrnuje tedy i lokality NSPTV IZS), celkem 12 lokalit (KDC DL a KDC PL jsou sloučena s CDC2 a CDC3).
- **NSPTV** – Operační střediska NSPTV - samostatné pro každou složku v každém kraji + GŘ HZS a PP PČR, toto označení je volteno z důvodu, že technologie dodávané do těchto lokalit budou umístěny jak v technologické místnosti NSPTV, tak na operačním sále, operační středisko NSPTV tedy zahrnuje:
  - a) technologickou místnost pro umístění síťových technologií a
  - b) vlastní operační sál NSPTV s operátorskými pracovišti.

  Celkem se jedná o 30 lokalit (tj. 14 x NSPTV ZZS, 14 x NSPTV PČR, 1 x PP PČR, 1 x GŘ HZS, operační střediska NSPTV složky IZS jsou již zahrnuta v lokalitách KDC, resp. CDC).

Technologie jsou tedy celkem dodávány do 45 lokalit:

- 1 x lokalita CDC bez rozšíření
- 2 x lokalita CDC s rozšířením o funkce KDC HZS a NSPTV HZS
- 12 x lokalita KDC HZS s rozšířením o funkce NSPTV HZS
- 14 x lokalita NSPTV PČR
- 14 x lokalita NSPTV ZZS
- 1 x lokalita PP PČR
- 1 x lokalita GŘ HZS

3.2 Konvence pro jednoznačnou identifikaci lokalit

Identifikátor lokalit NIS IZS byl volen na základě logických zkratek – centrální datové centrum (CDC), krajské datové centrum (KDC) a operační středisko NSPTV (NSPTV), krajské zkratky byly voleny dle standardu ISO 3166-2:CZ. U NSPTV lokalit složky PČR byla zvolena zažitá konvence označení krajských lokalit KRP + jedno písmeno identifikující kraj.

Seznam konkrétních lokalit, do kterých bude dodáván HW, včetně identifikátorů je uveden v příloze č. 1.

3.3 Konvence pro jednoznačnou identifikaci komponent

Každá dodávaná komponenta má přidělen jedinečný identifikátor.

Jedinečný identifikátor je ve tvaru:

IDENTIFIKÁTOR_OZN.LOKALITY_POŘ.Č./CELKEM

- ZKRATKA – identifikátor komponenty (viz příloha č. 2)
- OZN.LOKALITY – identifikátor lokality, do které bude zařízení umístěno (viz příloha č. 1)
- POŘ.Č. – Pořadové číslo komponenty v rámci dané lokality
- CELKEM – Celkový počet komponent stejného typu, které jsou dodávány do dané lokality

Příklad označení:

CDC_SMEROVAC_CDC1_1/2 – Centrální CE směrovač dodávaný do lokality CDC1, první z celkových 2, které jsou dodávány do lokality CDC1.

CDC_LB_CDC2_1-2/2 – Centrální Loadbalancery označované identifikátorem CDC_LB_CDC2_1 a CDC_LB_CDC2_2 dodávané do lokality CDC2. 2 z celkových 2, které jsou dodávány do lokality CDC2.

V příloze č. 2 je každé dodávané HW komponentě (bližší specifikace je obsažena v dokumentu, kterému přísluší tato příloha, v části C – Sít nebo v části I – Telefonie) přidělen jednoznačný identifikátor. Zároveň je zachycen souhrn počtu jednotlivých HW komponent dodávaných v rámci projektu NIS IZS.

3.4 Požadavky na technologické zajištění lokalit

3.4.1 CDC

Pro umístění zařízení do CDC (resp. CDC+KDC) je vyžadováno splnění standardů definovaných v Analýze interoperability a těchto požadavků:

3.4.1.1 Energie a napájení

1. Redundantní přívod elektrické energie. Redundantní přívod el. energie do každého racku, fyzicky odělitelných na úrovni rednundantních rozvodných skříní
2. Přívod el. energie je v případě výpadku el. proudu primárního zdroje zajištěn a nahrazen nezávislým zdrojem el. energie poháněným běžně komerčně dostupnými typy paliv (např. dieselagregát), doba provozu na záložní zdroj není definována, musí být možno dodávka el. energie zajistit doplněním paliva takového zdroje
3. Redundantní UPS pro překrytí okamžiku přechodu na záložní zdroj napájení s výdrží min. 1 hodina
4. Definovaný odběr na 1 fyzický RACK je odhadován na 12kW, předpokládáme umístění 4 takových RACKů v rámci jednoho datového sálu
5. Zajištěna energetická pohotovostní služba pro případ výpadku elektrické energie

3.4.1.2 Chlazení

1. Teplota v datovém sálu zajištěna v rozsahu 18 – 22 st. Celsia
2. Zdvojené okruhy zařízení zajišťující chlazení datového sálu, včetně zdvojeného přívodu napájení
3. Monitoring teploty serverovny s automatickým hlášením překročení mezní hodnoty

3.4.1.3 Technický způsob provedení

1. Statická nosnost podlahy (i zdvojené) jednoho racku NIS je minimálně 700 kg
2. Servisní prostor pro přístup k zařízením umístěných v každém racku z obou stran (přední a zadní) min. 800mm
3. Připojení ke komunikační infrastruktuře pomocí centrálních kabelových rozvodů umístěných buď pod zdvojenou podlahou, nebo jiným kabelovým kanálem umístěným nad rackovým prostorem
4. Minimálně 4 x RACK 19" 800* 1000 (42 U)

3.4.1.4 Fyzické zajištění bezpečnosti

1. Objekt přístupný v režimu 24/7
2. Zajištění monitorované a evidované fyzické identifikace osob dle přiděleného oprávnění v režimu autorizace založené na více definovatelných faktorech (např. kartový přístupový systém nebo další technologie, pracující např. na neměnných biometrických parametrech)
30. Stálá dohledová služba monitorující celkový stav datového centra jako funkčního celku

3.4.2 KDC

Pro umístění zařízení do KDC je vyžadováno splnění standardů definovaných v Analýze interoperability a těchto požadavků.

3.4.2.1 Energie a napájení

1. Redundantní přívod elektrické energie do každého racku, fyzicky oddělených na úrovni redundantních rozvodných skříní
2. Přívod el. energie je v případě výpadku el. proudu primárního zdroje el. energie zajištěn a nahrazen nezávislým zdrojem el. energie pohaněným běžně komerčně dostupnými typy paliv (např. dieselagregát), doba provozu na záložní zdroj není definována, musí být možno dodávku el. energie zajistit doplněním paliva tohoto zdroje
3. Redundantní UPS pro překrytí okamžiku přechodu na záložní zdroj napájení s výdrží min. 30 minut
4. Definovaný odběr na 1 fyzický RACK je odhadován na 8kW, předpokládáme umístění jednoho takového RACKu v rámci jednoho datového sálu

3.4.2.2 Chlazení

1. Teplota v datovém sálu zajištěna v rozsahu 18 – 22 st. Celsia
2. Zdvojené okruhy zařízení zajišťující chlazení datového sálu, včetně zdvojeného přívodu napájení
3. Monitoring teploty serverovny s automatickým hlášením překročení mezní hodnoty

3.4.2.3 Technický způsob provedení

1. Statická nosnost podlahy (i zdvojené) jednoho racku NIS je minimálně 500 kg
2. Servisní prostor pro přístup k zařízením umístěných v každém racku z obou stran (přední a zadní) min. 800 mm
3. Připojení ke komunikační infrastruktuře pomocí centrálních kabelových rozvodů umístěných buď pod zdvojenou podlahou, nebo jiným kabelovým kanálem umístěným nad rackovým prostorem
4. Minimálně 1 x RACK 19" 800*1000 (42 U)

3.4.2.4 Fyzické zajištění bezpečnosti

1. Objekt přístupný v režimu 24/7
2. Zajištění monitorované a evidované fyzické identifikace osob dle přiděleného oprávnění v režimu autorizace založené na více definovatelných faktorech (např. kartový přístupový systém nebo další technologie, pracující např. na neměnných biometrických parametrech)
31. Stálá dohledová služba monitorující celkový stav datového centra jako funkčního celku

3.4.3 NSPTV - Technologická místnost

Pro umístění zařízení NSPTV do technologické místnosti je vyžadováno splnění standardů definovaných v Analýze interoperability a těchto požadavků.

3.4.3.1 Energie a napájení

1. Zdvojené on-line UPS (tam, kde to stavební připravenost a úroveň technologického zázemí dovoluje)
2. Dieselagregát
3. Možnost připojení mobilního agregátu
4. Současně se předpokládá pro operační řízení oddělená elektrorozvodná soustava od zbytku objektu
5. Definovaný odběr na 1 fyzický RACK je odhadován na 1kW, předpokládáme umístění jednoho takového RACKu v rámci jednoho datového sálu

3.4.3.2 Chlazení

1. Teplota v datovém sálu zajištěna v rozsahu 18 – 22 st. Celsia
2. Zdvojené okruhy zařízení zajišťující chlazení datového sálu, včetně zdvojeného přívodu napájení
3. Monitoring teploty serverovny s automatickým hlášením překročení mezní hodnoty

3.4.3.3 Technický způsob provedení

1. Statická nosnost podlahy (i zdvojené) jednoho racku NIS je minimálně 300 kg
2. Servisní prostor pro přístup k zařízením umístěných v každém racku z obou stran (přední a zadní) min. 800 mm
3. Připojení ke komunikační infrastruktuře pomocí centrálních kabelových rozvodů umístěných buď pod zdvojenou podlahou, nebo jiným kabelovým kanálem umístěným nad rackovým prostorem
4. Minimálně 1 x RACK 19" 800*1000 (10 U)

3.4.3.4 Fyzické zajištění bezpečnosti

1. Objekt přístupný v režimu 24/7
2. Zajištění monitorované a evidované fyzické identifikace osob dle přiděleného oprávnění v režimu autorizace založené na více definovatelných faktorech (např. kartový přístupový systém nebo další technologie, pracující např. na neměnných biometrických parametrech)
3. Stálá dohledová služba, u vstupu do objektu, bude chápána i jako služba zajišťovaná technickými prostředky. Např. kartový vstup, kamerový monitorovací systém nebo kombinace fyzické služby v pracovní době a technických prostředků v mimopracovní době.

3.4.4 NSPTV - Operační sál

Pro umístění zařízení NSPTV na operační sál je vyžadováno splnění standardů definovaných v Analýze interoperability a těchto požadavků:

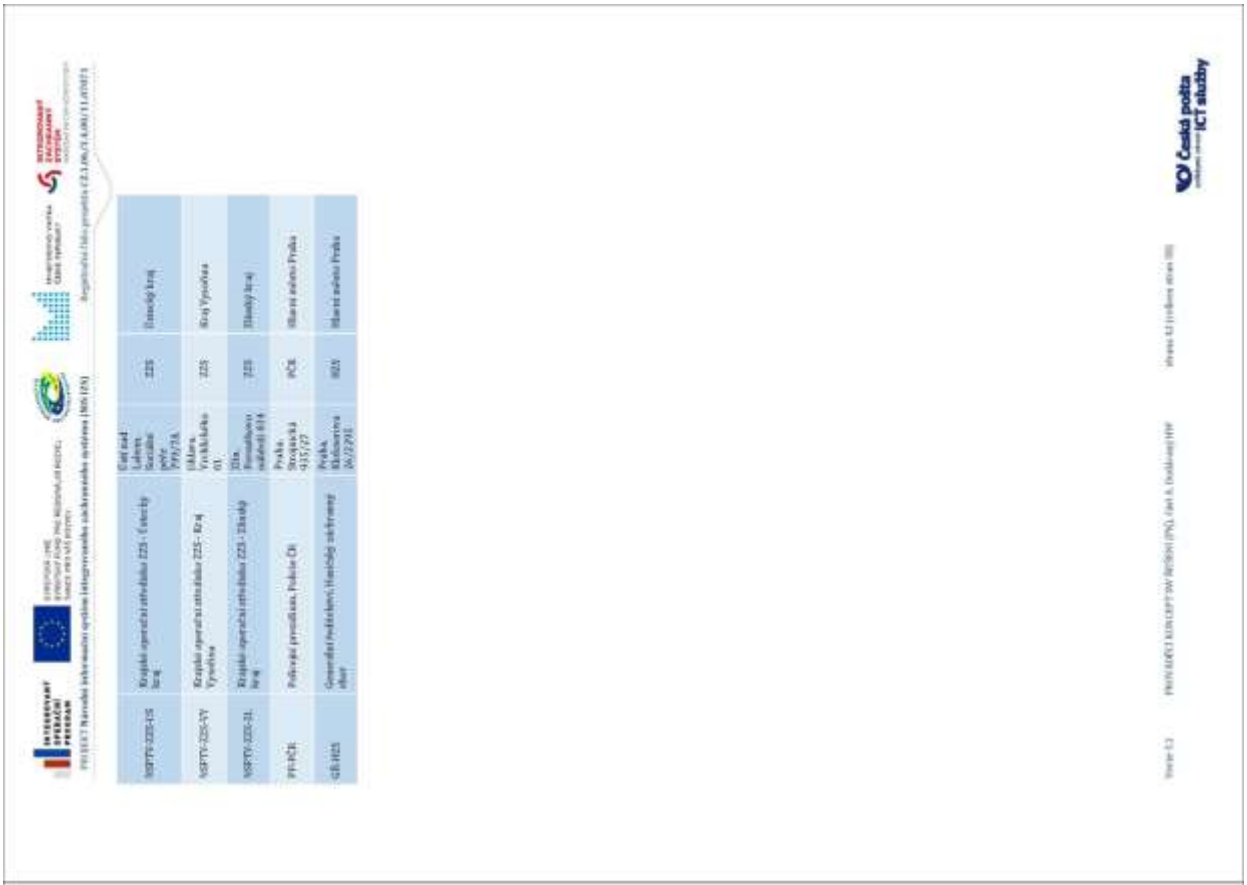
1. Počet volných operátorských stolů – podle počtu dodávaných pracovišť NSPTV viz příloha č. 3.
2. Prostory IZS musí umožnit pořízení veškeré kabeláže z technologické místnosti k operátorským stolům.
3. Parametry jednoho pracoviště (stolu)
   - Počet volných držáků na monitory 3 nebo 0, monitory budou dodány s odnímatelnými stojany. Rozměr monitoru (bez stojanu) 550 x 370 x 250 mm, max. váha 7 kg.

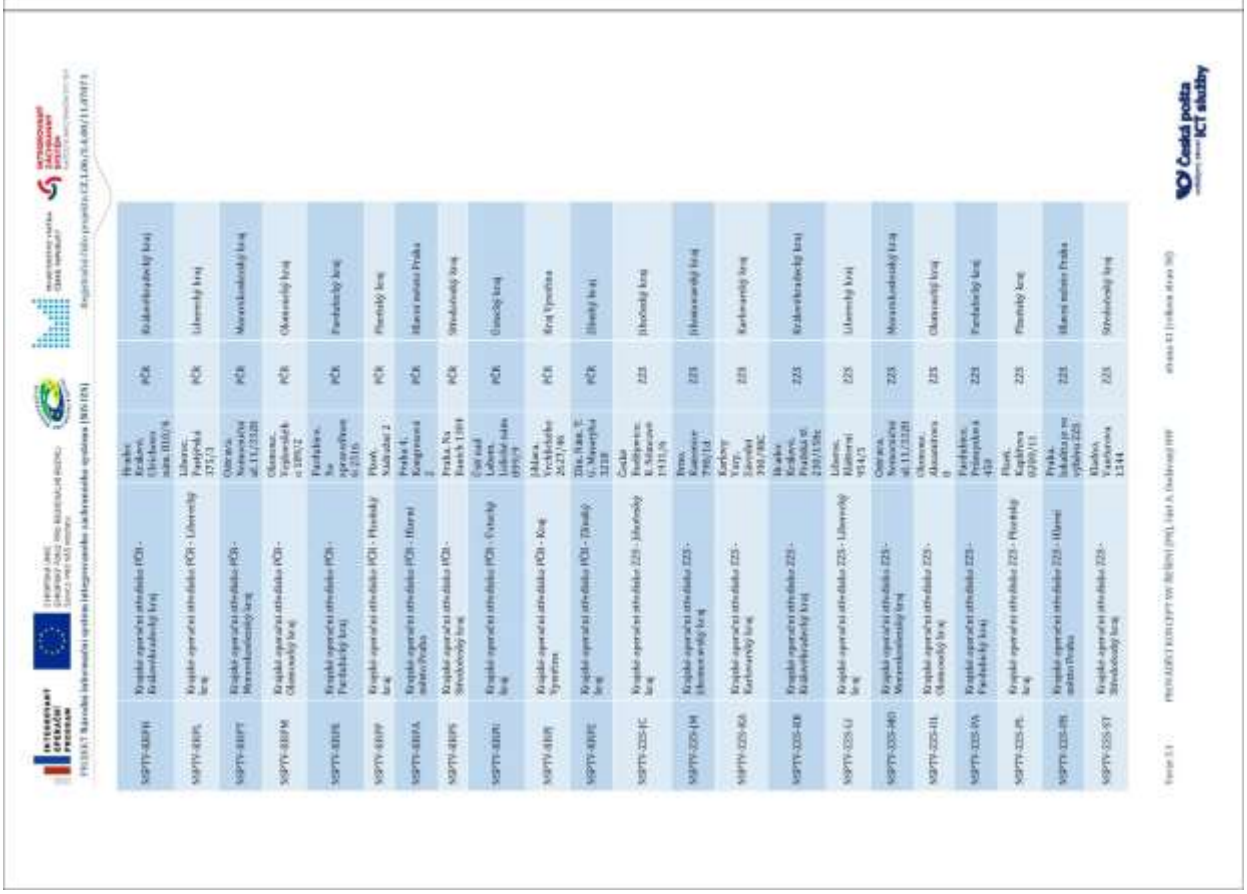
- Počet volných zásuvek 230V ve stále
  a. pracovišté NSTTV - 3 x záložované (3x display), 2 x nezálohované (1x nabíjení na náhlavní soupravu + 1x rezerva). Rezerva napájení 0,23 kVA.
  b. hybridní pracovišté IZS a ZZS - 4 x záložované (3x display, 1x křížový počítač), 2 x nezálohované (1x nabíjení na náhlavní soupravu + 1x rezerva). Rezerva napájení 0,23 kVA. Bude upřesněno za pomoci místního Setfrení, které vyhlédnuje možnosti připojení v jednotlivých lokalitách.
  c. hybridní pracovišté PČp - 5 x záložované (3x display,), 2 x nezálohované (1x nabíjení na náhlavní soupravu + 1x rezerva). Rezerva napájení 0,23 kVA.
- Připojení na 2 x zásuvka LAN 100/1000 Base-T Gigabit Et.
- Volné místo pro tiskárnu vč. zásuvky 230V a připojení na LAN 100 Mb/s ethernet.

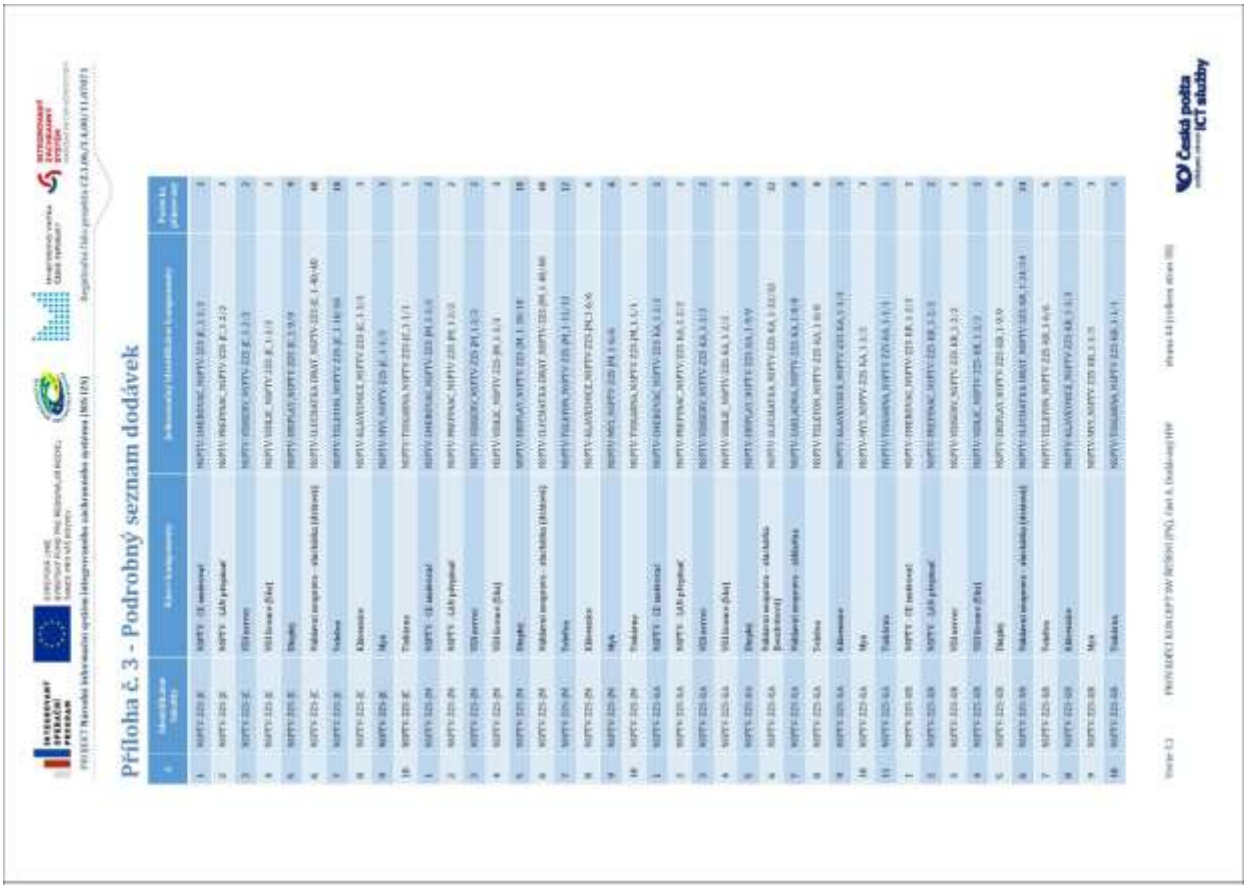
Přílohy

Příloha č. 1 - Identifikace lokalit

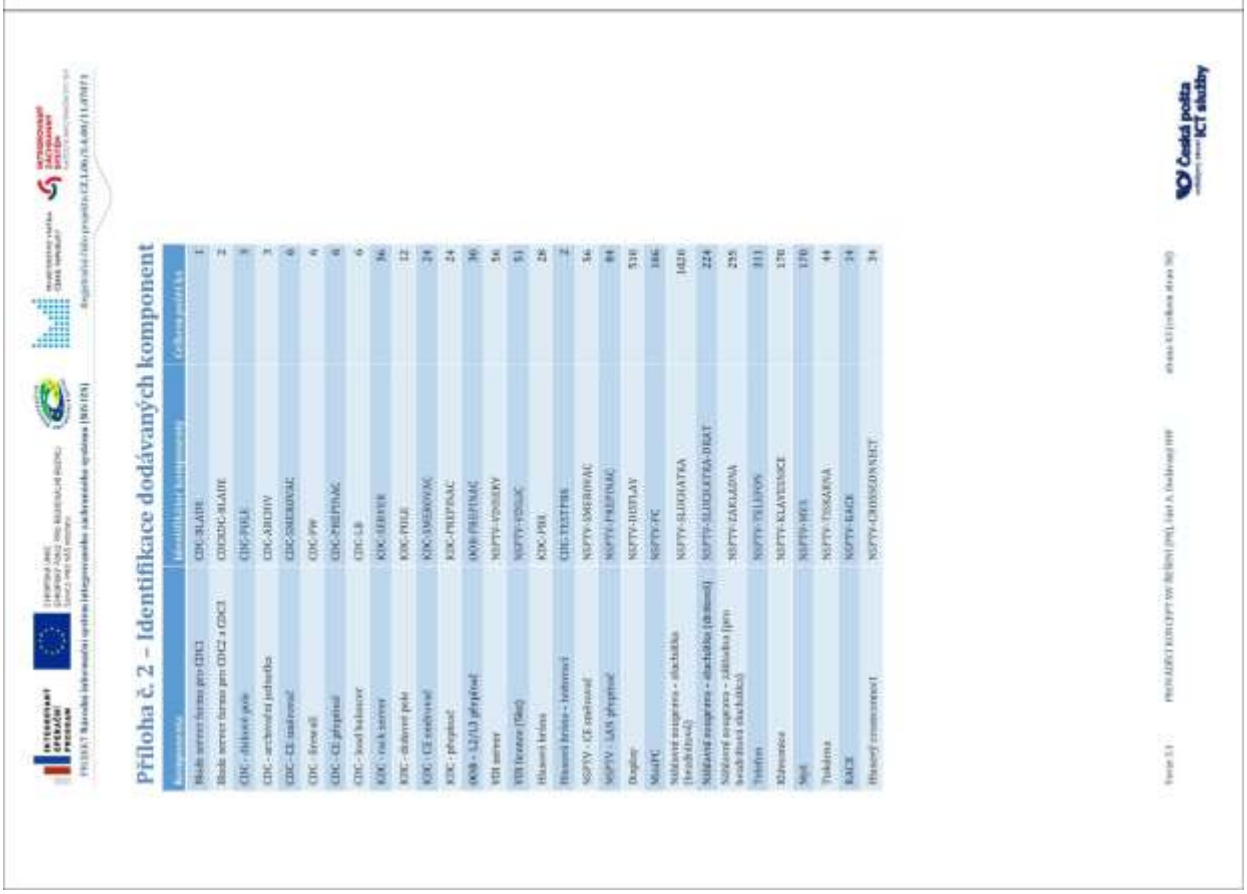
Identifikátor	Název lokality	Adresa	Budova	Kraj
CDC-1	Centrální datové centrum SIS IZS 1	Praha, Olšanská 4	NIS	Hlavní město Praha
CDC-2	Centrální datové centrum SIS IZS 2; Krajské datové centrum - Olomoucký kraj a Krajské operační středisko IZS - Olomoucký kraj	Olomouc, Schwetzerova 524/11	IZS	Olomoucký kraj
CDC-3	Centrální datové centrum SIS IZS 3; Krajské operační středisko IZS - Plzeňský kraj	Plzeň, Kopečkova 2726/9	IZS	Plzeňský kraj
KDC-VC	Krajské datové centrum - Libereckého kraje a Krajské operační středisko IZS - Libereckého kraje	Česká Lípa, Purkyňova, Prachová 52b	IZS	Liberecký kraj
KDC-JM	Krajské datové centrum - Jihomoravský kraj a Krajské operační středisko IZS - Jihomoravského kraje	Brno, Cejl 434/4, 1998/20a	IZS	Jihomoravský kraj
KDC-KA	Krajské datové centrum - Karlovarský kraj a Krajské operační středisko IZS - Karlovarského kraje	Karlovy Vary, Závodní 2017/70	IZS	Karlovarský kraj
KDC-KR	Krajské datové centrum - Královéhradecký kraj a Krajské operační středisko IZS - Královéhradeckého kraje	Hradec Králové, Pivovarská 1/1 739/1380	IZS	Královéhradecký kraj
KDC-LI	Krajské datové centrum - Liberecký kraj a Krajské operační středisko IZS - Libereckého kraje	Liberec, Sokolovská 414/11	IZS	Liberecký kraj
KDC-MO	Krajské datové centrum - Moravskoslezský kraj a Krajské operační středisko IZS - Moravskoslezského kraje	Ostrava, Nádražní ul. 11/1320	IZS	Moravskoslezský kraj
KDC-PA	Krajské datové centrum - Pardubický kraj a Krajské operační středisko IZS - Pardubického kraje	Pardubice, Teplého 1526	IZS	Pardubický kraj
KDC-PR	Krajské datové centrum - Hlavní město Praha a Krajské operační středisko IZS - Hlavní město Praha	Praha, Modřanská	IZS	Hlavní město Praha
KDC-ST	Krajské datové centrum - Středočeský kraj a Krajské operační středisko IZS - Středočeského kraje	Kladno, Zámecká Podbřeh 226	IZS	Středočeský kraj
KDC-US	Krajské datové centrum - Ústecký kraj a Krajské operační středisko IZS - Ústeckého kraje	Ústí nad Labem, Masarykova 347/101	IZS	Ústecký kraj
KDC-VY	Krajské datové centrum - Kraj Vysočina a Krajské operační středisko IZS - Kraj Vysočina	Jihlava, Kosmonosova 1910/12	IZS	Kraj Vysočina
KDC-ZL	Krajské datové centrum - Zlínský kraj a Krajské operační středisko IZS - Zlínského kraje	Zlín, Prštalská 213	IZS	Zlínský kraj
NSPTV-KDPC	Krajské operační středisko PČR - Jihočeský kraj	České Budějovice, Lastovska 1313/35	PČR	Jihočeský kraj
NSPTV-KDPB	Krajské operační středisko PČR - Jihomoravský kraj	Brno, Kounicova 687/24	PČR	Jihomoravský kraj
NSPTV-KDPK	Krajské operační středisko PČR - Karlovarský kraj	Karlovy Vary, Závodní 966/100	PČR	Karlovarský kraj



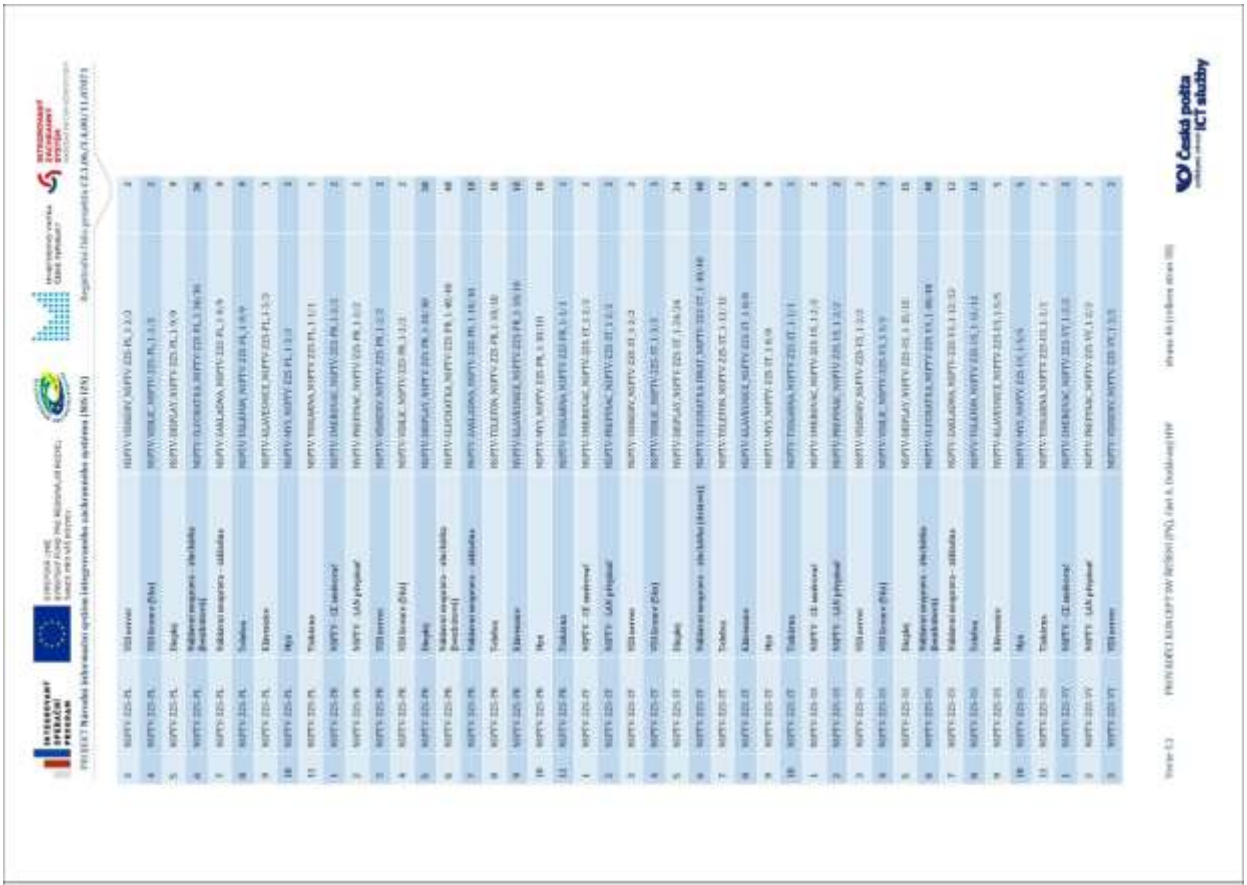


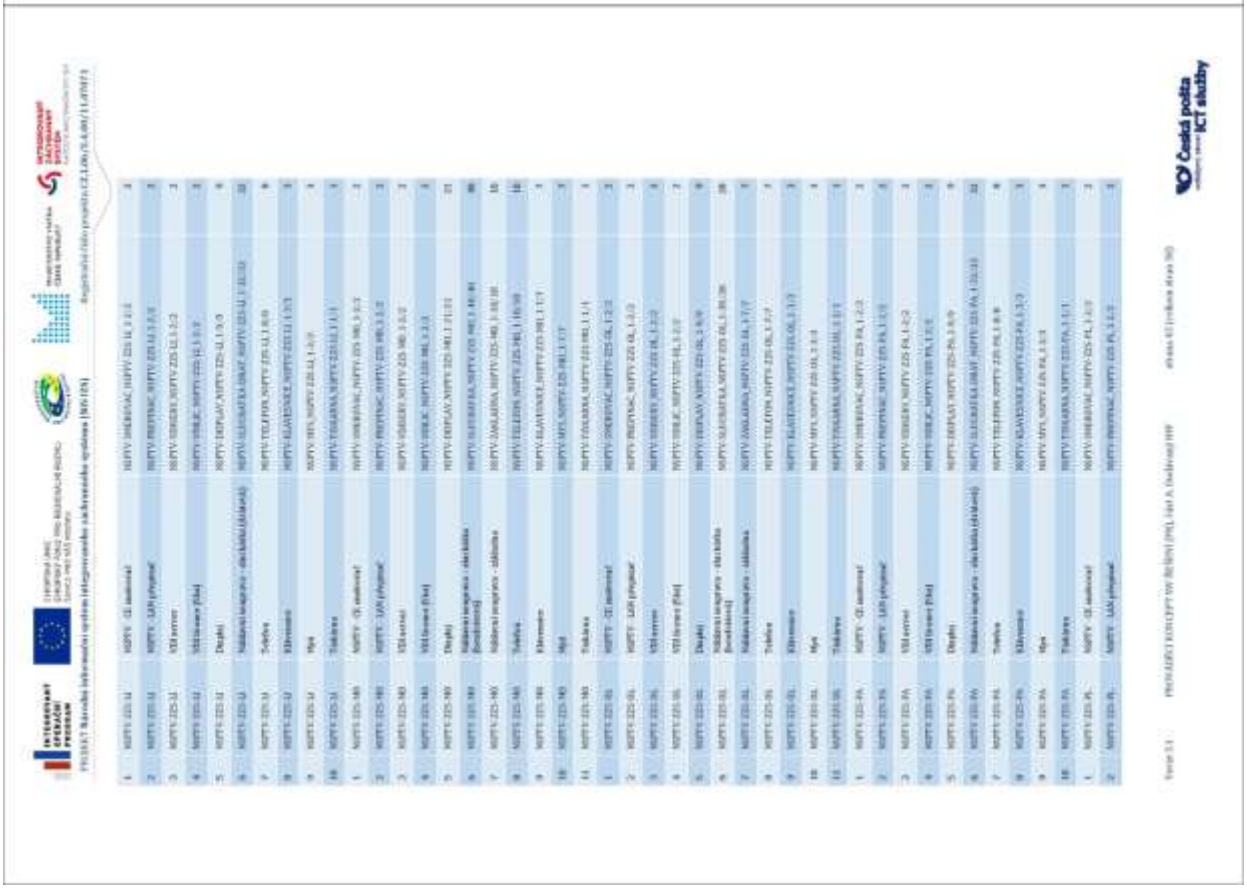


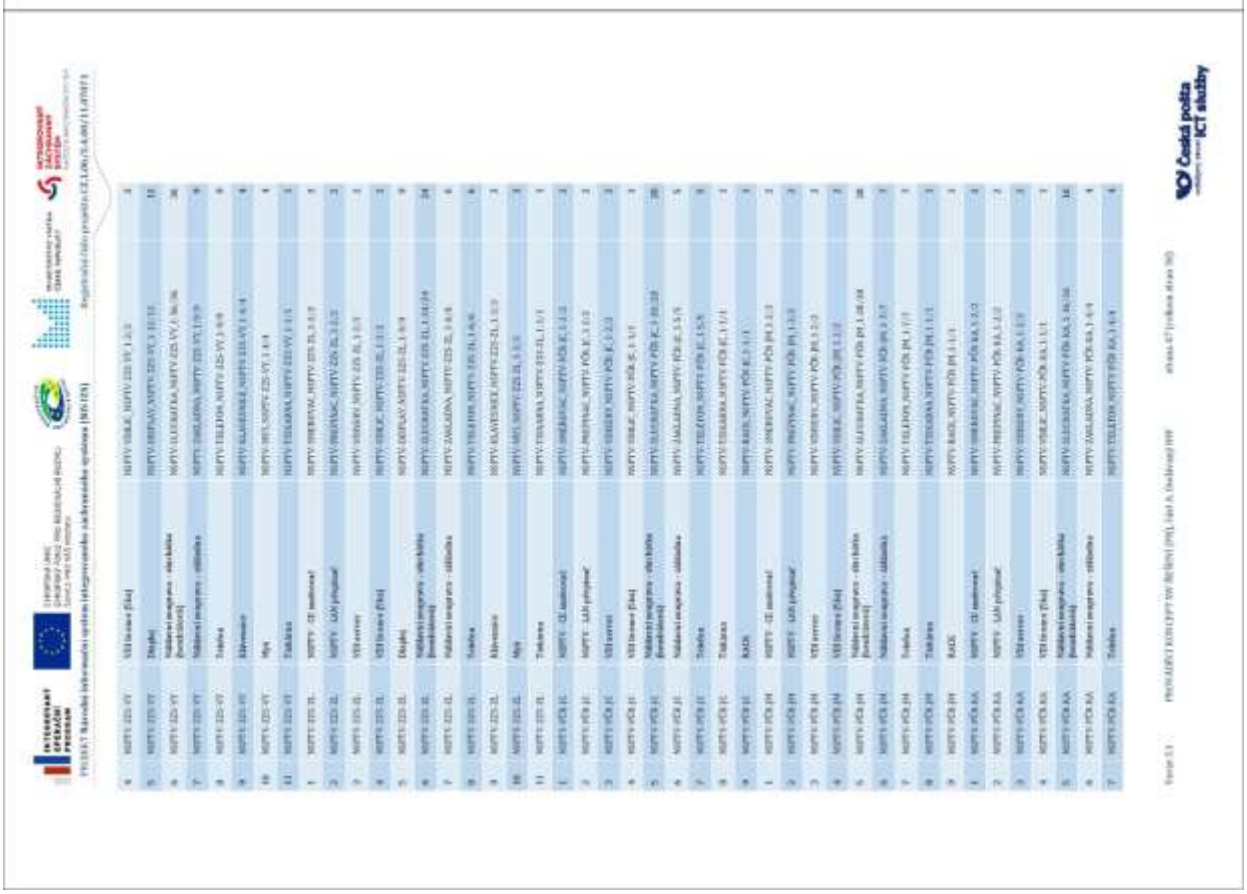
Příloha č. 3 - Podrobný seznam dodávek

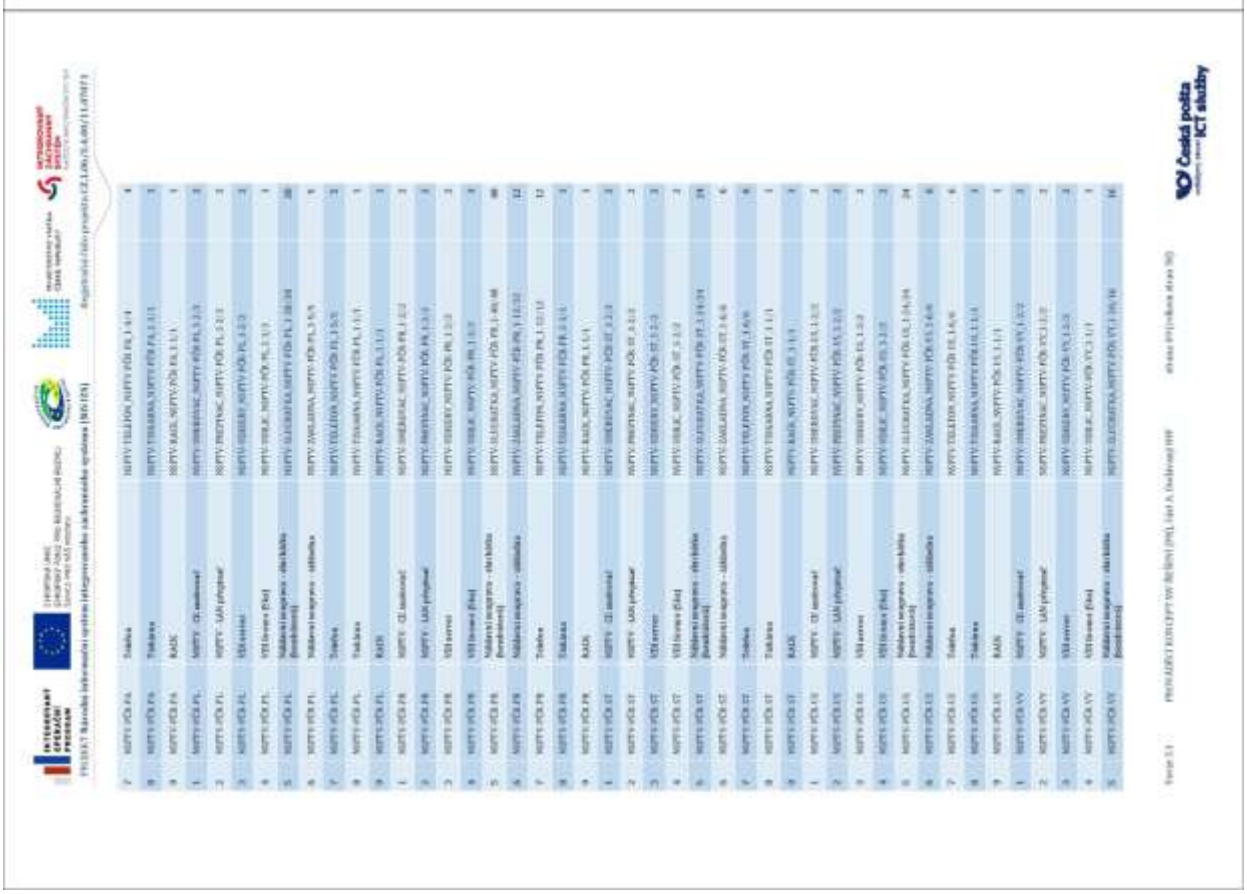


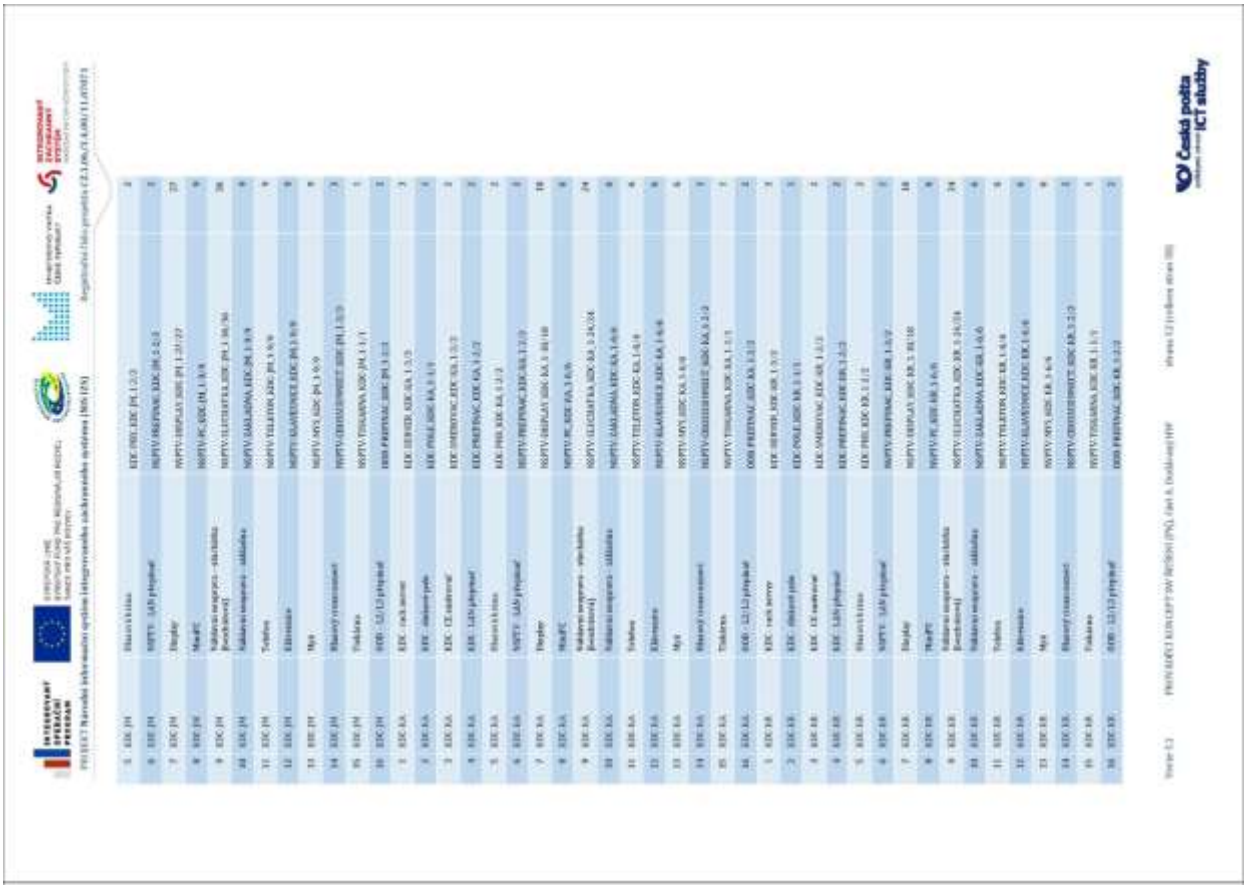
Příloha č. 2 – Identifikace dodávaných komponent

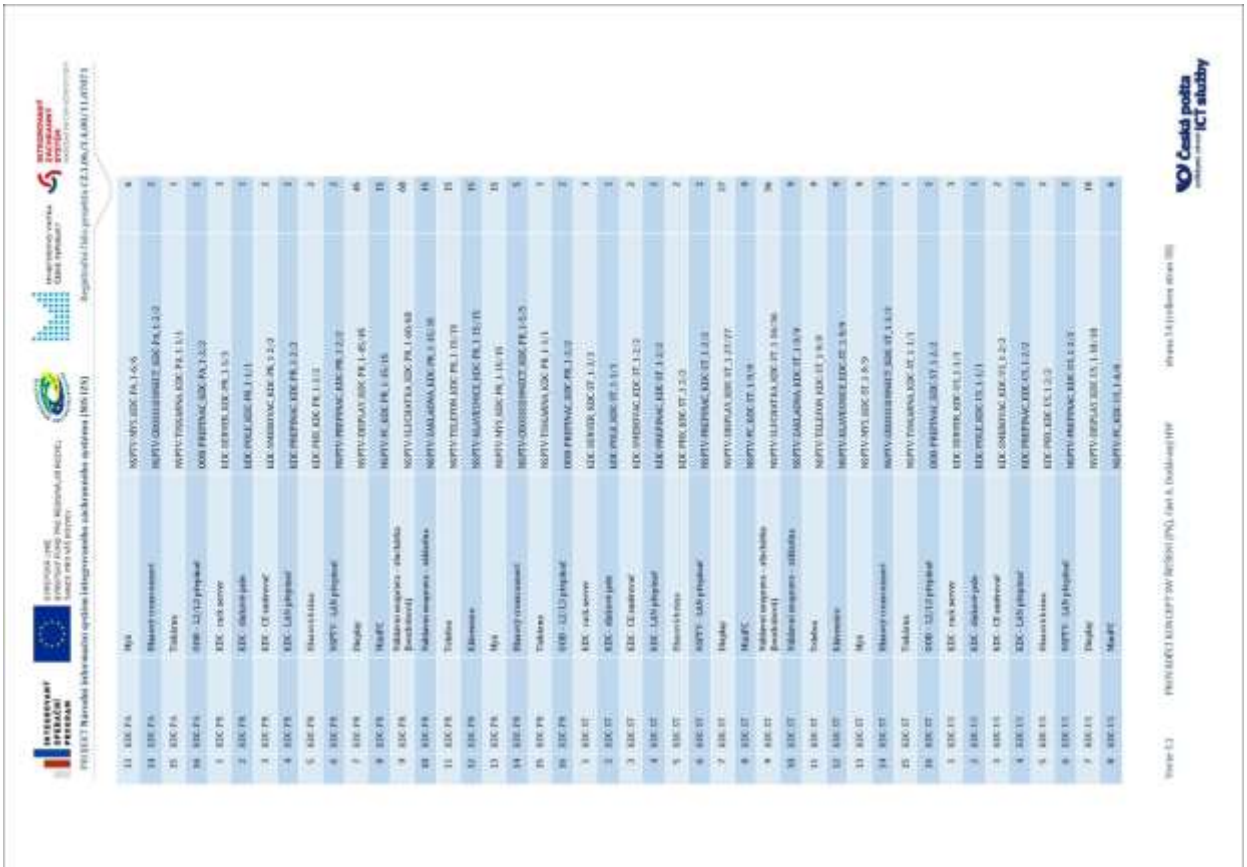


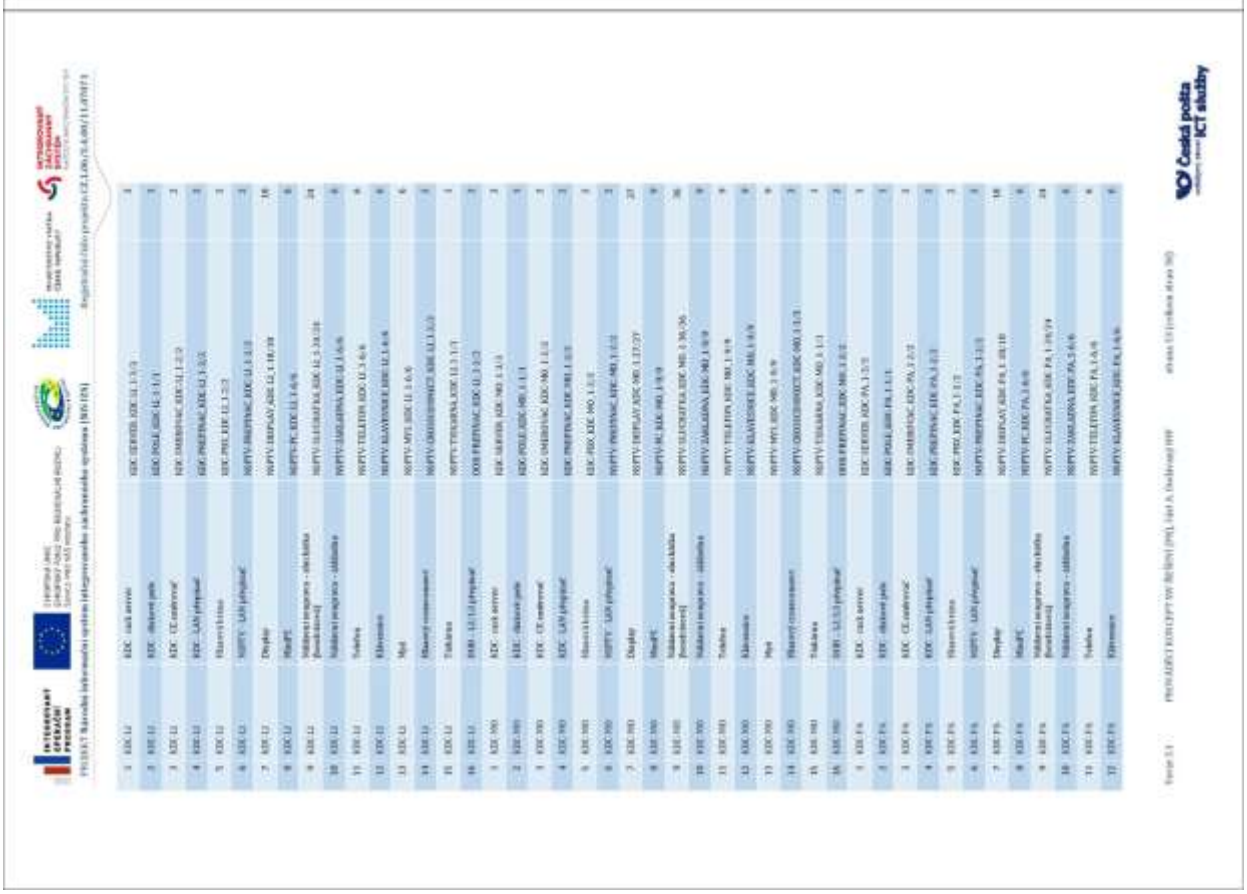


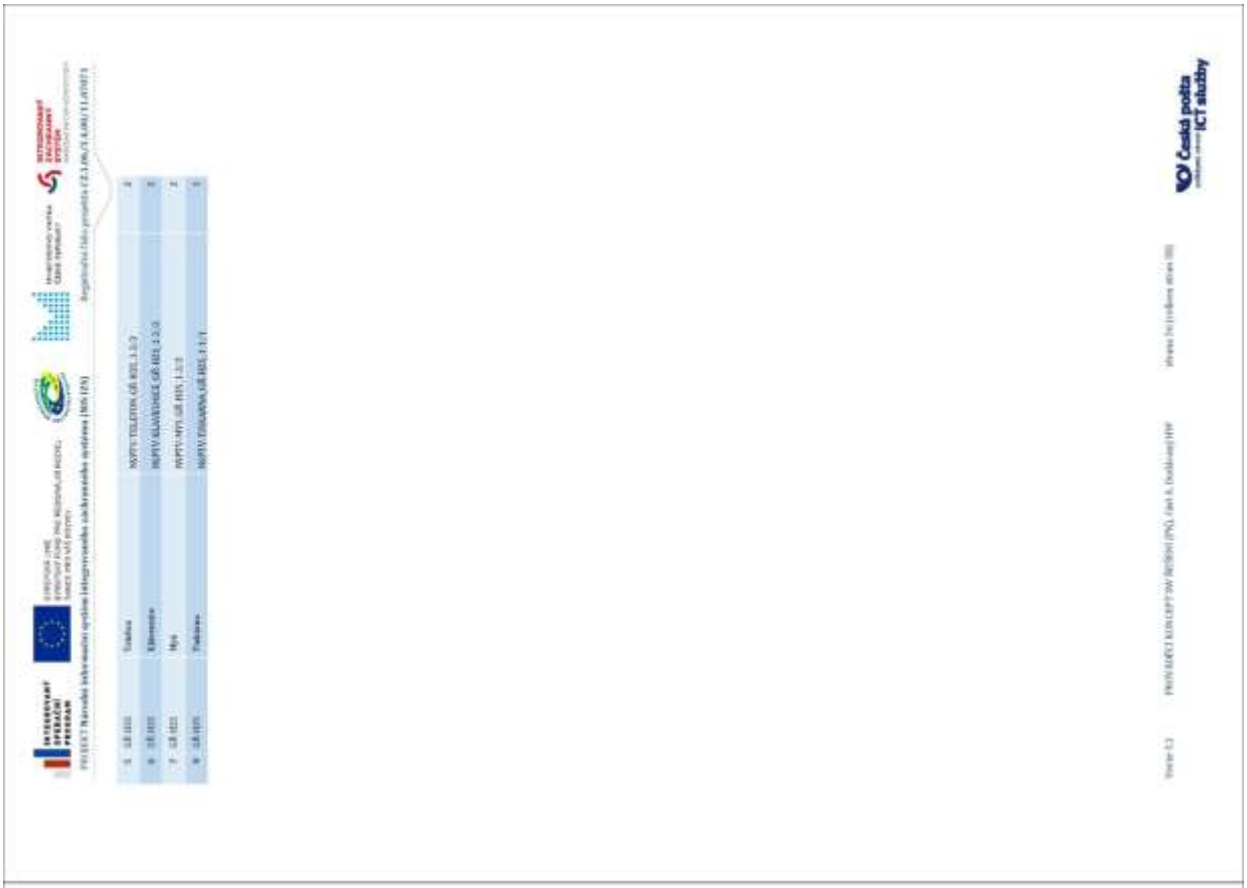


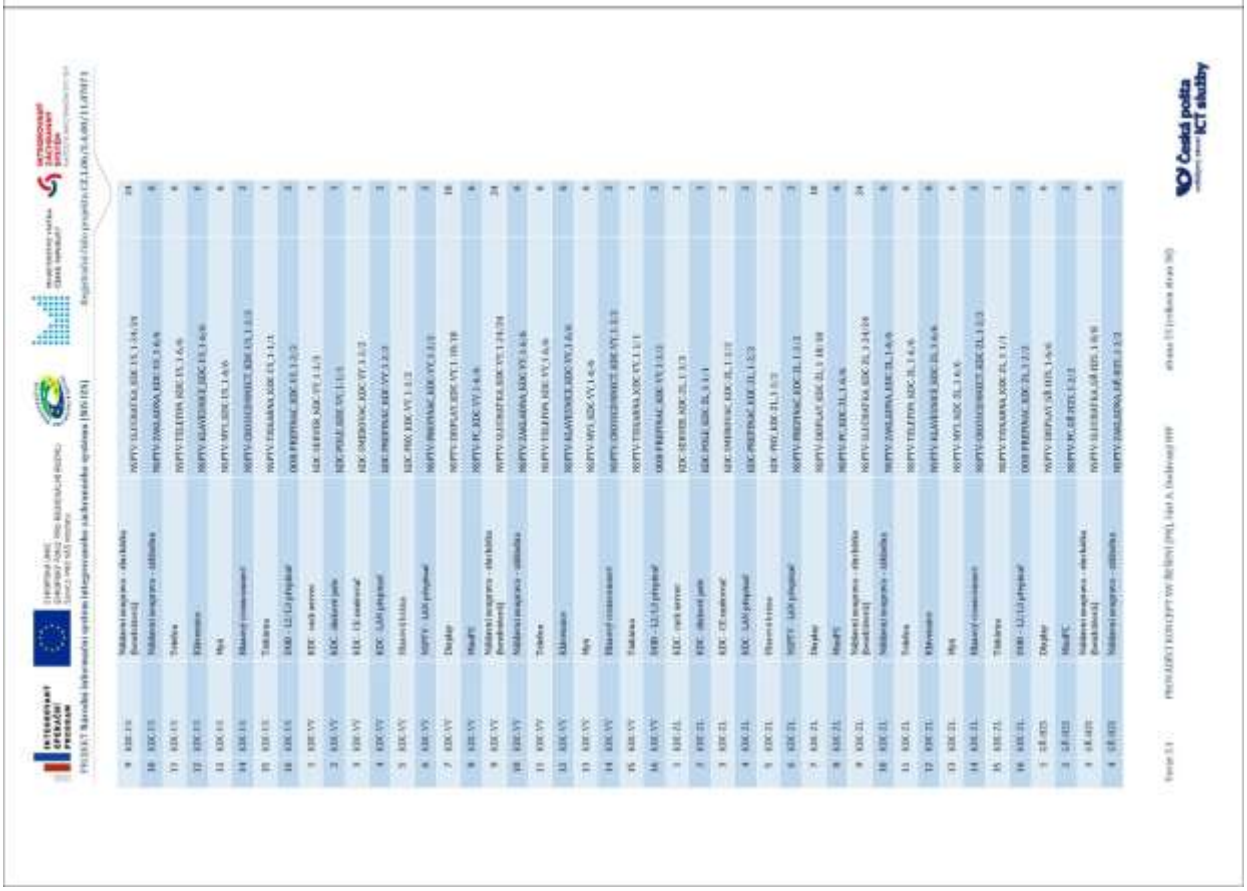












Seznam zkratek

API	Application Programming Interface
CDC	Centrální datové centrum – celkem 3 instance
CE	Střední zařízení, které tvoří tvořky oddělují od ITS
CKS	Centrální úložiště dat
DB	Database
DC	Data centrum
GIS	Geografický informační systém
HA	Hlavní architekt
HTTPS	Hypertext Transfer Protocol Secure - Zabezpečený webový protokol pomocí SSL
HW	Počítačový Hardware
IP	Internet protokol
IS	Informační systémy
ITS NGN	Integrovaná telekomunikační síť nové generace pro Policii České republiky, dodány integrovaného zákaznického systému a ústředí urgentní tísňové správy. Též ve významu projekt „Zajištění infrastruktury pro operační středisko základních složek IZS"
KDC	Krajské datové centrum – 1 v každém kraji (umístěno u HZS), celkem 14 instancí
KVM	Hardwarové zařízení, které umožňuje uživateli ovládat více počítačů z jedné klávesnice, monitoru, myši atd.
LDAP	Systém ověřování v síti
NIS IZS	Národní informační systém integrovaného záchranného systému
NSPTV	Národní systém příjmu tísňového volání
OAM	Out-Of-Band správa
OS	Operační středisko - samostatné pro každou složku v každém kraji + 6 HZS a PP PČR, operační středisko záchranné a technologická nadstavba pro nadstavbu aktivních technologií a k vlastní operační síť, ve kterém bude provozovaný kancelář datové NIS IZS, celkem 44 instancí
OR	Operační Hasiči
PoE	Napájení přes ethernetový kabel
QoS	Quality of Service
reinPC	Konzolová stanice klientů NSPTV. Stažené partitial type tenký klient
SW	Software/Aplikace

Seznam obrázků

Obrázek 1 - Úroveň centralizace/distribuce služeb 5
Obrázek 2 - Poskytovatelé a příjemci služeb z pohledu centrálních a krajských lokalit složek IZS 5
Obrázek 3 - Rozdělení systémových prostředí provozovaných v lokalitě CDC1 7
Obrázek 4 - Rozdělení systémových prostředí provozovaných v lokalitách CDC2 a CDC3 8
Obrázek 5 - Rozdělení systémových prostředí provozovaných v lokalitách KDC 8
Obrázek 6 - Schéma archivačních procesů 11
Obrázek 7 - Princip zálohování mezi centrálními lokalitami 14
Obrázek 8 - Rozsah HW technologií dodávaných do CDC, resp. CDC + KDC, podrobně specifikovaných v části A - HW 17
Obrázek 9 - Rozsah HW technologií dodávaných do jednotlivých KDC, podrobně specifikovaných v části A – HW 21
Obrázek 10 – Samostatné Pracoviště NSPTV z pohledu operátora 29

Seznam tabulek

Tabulka 1- Předpoklady dlouhodobé ukládaných dat 9
Tabulka 2 - Predikce uchovávaných dat na centrálním diskovém poli a v archivu 9
Tabulka 3 - Alokace HW prostředků pro SW komponenty provozované v rámci jednoho CDC 24
Tabulka 4 - Alokace HW prostředků pro SW komponenty provozované v rámci jednoho KDC 25

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

B. Dodávaný SW

Dokument obsahuje:	Popis softwarové architektury NIS IZS.
Verze:	5.1
Schválil za Dodavatele:	Tomáš Faško
Datum předání k připomínkám:	30/10/2013

Projekt Národní informační systém integrovaného záchranného systému (NIS IZS) Registrační číslo projektu CZ.1.06/3.4.00/11.07471

Obsah

1 Architektura softwarové části 5
1.1 Architektura CDC ... 5
1.1.1 Architektura CDC – detail IPL ... 6
1.2 Architektura KDC ... 7
1.2.1 Architektura KDC – detail GIS ... 8
1.2.2 Architektura KDC – detail miniIPL ... 9
1.3 Schéma komunikace ... 10
1.4 Vývojová platforma ... 13
1.4.1 Technologie podporující vývoj ... 13
1.5 Testovací a ověřovací platforma ... 14
1.6 Školící platforma ... 14
1.7 Datová věta ... 14
1.8 Datový Model ... 15
1.8.1 Metodika popisu datového modelu ... 15
1.9 Integritní kritéria ... 17
2 Technické řešení SW komponent 17
2.1 NSPTV aplikace ... 17
2.2 Architektura klienta ... 18
2.2.1 Tlustý klient ... Chyba! Záložka není definována.
2.3 Integrační platforma (IPL) ... 19
2.3.2 Failover ... 20
2.3.3 Balancing ... 20
2.4 MiniIPL na KDC ... 23
2.4.1 Ostrovní režim ... 23
2.5 Komponenty pro centrální GIS v rámci NIS IZS ... 23
2.5.1 Popis komponent centrálního GIS ... 24
2.6 Komponenty pro GIS v rámci KDC ... 27
2.7 Databáze ... 28
2.7.1 Replikace DB ... 28
2.7.2 Návrh lokálního fail-over řešení pro PostgreSQL databázi ... 30
2.7.3 Návrh řešení geografické konfigurace database ... 31

Podpis/signature:.....

2.7.4 Další původně zvažované varianty implementace databázové vrstvy:...**Chyba! Záložka není definována.**
2.7.5 Replikační technologie:...**Chyba! Záložka není definována.**
2.7.6 Příklady replikačních řešení pro konkrétní produkty....**Chyba! Záložka není definována.**
2.7.7 Analýza zvažovaných řešení:...**Chyba! Záložka není definována.**
2.8 Licence...31
2.8.1 OS - Operační systém...31
2.8.2 DBMS - Databáze...32
2.8.3 BIRT - Business Intelligence and Reporting Tools...32
2.8.4 JBoss Fuse - IPL...32
2.8.5 ACTIVITI - BPM systém...32
2.8.6 DROOLS - BR systém...32
2.8.7 MYBATIS - Objektově relační mapování...32
2.8.8 GISSRV - GIS server...32
2.8.9 GISADM - Administrátorský nástroj GIS...33
2.8.10 METAGIS - Metainformační systém pro GIS...33
2.8.11 ETL - Transformace dat...33
2.8.12 VFR - RUIAN import...33
2.8.13 Mapové podklady CEDA...34
2.8.14 JSDI - Příjem a zpracování DDR JSDI...34
2.8.15 HELPER - MST Helper service...**Chyba! Záložka není definována.**
2.9 Reporting...35
2.10 Reference na produkty...35
2.10.1 JBoss Fuse...35
2.10.2 Activiti...35
2.10.3 PostgreSQL...35
2.11 Open source...36
2.12 Koncept provozu...36
2.12.1 Instalace serverové části...36
2.12.2 Instalace klientské aplikace...36
2.13 Aktualizace...37
2.13.1 Aktualizace serverové části...37
2.13.2 Aktualizace klientské aplikace...37
2.14 Monitoring...37
2.14.1 Monitoring serverové části...37
2.14.2 Monitoring koncových pracovišť...37
2.15 Release a Incident Management...38

1 Architektura softwarové části

Softwarové řešení dodávané aplikace NIS IZS je členěno do několika logických celků, které jsou rozmístěny jednak v centrálních datových centrech a jednak v krajských datových centrech. Navržené řešení a použité technologie jsou vybrány s ohledem na požadovanou robustnost výsledného řešení. CDC představuje logickou jednotku, ve které je řízen samotný proces příjmu tísňového volání včetně ukládání primárních dat o událostech a informacích s nimi spojených. Softwarové řešení v CDC je navrženo tak, aby mohlo fungovat jak v paralelním režimu pro rozložení zátěže, tak v režimu, kdy je funkcionalita v CDC omezena.

Krajské datové centrum z pohledu softwaru představuje hlavní vstupní komunikační uzel. Do KDC přechází telefonní hovory z VTS a jsou dále směrovány na odpovídající pracoviště složek IZS. KDC jako takové poskytuje funkcionalitu i pro OŘ a umožňuje v rámci složek komunikaci mezi OŘ a NSPTV. Při ostrovním režimu zajišťuje KDC mezisložkovou komunikaci v rámci OŘ a následnou aktualizaci událostí s NSPTV po přechodu do normálního režimu. Složkami IZS se dále v textu myslí základní složky IZS".

Softwarové řešení NIS IZS je děleno do následujících funkčních bloků:

Telefonie a nahrávání – skládá se z prvku realizující zpracování telefonních hovorů, ovládání telefonu a managementu telefonních ústředen. Dále je součástí tohto bloku i řešení pro nahrávání a přehrávání hovorů (viz kapitola Telefonie).

GIS – reprezentuje produkty pro práci s mapovými podklady a vrstvami informací nad nimi. Funkcionalita GISu je formou mapových služeb na protokolu REST. GISová komponenta má vlastní databázi oddělenou od databáze událostí.

IPL – představuje logický celek, který propojuje logickou komunikaci v systému a směřuje požadavky na informace. Jádrem IPL je opensource technologie JBoss Fuse. Součástí IPL je také integrace na procesní engine realizující samotný proces příjmu tísňového volání opět na opensource technologii Activiti a JBoss Drools. IPL jako takové je pouze na CDC.

miniIPL – plní obdobnou roli jako IPL na CDC s tím rozdílem, že neobsahuje procesní engine. Řešení je analogicky postavena na technologii JBoss Fuse.

Databáze událostí – slouží k ukládání primárních dat NSPTV. Databázové řešení je realizováno pomocí opensource produktu PostreSQL a komerční nástavby enterpriseDB (nebo jiné s minimálně odpovídající 100% funkcionalitou a spolehlivostí), které realizuje multi-master replikaci mezi jednotlivými CDC.

1.1 Architektura CDC

Centrální datové centrum poskytuje z pohledu NSPTV centrální logické úložiště pro práci s jednotlivými událostmi. Dále je v CDC řízen samotný proces příjmu tísňového volání a přístup k mapovým podkladům pro NSPTV. Telefonie a nahrávání jsou popsány v samostatné kapitole.

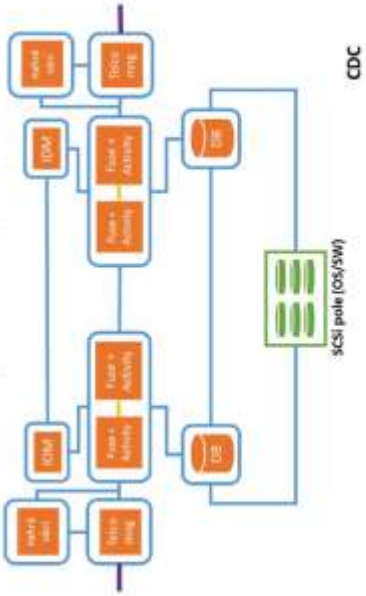
Obrázek 1 popisuje kompletní pohled na rozložení řešení v rámci CDC do detailních logických bloků. SW řešení v rámci jednoho CDC obsahuje dvě funkční větve, které jsou logicky oddělené a v případě výpadku jednoho celku, přejímá bez výpadku funkcionality CDC činnosti větev druhá.

Projekt Národní informační systém integrovaných záchranných systémů (NIS IZS) — Registrovaný projekt (CZ.1.06/3.4.00/11.0797)

Toto zdvojení je důležité pro zajištění běhu řešení při výpadku na úrovni operačních systémů či jednotlivých aplikací.

Legenda

- Oranžové jsou na obrázku zobrazeny jednotlivé SW řešení
- Modře jsou zobrazeny logické celky na úrovni virtualizovaných operačních systémů. Modrá propojení reprezentují komunikaci mezi jednotlivými systémy.
- Zeleně jsou zobrazeny HW segmenty, které jsou důležité z pohledu komunikace mezi softwarovými celky
- Fialová a žlutá znázorňují komunikace uvnitř jednotlivých clusterů.



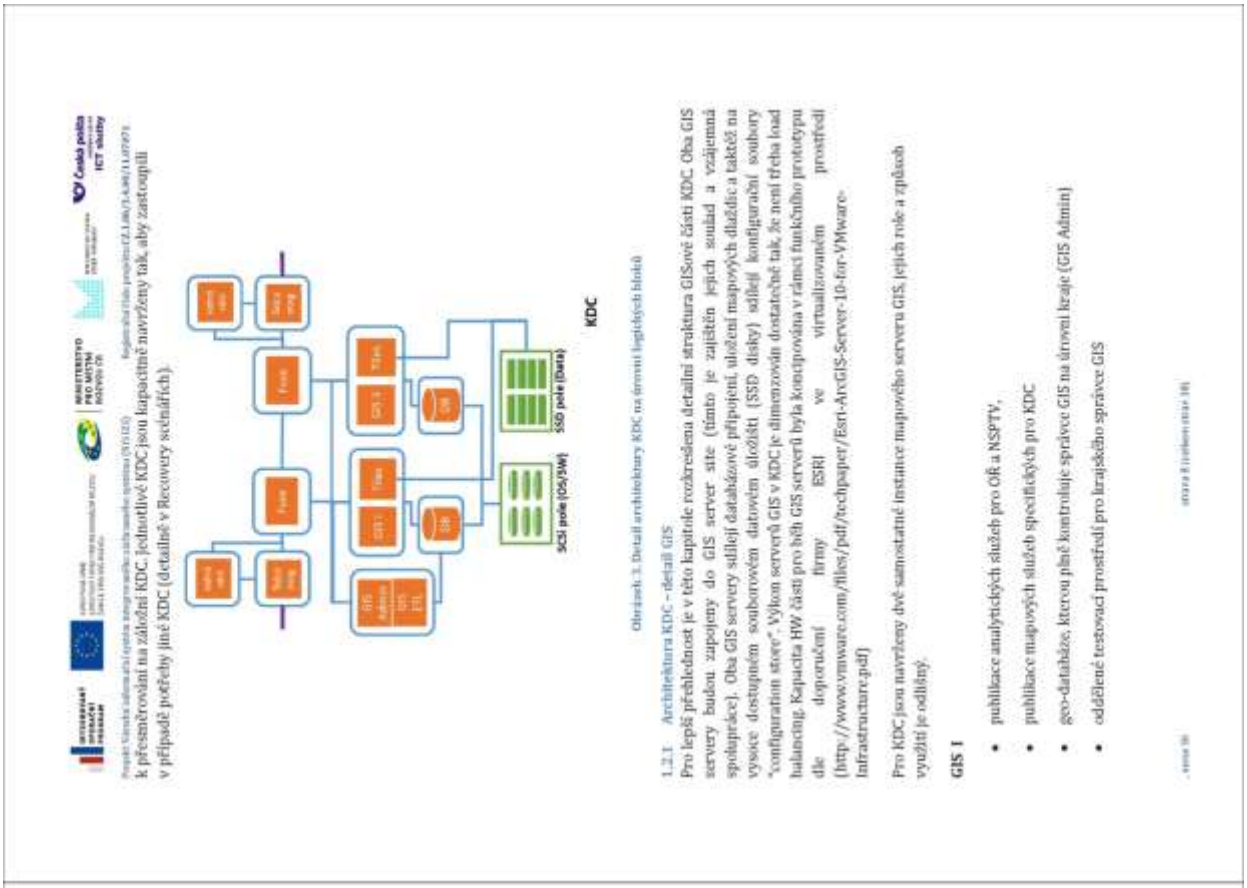
Obrázek 1. Detail architektury CDC na úrovni logických bloků

Rozdělení na dvě funkční větve v rámci CDC je zajištěno na úrovni balancingu a konfigurace aplikační logiky, které sama o sobě podporuje běh v clusteru.

Při nedostupnosti některé ze služeb CDC (tzn. pro výpadku dvojené funkcionality) je CDC do opravení výpadku odpojeno a jeho funkcionalita přechází další CDC. Dle typu výpadku je odstavení zajištěno kombinací automatizovaných procesů a dohledového centra (detailně v Recovery scénářích).

1.1.1 Architektura CDC – detail IPL

Druhou velkou částí SW řešení na CDC je samotná integrační platforma včetně podpůrného SW. Jádrem IPL části je komplexní řešení JBoss Fuse (detailně v kapitole IPL), které poskytuje směrování informací a poskytování služeb v rámci NIS IZS. IPL CDC poskytuje operátorské aplikace NSPTV přístup k informacím událostech. V prvním kroku se na CDC řeší autentizace a autorizace uživatelů v rámci IDM (Microsoft Active Directory). IDM řešení je zapojeno v clusteru tak, aby byli dostupné jednotné informace v rámci všech CDC.



Projekt Národní informační systém integrované záchranné služby – fázi pravidla systému (NIS IZS)

Dokumentace k fázi projektu CZ.1.06/3.4.00/11.07971

k přesměrování na záložní KDC. Jednotlivé KDC jsou kapacitně navrženy tak, aby zastoupili v případě potřeby jiné KDC (detailně v Recovery scénářích).

Obrázek 3. Detail architektury KDC na úrovni logických bloků

KDC

SCSI pole (OS/SW)

SSD pole (Data)

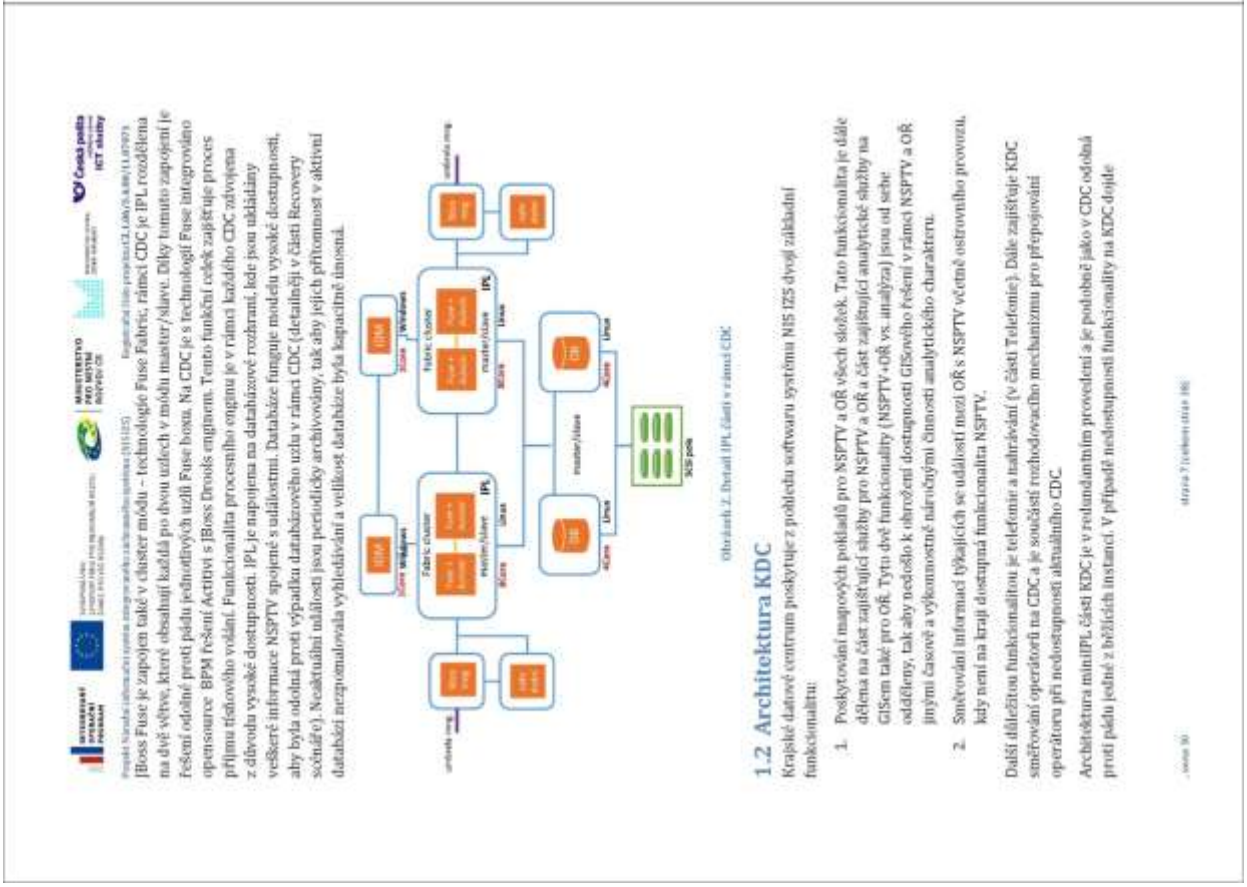
1.2.1 Architektura KDC – detail GIS

Pro lepší přehlednost je v této kapitole rozkreslena detailní struktura GISové části KDC. Oba GIS servery budou zapojeny do GIS server site (tímto je zajištěn jejich soulad a vzájemná spolupráce). Oba GIS servery sdílejí databázové připojení, uložení mapových dlaždic a taktéž na vysoce dostupném souborovém datovém úložišti (SSD disky) sdílejí konfigurační soubory "configuration store". Výkon serverů GIS v KDC je dimenzován dostatečně tak, že není třeba load balancing. Kapacita HW části pro běh GIS serverů byla koncipována v rámci funkčního prototypu dle doporučení firmy ESRI ve virtualizovaném prostředí (http://www.vmware.com/files/pdf/techpaper/Esri-ArcGIS-Server-10-for-VMware-Infrastructure.pdf)

Pro KDC jsou navrženy dvě samostatné instance mapového serveru GIS, jejich role a způsob využití je odlišný.

GIS 1

- publikace analytických služeb pro OŘ a NSPTV,
- publikace mapových služeb specifických pro KDC
- geo-databáze, kterou plně kontroluje správce GIS na úrovni kraje (GIS Admin)
- oddělené testovací prostředí pro krajského správce GIS



Projekt Národní informační systém integrované záchranné služby – fázi pravidla systému (NIS IZS)

Dokumentace k fázi projektu CZ.1.06/3.4.00/11.07971

JBoss Fuse je zapojen také v cluster módu - technologie Fuse Fabric, rámci CDC je IPL rozdělena na dvě větve, které obsahují každá po dvou uzlech v módu master/slave. Díky tomuto zapojení je řešení odolné proti pádu jednotlivých uzlů Fuse boxu. Na CDC je s technologií Fuse integrováno opensource BPM řešení Activiti s JBoss Drools enginem. Tento funkční celek zajišťuje proces příjmu tísňového volání. Funkcionalita procesního enginu je v rámci každého CDC závislá z důvodu vysoké dostupnosti. IPL je napojena na databázové rozhraní, kde jsou ukládány veškeré informace NSPTV spojené s událostmi. Databáze funguje modelu vysoké dostupnosti, aby byla odolná proti výpadku databázového uzlu v rámci CDC (detailněji v části Recovery scénáře). Neaktuální události jsou periodicky archivovány, tak aby jejich přítomnost v aktivní databázi nezpomalovala vyhledávání a velikost databáze byla kapacitně únosná.

Fabric cluster

master/slave

IPL

SSD pole

Obrázek 2. Detail IPL části v rámci CDC

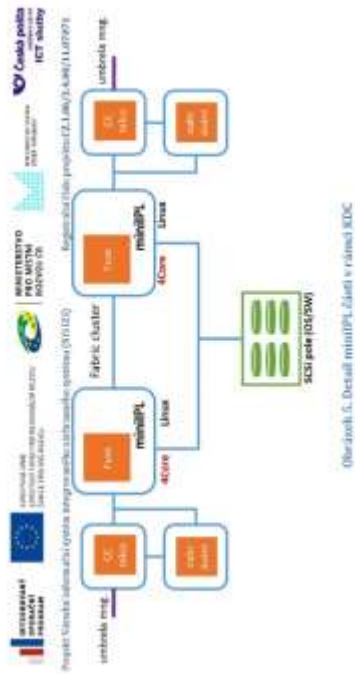
1.2 Architektura KDC

Krajské datové centrum poskytuje z pohledu softwaru systému NIS IZS dvojí základní funkcionalitu:

1. Poskytování mapových podkladů pro NSPTV a OŘ všech složek. Tato funkcionalita je dále dělena na část zajišťující služby pro NSPTV a OŘ a část zajišťující analytické služby na GISem také pro OŘ. Tyto dvě funkcionality (NSPTV+OŘ vs. analýza) jsou od sebe odděleny, tak aby nedošlo k ohrožení dostupnosti GISového řešení v rámci NSPTV a OŘ jinými časově a výkonnostně náročnými činnosti analytického charakteru.
2. Směrování informací týkajících se událostí mezi OŘ s NSPTV včetně ostrovního provozu, kdy není na kraji dostupná funkcionalita NSPTV.

Další důležitou funkcionalitou je telefonie a náhrávání (v části Telefonie). Dále zajišťuje KDC směrování operátorů na CDC a je součástí rozhodovacího mechanizmu pro přepojování operátoru při nedostupnosti aktuálního CDC.

Architektura miniIPL části KDC je v redundantním provedení a je podobně jako v CDC odolná proti pádu jedné z běžících instancí. V případě nedostupnosti funkcionality na KDC dojde



Obrázek 4. Detail GISové části v rámci KDC

1.2.2 Architektura KDC – detail miniIPL

Jádro miniIPL na KDC tvoří opět Fuse Fabric cluster, který zabezpečuje vysokou dostupnost řešení. Obecně se miniIPL v KDC liší od IPL v CDC tím, že miniIPL neobsahuje procesní engine a není napojena přímo na databázi událostí. Technologicky staví na stejném nástroji: JBoss Fuse, který je nakonfigurován na jinou funkcionalitu KDC.

MiniIPL na KDC komunikuje s telefonní ústřednou a umožňuje propojení hovoru a aplikace NSPTV operátorů. MiniIPL zpracovává požadavky na přihlášení jednotlivých operátorů, respektive vybírá CDC, na které se operátoři hlásí. Pro výběr je použitý jednoduchý algoritmus Round Robin (http://en.wikipedia.org/wiki/Round-robin_scheduling). Tímto mechanizmem, je zaručeno, že operátoři dané složky v daném kraji nejsou v jeden okamžik připojeni na stejné CDC a snižuje se tím dopad případného výpadku konkrétního CDC na zabezpečení funkcionality příjmu tísňového volání v daném kraji.

MiniIPL také publikuje služby NSPTV jako pro příjem tísňového volání, tak pro OŘ. Stejně tak miniIPL, slouží jako komunikační gateway mezi systémy NIS a KSP. Datové věty jsou směrovány přes miniIPL na KDC. Funkcionalita KDC je zastupitelná jiným KDC. Aplikace OŘ mohou v případě nedostupnosti mateřského KDC použít jiné KDC pro doručení datových vět na CDC.

Obrázek 5. Detail miniIPL části v rámci KDC

Legenda

- Oranžové jsou na obrázku zobrazeny jednotlivé SW řešení
- Modře jsou zobrazeny logické celky na úrovni virtualizovaných operačních systémů. Modré propojuje reprezentují komunikaci mezi jednotlivými systémy.
- Zeleně jsou zobrazeny HW segmenty, které jsou důležité z pohledu komunikace mezi softwarovými celky
- Fialová a žlutá znázorňují komunikace uvnitř

1.3 Schéma komunikace

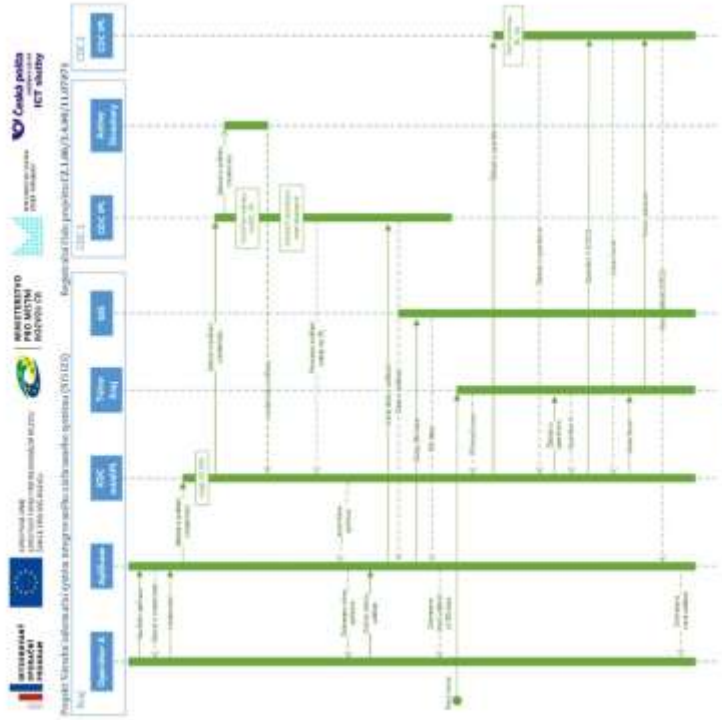
Obrázek 6 znázorňuje komunikaci mezi CDC, KDC a OŘ v rámci jednoho kraje na úrovni protokolů.

Do KCD jsou připojeny tísňové linky z VTS, v případě nedostupnosti ITS v ostrovním režimu jsou linky směrovány z KDC na jednotlivé OS v kraji. Telefonie je zapojena do clusteru a v rámci telefonního řízení (umbrella management) jsou vymiňovány informace telefonií v krajích do centra. Telefonní část ovládá pomocí CTI telefony jednotlivých operátorů NSPTV. MiniIPL pomocí technologie observerva komunikuje s ústřednou na KDC a zjišťuje existenci příchozích hovorů. Problematika telefonie je detailně zpracována v samostatném dokumentu PK.

GISová část KDC komunikuje na úrovni REST protokolu s pracovišti OŘ (operační řízení a analytické úlohy, včetně administrace). Operátoři NSPTV a dispečeři OŘ jsou připojeni ke GISové části v KDC. Odkaz na GISové služby získají při přihlášení.

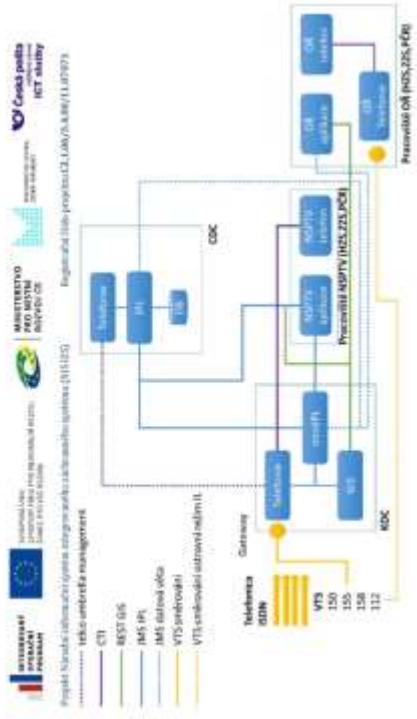
Aplikace NSPTV komunikuje iniciálně s miniIPL a dostává tak pokyn, ke kterému CDC se má připojit. MiniIPL dává informaci aplikaci NSPTV o stavu sítě a rozhoduje o chování v nestandardních situacích. Dále miniIPL zprostředkovává komunikaci mezi CDC a OŘ pro přenos datové věty.

V případě, že dojde k běhu systému v ostrovním režimu, tak miniIPL zajišťuje komunikaci s relevantními složkami OŘ v rámci daného kraje. Po obnovení normální stavu zajišťuje miniIPL synchronizaci uložených informací o událostech při ostrovním režimu do centrální databáze v CDC. Navržený protokol pro přenos datových vět je messaging, konkrétně standard JSR 914 (http://jcp.org/en/jsr/detail?id=914).



Obrázek 7. Přijmání operátora

Níže uvedený sekvenční diagram konferenčního hovoru (Obrázek 8) zobrazuje jednotlivé zprávy, které si mezi sebou vyměňují účastníci komunikace při vytváření konferenčního hovoru. Z důvodu přehlednosti je zde zjednodušeně navázání spojení mezi ústřednou a operátorem. Problematika příjmu hovoru je detailněji popsána na následujícím sekvenčním diagramu.



Obrázek 8. Schéma komunikace v rámci NIS a ISIP

Sekvenční diagram příjmu nové události (Obrázek 7) začíná přihlášením operátora k aplikaci, která jeho identitu ověří v centrálně vedené správě identit. Následně obdrží data o přihlášených operátorech a otevřených událostech a dalších přehledech dostupných na 3 okně aplikace. Sekvenční diagram končí přiřazením nové události operátorovi.

Zdrojové kódy jsou komentovány a prolinkovány s funkčními i systémovými požadavky dle specifikace. Jednotlivé nasazované verze jsou tagovány, aby bylo možné sledovat přidanou funkcionalitu mezi verzemi.

1.4.1.3 YouTrack (http://jetbrains.com/youtrack/)

YouTrack je systém pro správu projektu, řízení vývoje a změnových požadavků. V systému je plánována práce podle iterací a požadavků ze strany zákazníka. YouTrack zároveň podporuje integraci s GitHubem, takže je možné sledovat změny v kódu přímo v založené události/chybě.

1.4.1.4 TeamCity (http://jetbrains.com/teamcity/)

TeamCity je serverem průběžné integrace (angl. Continuous Integration), který zajišťuje spouštění buildu po každé změně kódu v GitHubu. Po úspěšném buildu je taktéž spuštěna sada jednotkových testů, které ověřují správnou funkčnost jednotlivých komponent v systému NIS IZS. TeamCity taktéž podporuje statickou analýzu kódu a tedy nejen předchází chybovosti aplikace, ale i analyzovat případné budoucí problémy, které neodhalí jednotkové testy. V případě označení verze jako stabilní je verze přidána do repozitáře pro nasazení v testovacím/produkčním prostředí.

1.4.1.5 Nexus (http://sonatype.org/nexus/)

Nexus server je repozitář buildů vytvořených během vývojového cyklu a označených jako stabilní verze.

1.4.1.6 Maven (http://maven.apache.org/)

Aplikace pro správu závislostí externích komponent a tvoření jednotlivých buildů. Maven je používán v TeamCity pro vytvoření buildu, ale i na vývojářských stanicích pro vytvoření experimentálních verzí. Verze označená jako stabilní je pomocí Mavenu přidávána do centrálního repozitáře Nexus.

1.5 Testovací a ověřovací platforma

Testovací a ověřovací platforma bude sdílena a bude řešena virtualizací kopie stávající infrastruktury CDC a vybraných KDC. Tím dosáhneme téměř identické infrastruktury, která je předpokladem k přednímu provozu.

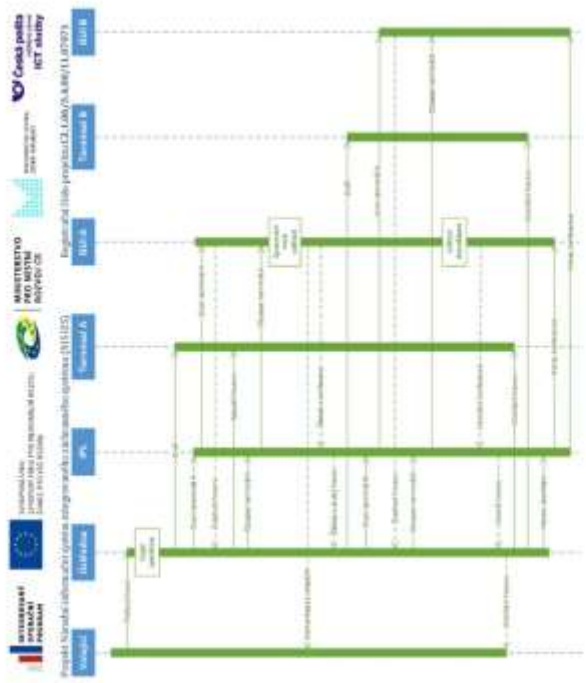
Testováním a následným ověřovacím provozem musí projít všechny updaty aplikace NSPTV stejně jako serverové části na CDC i KDC.

1.6 Školící platforma

Školící platforma bude provozována v odděleném virtualizovaném prostředí. Všechny události pro operátory budou simulovány. Budou vytvořeny simulace pro všechny čtyři druhy školení: operátoři, supervizoři, vedoucí složky a vedoucí IZS.

1.7 Datová věta

Datová věta slouží k obousměrné výměně dat mezi NSPTV a krajskými OŘ všech tří zúčastněných složek. Její struktura je definována pomocí XML Schema Definition (XSD) formátu, viz příloha (NSIZS_PKv50_CAST_B_SW_veta_ornew.xsd). Pomocí datové věty jsme schopni zasílat nové události i updaty událostí. Z OŘ do NSPTV směřují informace o stavech výjezdů k jednotlivým událostem a operační situaci včetně nových událostí. Dále se datovou větou



Obrázek 11. Konference dvou operátorů

1.4 Vývojová platforma

Pro vývoj řešení byť použity nástroje, které zajišťují kontinuální uchování informací o vývoje sw. Tato řešení zamezují ztrátě informací a umožňují efektivní rozvoj řešení, jednotlivé zadání je formalizováno do podoby „ticketů", které jsou následně zpracovány vývojovým týmem. Výsledky vývoje jsou uloženy v systému na správu zdrojového kódu a jsou provázány se zadáním.

1.4.1 Technologie podporující vývoj

Během vývoje je využito několika nástrojů podporujících vyšší kvalitu doručeného software, které pokrývají celý životní cyklus vývoje.

1.4.1.1 Java (http://java.oracle.com/)

Pro běh aplikace NIS IZZ je využívána Java ve verzi 7. Pro vývoj i nasazení je využívána distribuce JVM od společnosti Oracle (dříve Sun), která zastřešuje celou Java platformu.

1.4.1.2 GIT (http://github.com/)

Git slouží ke správě zdrojových kódů, ale i k verzování libovolného jiného typu dokumentů. Pro hostování zdrojových kódů NIS IZZ je zvoleno cloudové řešení github.com, které je široce využívané jak opensource komunitou pro veřejné projekty, tak i komerční sférou pro projekty soukromé. NIS IZZ je druhým příkladem.

přenášení informace o stavech SaP – informace o stavu SaP se neukládají do databáze, pouze se zobrazují.

Technologicky bude komunikace realizována formou zasílání asynchronních zpráv do front hostovaných buckendovou částí aplikace. Na straně NSPTV to bude IPL, na straně OŘ je tato funkcionalita součástí KSP projektů a model komunikace bude součástí další fáze projektu. Výhoda frontované asynchronní komunikace je její robustnost a snadná implementace v případě, kdy se liší příjemci na základě obsahu zpráv (různá OŘ podle nastavené souřadnosti). Robustnost řešení využívá rozdílné náročnosti zpracování jedné zprávy ve prospěch asynchronní komunikace z důvodů absence okamžitého zpracování a odpovědi.

Každá zpráva bude korelována s událostí pomocí jejího UUID (http://en.wikipedia.org/wiki/Universally_unique_identifier).

1.8 Datový Model

Grafické zobrazení datového modelu je uvedeno v příloze. V průběhu tohoto projektu a následného provozu bude udržován a aktualizován.

V rámci této kapitoly následuje popis datového modelu, integritních kritérií a výtah hlavních entit modelu.

Kompletní datové modely IPL a GISu jsou součástí přílohy v čitelné podobě. (NISIZS_Provadeci_koncept_CAST_B_SW_verze_50_IPL_ERD.pdf, NISIZS_Provadeci_koncept_CAST_B_SW_verze_50_GIS_ERD.png)

1.8.1 Metadata popisu datového modelu

V rámci deskripce datového modelu byla pro popis tabulek použita následující jmenná konvence:

- prefix TD - datová tabulka
- prefix TC - tabulka číselníku
- prefix TDH - historizační tabulka datové tabulky

Ústředními tabulkami modelu jsou TD_UDALOST, TD_MISTO a TD_HOVOR_OBCAN. Obsah těchto tabulek je zřejmý z přiloženého datového modelu. Pro lepší čitelnost níže přikládáme detailní popis k tabulkám a názvovým číselníkům, které vybočují z průměru a mohly by tedy být bez popisu složité:

- Tabulka TD_UDALOST, na kterou jsou navázány tabulky číselníků definující atributy Události:
  - TC_STAV_UD
  - TC_STAV_SLOZKY
  - TC_HZS_TYP_UD
  - TC_ZZS_TYP_UD
  - TC_NEODKLADNOST_UD
  - TC_PCR_TYP_UD
  - TC_TYP_UD
  - TC_ZAVAZNOST_UD
- Číselník TC_STAV_SLOZKY slouží k definici tzv. agregovaných stavů celých složek IZS. Například agregovaný stav celé složky HZS je "poslední jednotka opustila místo" ve chvíli, kdy poslední zúčastněné OŘ HZS zaslalo status o opuštění Místa události.
- Tabulka TD_UDALOST je navázána vazbou 1:N na tabulku TD_MISTO, jelikož Míst události může být definováno více.
- Tabulka TD_HOVOR_OBCAN je na tabulku TD_UDALOST navázána přes vazební tabulku TD_HOVOR_UDALOSTI, do které se kromě jiného zapisuje identita Operátora NSPTV, který hovor k dané události přiřadil.
- Na tabulku TD_HOVOR_OBCAN jsou navázány tabulky číselníků definující atributy Hovoru občana:
  - TC_VOLANE_CISL
  - TC_SIT_VOLAJICIHO
  - TD_MISTO, kde je uložena strukturovaná poloha volajícího občana
- TC_TYP_HOVORU je na TD_HOVOR_OBCAN navázáno přes vazební tabulku TD_TYP_HOVORU, kde se kromě jiného zapisuje identita "subjektu", který tento typ určil. Subjektem může být buď Operátor NSPTV (v případě, že hovor byl spojen na operátora a ten určil jeho typ), nebo samotná IPL (v případě, že hovor nebyl spojen na Operátora NSPTV - Whitelist, Blacklist). V tabulce TD_TYP_HOVORU je pak zapsán celý životní cyklus odbavení Hovoru občana (např. IPL nejprve vyhodnotila příchozí hovor jako "blacklist s upozorněním" - tedy upozornila Operátora NSPTV, že volající byl v definované minulosti označen za zlomyslného volajícího, a po té byl Operátorem NSPTV tentýž hovor označen např. "hovor nové události").
- Do tabulky TD_ZLOMYSL_HOVOR se duplicitně zapisují informace o Zlomyslných hovorech (v tabulce TD_TYP_HOVORU je totiž informace). Tabulka TD_ZLOMYSL_HOVOR však tyto informace uchovává pouze po dobu, po kterou se na tato data může dotazovat Engine pravidel a vyhodnocovat z nich pravidla blacklistování a blacklistování s upozorněním.
- Tabulka TD_HOVOR_OPERATOR slouží k záznamům hovorů Operátorů NSPTV, včetně hovorů Operátor-Operátor. Navázaný číselník TC_UKONCENI_HOVORU slouží k definici atributu id_ukonceni_hovoru, kterým je zaznamenáno, v jaké situaci a který účastník ukončil hovor, nebo opustil konferenci. Tabulka TD_VYZADANE_ZNALOSTI pak zaznamenává, jaké znalosti si Operátor NSPTV vyžádal, pokud žádal operátora se specifickými znalostmi (vhodné pro vyhodnocování, plánování rozšiřování Fad Operátorů a plánování vzdělávání).
- Tabulky TD_POZNAMKA_UDALOST a TD_POZNAMKA_HOVOR_OBCAN slouží k zápisu Poznámky. Do tabulky TD_POZNAMKA_UDALOST se zapisují Poznámky

vedené k Událostí a do tabulky TD_POZNAMKA_HOVOR_OBCAN se zapisují poznámky k hovorům, na jejichž základě nebyla založena Událost.

- Tabulka TD_UCAST_SLOZEK slouží k záznamům stavů účasti na Události jednotlivých Operačních řízení všech složek. Z těchto stavů je pak dovozován agregovaný stav celé služby IZS (Číselník TC_STAV_SLOZKY).

1.9 Integritní kritéria

Integritní kritéria jsou definována datovým modelem uvedeným v příloze a jejich dodržování zaručuje DB server svými vlastnostmi (Aktivní referenční integrita).

- DB server neumožní zápis řádku, který nemá úplný primární klíč, ani zápis řádku s primárním klíčem, který je již v téže tabulce použit u jiného řádku (Entitní integritní omezení).
- DB neumožní zápis hodnoty jiného datového typu, než je pro atribut definován (Doménové integritní omezení).
- DB server hlídá Referenční integritní omezení a nedovolí zápis hodnoty cizího klíče, pokud neexistuje jeho hodnota v roli primárního klíče v tabulce, na kterou tento cizí klíč odkazuje.

Pro primární a cizí klíče jsou použita tato označení:

- PK - primární klíč
- FK - cizí klíč
- pfK - cizí klíč sloužící jako součást složeného primárního klíče

2 Technické řešení SW komponent

2.1 NSPTV aplikace

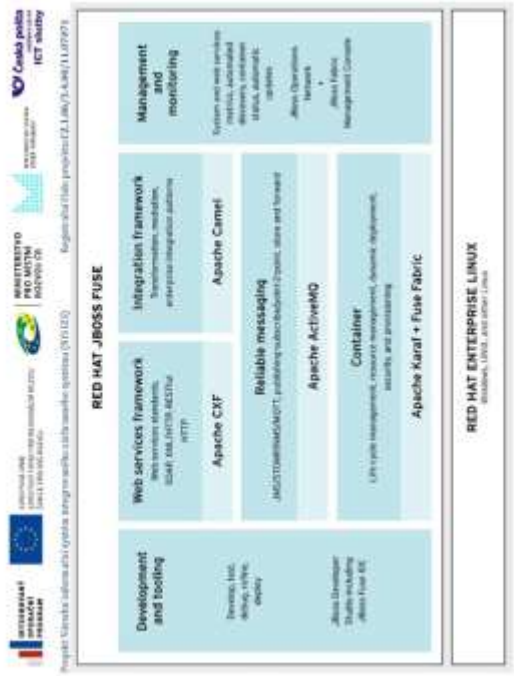
NSPTV aplikace bude tvořena třemi hlavními okny normalizovanými na rozhraní zobrazovacího zařízení 1920:1200. První okno představuje formulář pro vyplnění údajů získaných při vytěžování hovoru, druhé okno je tvořeno GIS mapovou komponentou a třetí okno obsahuje přehledy a stavy.

Všechny tři okna jsou tvořeny aplikací, která ke svému běhu vyžaduje Java Virtual Machine (JVM). Veškerá data jsou z aplikace odesílána do IPL, která zajišťuje distribuci aktualizace dat v rámci NSPTV a OR.

Každý operátor má své unikátní číslo v rámci NSPTV, aplikace zajistí, že po přihlášení operátora do aplikace NSPTV je operátor automaticky spřažen s terminálem u daného pracoviště a není potřeba se zvlášť hlásit k telefonnímu terminálu.

První okno aplikace je složeno z pěti hlavních grafických komponent. První komponentou je lišta záložek, ve které jsou řazeny otevřené události. Druhá komponenta obsahuje rozdělení příchozích hovorů do kategorií: Nová událost, informační hovor, zdvořilý hovor, předání výhradně pro jinou složku a FHQ. Třetí komponenta obsahuje samotný formulář, pomocí něhož jsou vytěžená data o hovoru zaznamenána a liší se podle kategorie příchozího hovoru. Čtvrtou komponentou je lišta záložek, ve které jsou řazeny otevřené události. Druhá komponenta obsahuje rozdělení příchozích hovorů do kategorií: Nová událost, informační hovor, zdvořilý hovor, předání výhradně pro jinou složku a FHQ. Třetí komponenta obsahuje samotný formulář, pomocí něhož jsou vytěžená data o hovoru zaznamenána a liší se podle kategorie příchozího hovoru. Čtvrtou komponentou je

Podpis/signature:……



Funkční komponenty JBoss Fuse jsou:

- **kontejner** – je základem JBoss Fuse. Tato komponenta je založena na Apache Karaf a dále rozšířena Fabric Managerem od konzoli, která zjednodušuje správu velkého množství distribuovaných kontejnerů
- **integrační framework** - tato vrstva je založena na Apache Camel a umožňuje využití velkého množství standardních metod a protokolů
- **framework pro webové služby** – umožňuje promítnit aplikaci ve službu a tedy zajistit její interoperabilitu s dalšími systémy a aplikacemi. Tato vrstva využívá Apache CXF
- **spolehlivé zprávy** - vrstva zajišťující asynchronní zpracování zpráv z ostatních systémů. Tato vrstva využívá Apache ActiveMQ
- **správa a monitoring** - správa prostředí nebo prostředí je podporována ve Fabric Management konzoli. Pro monitoring systému je možné využít JBoss Operations Network nebo jiné řešení

2.3.2 Failover

V rámci zajištění vysoké dostupnosti systému je každý uzel stínován v režimu (master-slave). Slave uzel čeká na nedostupnost mastera a v případě jeho výpadku přebírá veškeré jeho služby. Pro urychlení obnovení funkčnosti je slave uzel připraven v tzv. "hot" režimu, kdy jsou nastartovány všechny systémové služby a v případě přebírání funkčnosti se startují pouze služby aplikace IPL.

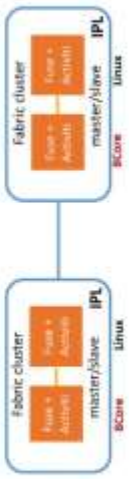
2.3.3 Balancing

Pro rozdělení zátěže je systém nasazen v clusteru (Fuse Fabric), který se stará o transparentnost celého systému. Konzistence jednotlivých uzlů je zajištěna pomocí algoritmu Quorum (http://en.wikipedia.org/wiki/Quorum_(distributed_computing))

2.3 Integrační platforma (IPL)

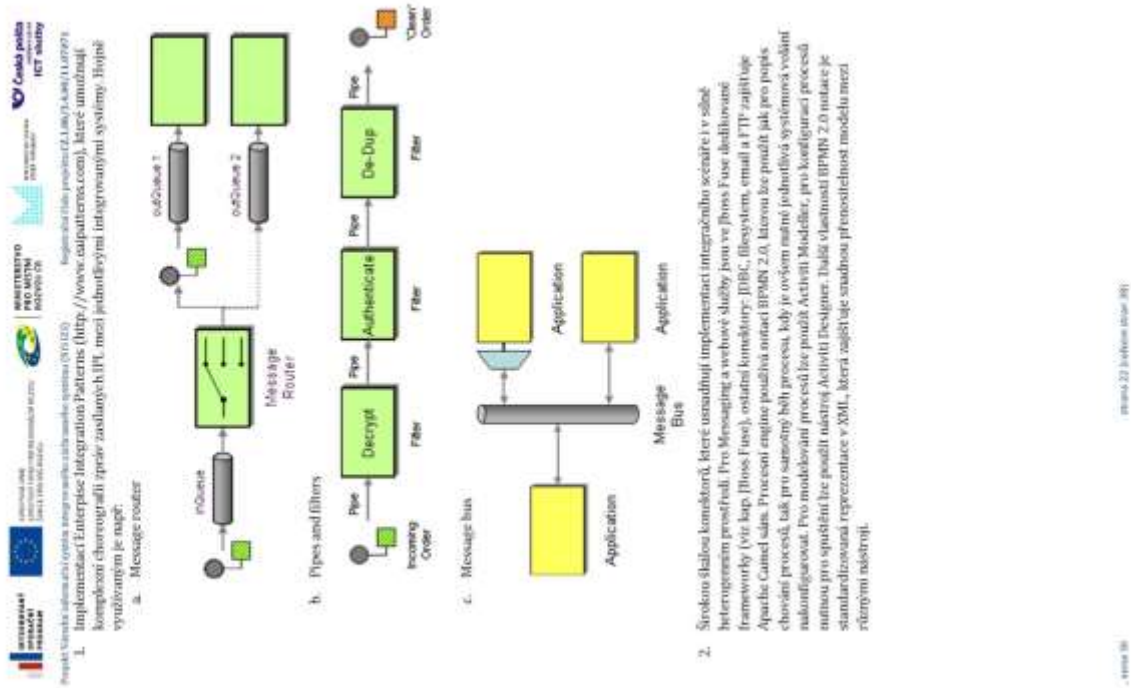
Systém IPL je srdcem celého projektu NIS IZS. Slouží jako zdroj dat pro klientské aplikace, mediátor krajských operačních řízení ucho pro správu telefonního subsystému. Dále zajišťuje perzistenci dat z NSPTV a operačního řízení. Dostupnost tohoto systému je kritická pro celkovou funkčnost NIS IZS.

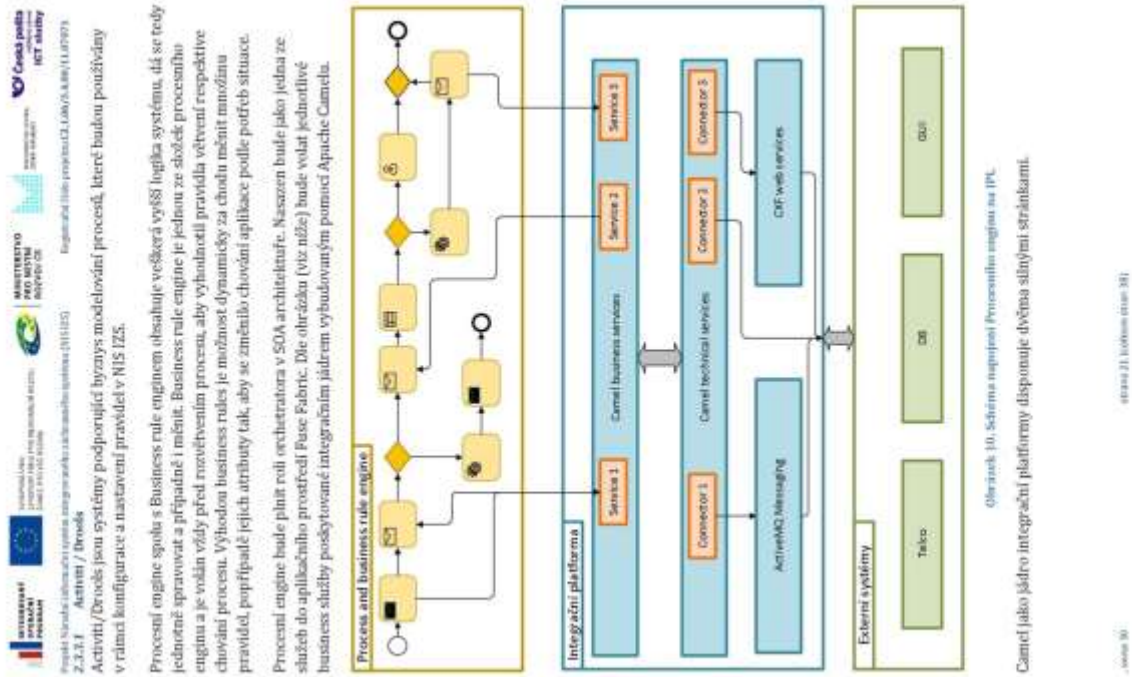
V každém datovém centru existují dvě instance IPL, které jsou navzájem nezávislé a tedy při kompletním výpadku (viz Failover) jedné z nich zůstává stále funkční jedna větev.
Ve standardním režimu se zátěž rozkládá mezi obě instance IPL (viz Balancing).



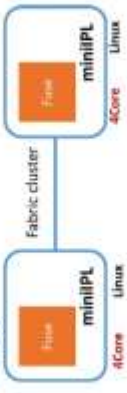
Obrázek 9. Detail IPL

2.3.1.1 JBoss Fuse (http://www.redhat.com/products/jbossenterprisemiddleware/fuse/)
JBoss Fuse je ESB (Enterprise Service Bus) implementace, která je využívaná v mnoha organizacích pro svoje vlastnosti jako je podpora clusteringu (cloudové řešení), jednoduchost konfigurace, nízká náročnost atd. JBoss Fuse integruje několik opensourcových technologií jako Apache Camel, Apache CXF, Apache Karaf, Apache ActiveMQ a další. Vývoj a podporu zastřešuje jedna z největších společností v IT sektoru společnost RedHat. Jedna její vývojová pobočka se nachází i v České republice, což dává záruku flexibilního řešení našich požadavků případně problémů.


Message Router
Pipe
Decrypt
Authenticate
De-Dup
Filter
Incoming Order
'Clean' Order
Application
Message Bus


Process and business rule engine
Integrační platforma
Externí systémy
Service 1
Service 2
Service 3
Connector 1
Connector 2
Connector 3
ActiveMQ Message
CXF web services
Telco
DB
GUI

2.4 MiniIPL na KDC



Obrázek 11. Detail miniIPL

V krajském datovém centru je taktéž nasazena IPL avšak ve standardním režimu funguje pouze jako mediátor do hlavních datových center. Až v případě nedostupnosti žádného centrálního datového centra přebírá plnohodnotnou funkcionalitu IPL a zajišťuje veškeré služby potřebné k provozu. K tunnelu směrování požadavků na CDC se používají definice ve frameworku Apache Camel. Rozřizování směrování požadavků lze nalézt v části dokumentu Schéma komunikace.

2.4.1 Odtrvení režim

V případě nedostupnosti CDC je provoz transparentně přesměrován na další CDC. V případě nedostupnosti všech CDC (až již výpadkem datového centra nebo veškeré konektivity do KDC) se KDC přepíná do tzv. „ostrovního" režimu. V něm IPL zabezpečuje komunikaci na úrovni kraje mezi jednotlivými operačními řízeními všech složek. Zajišťuje též vzájemnou komunikaci pro všechna operační řízení. V tomto režimu nejsou ostatní KDC informována o stavu jednotlivých operátorů ani řešených událostech, ale tento stav je viditelný pouze v rámci kraje. KDC se periodicky snaží obnovit spojení na CDC. Po obnovení spojení jsou stavy operátorů a řešené události synchronizovány do CDC a ostatní KDC. Systém se tak dostává do svého standardního režimu.

2.5 Komponenty pro centrální GIS v rámci NIS IZS

Centrální GIS na vstupu přebírá data externí (RUIAN, JSDI, ČHMÚ…) i složková. Pomocí automatizovaných nástrojů typu ETL udržuje v aktuálním stavu centrální databázi GIS. Tato databáze obsahuje prostorová i neprostorová data v optimalizovaném tvaru, kdy jsou některé vazby již přepočítány (materializované) tak aby lokalizace události byla co nejrychlejší a nejpřesnější. Tato optimalizaci provádějí (kromě samotné kontroly vstupních dat a vlastního importu) nástroje ETL.

Centrální GIS poskytuje služby pro NSPTV a slouží jako referenční geo-datová základna (C-GDB) pro krajské GIS (KDC). Do geo-databáze KDC je stav C-GDB průběžně přenášen pomocí aplikační one-way replikace pomocí technologie GIS. Složková geo-databáze je v rámci centrálního GIS buď udržovaná replikací geodatabáze složkového správce GIS (pro HZS je to pracoviště IOO Lázně Bohdaneč a pro PČR je to Oddělení krizového řízení PP) nebo nástroji správce GIS (GIS ADM). Také tato geodatabáze je replikována na všechna KDC. Složková data existují pro každou složku IZS separátně.

Na jednom CDC bude navíc k dispozici S-GDB (složková geo-datová základna) + GIS server vyhrazený pro potřeby PČR.

Obrázek 12. Schéma návrhu centrálního GIS a jeho komponent

2.5.1 Popis komponent centrálního GIS

- Základní GIS technologie
  - GIS SRV (4)
    - GIS server poskytující kromě dalšího
      - plnou implementaci GeoServices REST API
      - plnou implementaci OGC standardů WMS, WFS, WCS, WMTS
      - Administrátorské API (REST)
      - Databázové uložení prostorových dat (geodatabáze) nezávislé na konkrétním dodavateli DB (podporuje Oracle, MS SQL Server 2008, PostgreSQL)…
  - GIS ADM (6)
    - Administrátorské nástroje pro správu geodatabáze a GIS serveru na bázi výkonného desktop GIS nástroje
    - Požadavky
      - Plná integrace s technologií GIS server GIS server
      - Příprava map a jejich publikaci
      - Administrace služeb GIS server
  - Map cache
    - Obsahuje optimalizované mapové dlaždice s předpřipravenou základní mapovou kompozicí (společnou pro všechny složky) a optimalizované mapové dlaždice obsahující ortofotomapu

- C-GDB
  - Geodatabáze (vektorová data pro GIS) uložená v „enterprise relační databázi"
    - Základní vrstvy dle požadavků NSPTV a společných požadavků OÚ
    - Obsah registru RÚIAN optimalizovaný pro potřeby GIS, včetně reprezentace prostorových prvků
    - Vrstvy optimalizované pro vyhledávání, používané komponentou o MST Helper service
  - **Metainfo služby (5)**
    - Metainformační systém pro GIS
    - Funkčnost
      - Ukládá metadatových záznamů v souladu s platnou legislativou, směrnicí INSPIRE, Metadatovým profilem ČR a normami ISO 19115, ISO 19119 a ISO 19139
      - Rozhraní katalogové služby dle standardu OGC CSW 2.0.2
      - Webová aplikace pro evidenci metadat geografických dat a služeb založených na geoprávních datech
      - Umožňuje automatizovaný harvesting (zpracování změny dat v geodatabázi)
      - Je možné konfigurovat propojení s dalšími katalogy metadat (dle příslušných metadatových standardů)
- **Transformace dat - ETL**
  - **ETL (1)**
    - Konfigurovatelná Spatial ETL a geoprocessing technologie.
    - Požadavky funkčnost:
      - Automatizované transformační procesy, které zpracují vstupní data a provádí kontrolu a import dat do pracovní geodatabáze
      - Transformují data do schématu databáze místopisného helperu, dopočítají položky pro fulltext vyhledávání, prostorové vazby a indexy
      - Integrace s metainformačním systémem pro GIS
      - Řízené konfigurací (obsahuje nástroj pro přípravu ETL procesů), plně automatizované
      - Provádí logování činností a provádějících změn
  - **RÚIAN import (2)**
    - Importér dat RÚIAN ve formátu VFR (pro efektivní práci GIS je nutný přímý přístup do databáze obsahující vybrané prvky registru v podobě optimalizované pro použitou technologii)
    - Požadavky funkčnost
      - Aplikace umožňující ruční nebo automatizovaný, úplný nebo změnový import dat z registru územní identifikace, adres a nemovitostí (RÚIAN). Vytváří kompletní stav registru včetně reprezentace bodových liniových a plošných geometrií ve formě nativní a optimalizované geodatabáze pro „základní GIS technologii". Importuje a aktualizuje geometrie včetně ulic a stavebních objektů. Vytváří pohledy usnadňující práci s komplexním schématem databáze a zajišťuje podporu pro inteligentní fulltextové vyhledávání nad registrem.

- Služby pro místopisný helper
  - **MST Helper service (7)**
    - Konfigurovatelná služba pro vyhledávání v místopise a vyhledávacích vrstvách včetně administrátorského rozhraní
    - Požadavky funkčnost:
      - Umožňuje vyhledávání podle atributů a vazeb, podle úplného datového modelu RÚIAN
      - Přímá podpora práce s geodatabází, úzká vazba na datový model GIS
      - Vyspělé fulltextové vyhledávání
        - Podporuje prostorové omezování územní jednotkou nebo obecné geometrií
        - Podporuje synonyma, thesaurus, vyhledává na základě neúplných nebo i gramaticky nesprávných vstupů
      - Správcovské rozhraní pro údržbu synonym, výjimek a thesaurus, s možností konfigurace doplňujících vyhledávacích vrstev
      - Rozhraní SOAP, REST

Proces aktualizace dat je tvořen dvěma procesy.

1) Aktualizace místopisných dat z registru RÚIAN. Tento proces bude realizován pomocí komponenty RÚAIN import. Vstupní data (po primárním naplnění) budou přebírány a zpracovány jako každodenní přírůstky do geo-databáze. Součástí procesu bude také aktualizace odvozených tabulek používaných pro místopisné vyhledávání.

2) Aktualizace vrstev a vyhledávacích databází daty poskytovanými správcem GIS – IOO Lázně Bohdaneč. Toto proces bude realizován pomocí ETL nástroje, kde bude na základě konfigurace (skripty, modely, konfigurace) automatizovaně provádět kontrolu vstupních dat a provádět import do produkční geo-databáze CDC. Součástí procesu bude transformace dat do schématu databáze místopisného helperu, dopočítání položek pro fulltext vyhledávání, doplnění prostorových vazeb a indexů.

– Příprava specifických dat, mapových kompozic a služeb (správce KGIS bude mít v tomto široké možnost)

– Příprava specifických "vyhledávacích" vrstev a jejich registrace pro MST Helper service

– Předávání vybraných vrstev z místního geodatabáze správci složkového GIS ke kontrole a začlenění do složkové geodatabáze.

– Administrátor bude využívat plnou funkčnost vyspělého GIS desktop nástroje, doplněného o specifickou nadstavbu

Krajské služby GIS budou rozděleny do dvou skupin.

- Služby základní (mapové služby, mapové cache, vyhledávací služby) – GIS server I.
- Služby analytické (routování, ...) – GIS server II.

Aby nebylo možné provozem analytických služeb výkonnostně ovlivnit poskytování základních služeb, budou analytické služby poskytovány samostatným serverem. Tento server zároveň může sloužit pro přípravu a ověřování dalších specifických služeb, které bude připravovat podle potřeb správce GIS.

V případě přetížení serveru se základními službami bude možné provést přepnutí GIS server II využívat jako zálohu GIS server I.

GIS server je možné s využitím komponenty GIS Web Adaptor integrovat s krajským webovým serverem (který je mimo rozsah NIS IZS) a tímto způsobem řešit nastavení oprávnění přístupu ke službám pro uživatele, přebírané z místního (krajského) Active Directory.

2.7 Databáze

Zvolené řešení je založené na PostgreSQL databázi rozšířené o replikační vrstvu. Replikační vrstva bude implementována s použitím technologie „Slony-I". Toto řešení bylo vybráno na základě referenčního testu několika technologií.

2.7.1 Replikace DB

Pro řešení replikací DB bylo zvoleno řešení založené na PostgreSQL databázi rozšířené o replikační vrstvu. Replikační vrstva bude implementována s použitím technologie xDB Replication Server v5.0 (nebo jiné s minimálně odpovídající 100% funkcionalitou a spolehlivostí) v režimu Multi-Master.

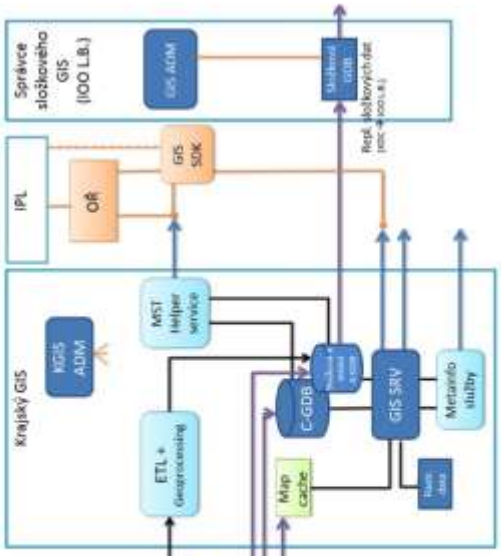
Zvolená koncepce systému plní především tyto požadavky:

- Multimaster db systém
- Plně nezávislý provoz databáze
- Datová synchronizace dat mezi jednotlivými nody
- Potenciálně replikace do jiných lokalit mimo hlavní datové centrum

Jednotlivé nody databáze jsou clustery, které pokrývají běžné výpadky HW.

2.6 Komponenty pro GIS v rámci KDC

V rámci KDC je GIS určen pro podporu OŘ všech základních složek IZS, společná geodata (centrální a složková) přebírá z centrálního GIS pomocí aplikační replikace. GIS v rámci KDC má zároveň možnost vytvářet vlastní (místní) geodatabázi a těmito daty a službami nad nimi postaveními řešit specifické potřeby OŘ každé složky IZS v daném kraji s využitím místně dosažitelných dat.



Obrázek 13. Schéma návrhu komponent GIS v rámci KDC

GIS v rámci KDC je budován ze stejných komponent jako centrální GIS, s některými odlišnostmi.

Na úrovni KDC pro GIS není navržena komponenta pro import dat z RUIAN, ani ISDI – tento import probíhá na úrovni CDC a změny jsou přenášeny replikačním mechanismem.

ETL nástroj umožní, podobně jako je to navženo pro CDC, automatizovat zpracování vstupních dat –vrstev (zde specifických pro konkrétní kraj). Administrátor GIS bude schopen pomocí ETL tyto činnosti popsat, automatizovat a zabezpečit kontrolami na správnou formu a obsah vstupních dat.

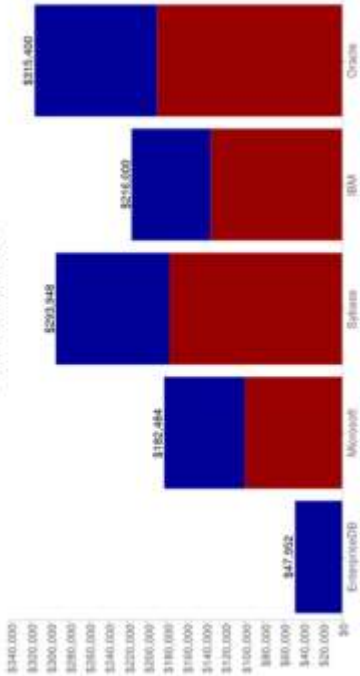
Nástroje pro administrátora (KGIS ADM) budou běžnější a určené pro aktivní práci správce krajského GIS.

Tato technologie je dostupná jako open source řešení, placená je podpora zvolené technologie.

Licenční pohled:

Replikační nadstavba dodávaná společností EnterpriseDB je poskytována bez základních licenčních poplatků. SW je distribuován pod dvěma různými licencemi. Komponenty, které nejsou produktem společnosti, spadají pod opensource licenci a jimi poskytované komponenty jsou distribuované pod „EnterpriseDB Limited Use License". Licence nebrání využívání řešení bez zakoupení podpory. V případě zakoupení SW podpory, je poté poskytována licence „EnterpriseDB Full Use License" a podle „Subscription Terms and Conditions".

Příklad srovnání nákladů pro jednotlivá databázová řešení pro vybranou konfiguraci:

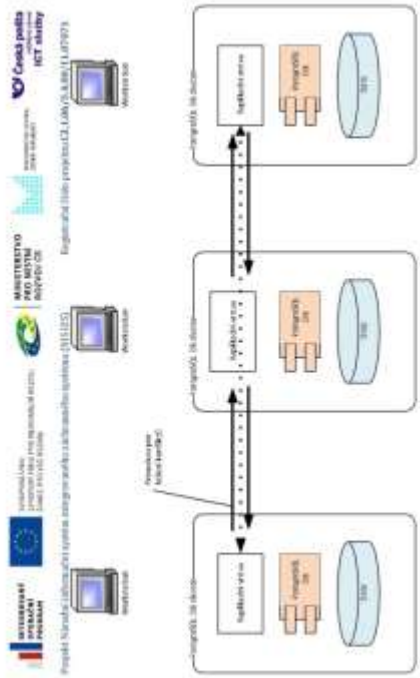


Obrázek 15. Porovnání nákladů na replikaci DB

2.7.2 Návrh lokálního fail-over řešení pro PostgreSQL databázi

Návrh řešení lokálního fail-over clusteru viz Obrázek 16. pro databázi PostgreSQL zohledňuje následující požadavky:

- Externí load balance se připojí na virtuální IP adresu služby v clusteru (VIP)
- Veškerý příchozí provoz musí být směrován na VIP tak aby bylo transparentně zajištěna dostupnost služby. Toto platí pro služby jako je datová replikace, kdy musí být zajištěno spojení na konkrétní cluster službu
- Databáze využívá failover mechanizmu pro řešení výpadku HW.
- Cluster služba musí zajistit přepnutí file systému, VIP IP adresy a jednotlivé služby (procesy) databáze a replikační vrstvy.



Obrázek 14. Replikační schéma

Technický detail řešení:

- Replikace probíhá mezi jednotlivými tabulkami
- Primární klíč slouží k identifikaci daných záznamů
- Pokud by nebylo možné zvolit unikátní klíč pro daný záznam, pak by nebylo možné zajistit párování záznamů mezi DB systémy
- Vytvoření procedury pro řešení konfliktů pro každou replikovanou tabulku

Datová izolace:

- Replikační vrstva provádí replikaci DBL operací z jednoho Master Definition Node.

Dopady na výkonnost databáze a odezvu:

Z důvodu požadavku na vysokou nezávislost jednotlivých databází, byl zvolen systém využívající asynchronní replikace. Toto řešení má výhodu, oproti synchronnímu, že odezva databáze na uživatelský požadavek není závislá na dalších nodech.

Nicméně replikační vrstva přidá dodatečnou zátěž systému:

- ukládání záznamu o replikaci (na úrovni dodatečného insertu)
- transportu dat do jiné databáze
- zpracování replikací z ostatních nodů

Recovery scénář:

Jednotlivé DB si ukládají seznam položek, které je nutné replikovat i stavovou informaci, které systémy již tyto data obdržely. V případě výpadku dojde k ukládání (těchto informací uvnitř DB a po obnovení spojení dojde k zahájení synchronizace mezi jednotlivými databázemi. Vzhledem ke zvolené technologii asynchronní replikace jsou jednotlivé uzly plně nezávislé.

Nákladová studie pro řešení založené na EnterpriseDB:

2.8.3 DBMS – Databáze
Specifikace: PostgreSQL verze 9
Forma licencování: BSD/MIT

2.8.4 BIRT - Business Intelligence and Reporting Tools
Specifikace: BIRT 4.3.0
Forma licencování: Eclipse

2.8.5 JBoss Fuse – IPL
Integrační platforma postavená na produktu JBoss Fuse.
Specifikace: Fuse
Forma licencování: Apache License Version 2.0

2.8.6 ACTIVITI - BPM systém
Procesní vrstva je postavena na Business Process Management (BPM) řešení Activiti (http://www.activiti.org/). Toto řešení umožňuje jak samotný proces namodelovat ve standardu BPMN 2.0 za pomocí nástroje Activiti Modeler, tak jej přímo z tohoto modelu spustit a propojit s dalšími komponentami řešení.
Specifikace: Activiti 5
Forma licencování: Apache License Version 2.0

2.8.7 DROOLS - BR systém
V rámci procesní vrstvy je začleněna z pohledu BPM stěžejní komponenta, kterou je Business Rule Engine. V navrženém řešení jsme zvolili produkt Drools (http://www.jboss.org/drools/). Business Rule Engine umožňuje za běhu měnit nastavení stěžejních rozhodovacích kroků v procesech dle nastavení systému.
Specifikace: Drools 5/6
Forma licencování: Apache License Version 2.0

2.8.8 MYBATIS - Objektové relační mapování
Aplikační vrstva je napojená na databázi pomocí Object-relational Mapping (ORM) na databázi, pro toto mapování, je využito řešení Mybatis (http://mybatis.github.io/mybatis-3/)
Specifikace: Mybatis verze 3
Forma licencování: Apache License Version 2.0

2.8.9 GISSRV - GIS server
Serverové řešení („GIS server") poskytující plnou implementaci GeoServices REST API (OGC Candidate), plnou implementaci OGC standardů WMS, WFS, WCS, administrátorské API (REST), databázové uložení prostorových dat (geodatabáze) nezávislé na konkrétním dodavateli DB (musí podporovat minimálně Oracle, MS SQL Server 2008 a Postgre SQL).
Počet licencí potřebných pro provoz: 2 pro 1 KDC (1 licence je na 4 fyzické CPU)
1 pro PČR
1 replikace v CDC

Obrázek 16. Model HA databázového sváu CDC

2.7.3 Návrh řešení geograficky konfigurace database
- Geografické řešení vysoké dostupnosti database je zajištěno plnou multi - master replikací dat mezi jednotlivými DB clustery
- Směrování provozu bude zajištěno pomocí load balance zařízení, které se zároveň zajišťuje směrování přicházejících hovorů operátora
- V případě nedostupnosti vybrané lokace, jsou data pro replikace ukládána v jednotlivých databázích a po obnovení spojení dojde k synchronizaci dat podle replikačního schématu

2.8 Licence

2.8.1 NSPTV a GIS klient NSPTV
Budou dodány jako multilicence vč. Majetkových autorských práv (viz kap. 07. Č. 9. Smlouvy o dílo na dodávku pro projekt NIS IZS).

2.8.2 OS – Operační systém
Budou pořízeny OS dvojího typu – pro servery po běh IPL, GIS, TEL a serverové části NSPTV. Konkrétní operační systém a počet licencí bude zřejmý po realizaci výběrového řízení.

Počet licencí potřebných pro provoz celkem: 30

2.8.10 GISADM – Administrátorský nástroj GIS

Administrátorské nástroje pro správu geodatabáze a GIS serveru s plnou integrací s technologií GIS serveru umožňující přípravu map a jejich publikaci a administrace služeb GIS Serveru.

Technologie vytvořená nad standardní funkčností „krabicového" desktop GIS nástroje v podobě aplikační nadstavby bude dodaná včetně zdrojových kódů a v licenčním modelu multilicence (viz čl. 2.8.1. tohoto dokumentu).

Počet licencí potřebných pro provoz: 1 pro 1 KDC
1 pro PČR

Počet licencí potřebných pro provoz celkem: 15

2.8.11 METAGIS - Metainformační systém pro GIS

Zajišťuje uložení metadatových záznamů v souladu s platnou legislativou, směrnicí INSPIRE, Metadatovým profilem ČR a normami ISO 19115, ISO 19119 a ISO 19139, poskytuje rozhraní katalogové služby dle standardu OGC CSW 2.0.2. Obsahuje webové aplikace pro evidenci metadat geografických dat a služeb založených na geografických datech. Umožňuje vytváření a ukládání, správu, vyhledávání, zobrazování, stahování a publikování metadat, podporuje vydávání dat. Zaručuje plnou integraci s GIS serverem. Umožňuje automatizovaný harvesting (zpracovává změny dat v geodatabázi). Je realizován technologií Java a jeho zdrojové kódy jsou bez licenčních omezení.

Počet licencí potřebných pro provoz:
server 1 pro neomezený počet uživatelů
klient(editor) 18 (pro KDC, PČR, testování a školení)

2.8.12 ETL - Transformace dat

Automatizované transformační procesy, které zpracují vstupní data a provádí kontrolu a import dat do pracovní geodatabáze, transformují data do schématu databáze místopisného helperu, dopočítají položky pro fulltext vyhledávání, prostorové vazby a indexy. Zaručuje plnou integraci s metainformačním systémem pro GIS. Má řízené konfigurací (obsahuje nástroj pro přípravu ETL procesů), plně automatizované. Je realizován v technologii Java a zdrojové kódy jsou bez licenčních omezení.

Specifikace: včetně zdrojových kódů

Počet licencí celkem: 1 pro neomezený počet uživatelů

2.8.13 VFR - RUIAN import

Importér dat RUIAN ve formátu VFR. Aplikace umožňuje ruční nebo automatizovaný, úplný nebo změnový import dat z registru územní identifikace, adres a nemovitostí (RUIAN). Vytváří kompletní stav registru včetně reprezentace bodových liniových a plošných geometrií ve formě geodatabáze nativní a optimalizované pro „základní GIS technologii". Importuje a aktualizuje geometrie včetně ulic a stavebních objektů. Vytváří pohledy usnadňující práci s komplexním schématem databáze a zajišťuje podporu pro inteligentní fulltextové vyhledávání nad registrem. Poskytuje uživatelské rozhraní pro „ruční aktualizaci" a zároveň umožňuje plně automatizovaný provoz. Má řízenou konfiguraci (konfigurace se připravuje pomocí uživatelského rozhraní), plně automatizované. Je realizován v technologii Java a zdrojové kódy jsou bez licenčních omezení.

Specifikace: včetně zdrojových kódů

Počet licencí celkem: 1 pro neomezený počet uživatelů

2.8.14 Mapové podklady

V rámci projektu je počítáno s nákupem multilicencí pro složky IZS, tak aby bylo umožněno tyto mapové podklady pro potřeby NSPTV a OŘ.

Jedná se o data sítě pozemních komunikací a bodů zájmu (POI)

2.8.15 JSDI - Příjem a zpracování DDR JSDI

Na serverové straně se udržuje stav JSDI (zpracovávají se přicházející updaty, dochází k expiraci událostí atd.). DDR JSDI je postaveno tak, že externí strana posílá informace konzumentovi (ne naopak). Na straně konzumenta musí být otevřené rozhraní (např. servlet) a potřebný port. Udržovaný stav JSDI (dopravní informace) je následně prostřednictvím „GIS server" publikován ve formě kterou může klient využívat už standardním způsobem (GeoServices REST API). Umožňuje plně automatizovaný provoz. Je realizován v technologii Java a zdrojové kódy jsou bez licenčních omezení.

Specifikace: včetně zdrojových kódů

Počet licencí celkem: 1 pro neomezený počet uživatelů

2.8.16 Souhrn licencí na GIS SW

	Typ licence	CDC active	CDC standby	KDC	celkem licencí
Server site					
GIS server (KDC)	Každá licence musí být poskytnuta pro jednu běžící instanci na virtualizovaném prostředí (tato instance musí být provozovatelná přes celou virtualizační farmu)			28	**28**
GIS server (PČR)		1	2		**1**
GIS server (replikace v CDC)		1	2		**1**
ETL RUIAN		1	2	0	**1**
ETL JSDI		1	2	0	**1**
Metadatový server		1	2	0	**1**
Client site					
Metadatový		1		14	**18**

Podpis/signature:.....

klient editor	licence bez omezení			
Metadatový klient prohlížeč				
GIS administrátor (jedna licence pro PCR)	1	14	15	

Tab.1. Licence požadované pro provoz GIS SW

2.9 Reporting

Reporting bude zastřešovat nástroj Eclipse BIRT (http://www.eclipse.org/birt/), který je složen ze dvou hlavních částí: Report designer, který slouží k navrhování reportů a report engine, který reporty generuje ze šablon z připojených dat. BIRT nabízí kromě vlastních standardních konektorů (Web services, XML, JDBC) také možnost psaní vlastních konektorů, čímž umožní zahrnout pod jeden reporting celé NIS-IZS a dále ten reporting rozvíjet s tím, jak se bude rozvíjet aplikace NIS-IZS. Nedílnou součástí reportovacího řešení je též transformace dat a logika jejich zpracování.

2.10 Reference na produkty

2.10.1 JBoss Fuse

Fuse ESB je založeno na běžně používaných standardech, čímž zajišťuje snadnou rozšiřitelnost či napojení na řešení třetích stran. Celý balík Fuse ESB je složen z několika rozšířených frameworků, které jsou základem funkční SOA architektury.

Sabre Holdings úspěšně nasadili jboss Fuse v roce 2013 aby čelil nárůstu pál milionu transakcí za den pomocí řešení, které je kompatibilní se servisně orientovanou architekturou.

2.10.2 Activiti

Activiti má téměř 10 letou historii (dříve jako jBPM) a patří k nejvyspělejším BPM enginům, jeho vyspělost dokládá i několik derivátů jako je stávající jBPM v5, Kamunda a Effektiv. Activiti má dlouhodobě silné vazby na Alfresco, které tento engine využívá ve svém ECM řešení pro workflow.

Momentálně není na trhu tak verzatilní engine jako Activiti, který lze programově ovládat. Většina dnešních řešení je zaobalena spousttou dalších nástrojů, které znesnadňují hlubší integraci s výše popsaným Fuse ESB.

2.10.3 PostgreSQL

PostgreSQL je objektově-relační databázový systém (ORDBMS). Vydáván je pod licencí typu MIT a tudíž se jedná o free a open source software. Společnost EnterpriseDB vyvíjí Postgres Plus což je plnohodnotná distribuce PostgreSQL, zahrnující mnoho contrib modulů a doplňkových komponent. Postgres Plus je dostupný ve dvou verzích: Postgres Plus Standard Server, který má všechny vlastnosti PostgreSQL, je dodatečné QA testování, obsahuje integrované komponenty, možnosti ladění a jednoduchou instalaci, a Postgres Plus Advanced Server, který kromě

Projekt Národní informační systém integrovaného záchranného systému (NIS IZS) | Registrační číslo projektu CZ.1.06/3.4.00/11.07971

vlastností produktu Postgres Standard Server navíc disponuje i kompatibilitou s Oracle, vlastnostmi pro zlepšení škálovatelnosti a nástroji pro DBA a vývojáře.

Referenční nasazení PostgreSQL:

- Yahoo - provozuje řešení pro analýzu chování uživatelů na webu, obsahuje dva petabyty dat
- MySpace - popularní sociální síť, používá Aster nCluster Database pro data warehousing, který je postavený na nemodifikované verzi PostgreSQL
- BASF - nákupní platforma pro jejich zemědělský portál
- Mezi další významné uživatele patří např. Cisco, Fujitsu nebo NTT Data.

2.11 Open source

Výhoda využití open source spočívá zejména v možnosti upravit funkcionalitu podle potřeby projektu díky dostupnému zdrojovému kódu. Komunita je schopna sebeposilujícím mechanizmem vytřídit nejúspěšnější projekty.

Open source model přináší i možnost rychlé opravy v produktu a i možnost backportování této opravy do starší verze produktu (menší riziko - není nutné přejít na novější verzi, u které může být odlišná funkcionalita).

Snížená pořizovací cena, při stejné kvalitní podpoře díky business partnerům, kteří nabízejí konzultace i hotová řešení využívající OSS. Díky komerční podpoře (placené služby) OSS produktů je poskytnutí podpora kvalitní srovnatelné s komerčními produkty (placená je licence i podpora).

Z pohledu bezpečnosti přináší open source model větší kontrolu nad případnými backdoory oproti proprietárnímu řešení, kdy je dodáván pouze binární kód.

2.12 Koncept provozu

2.12.1 Instalace serverové části

Předpokládáme nainstalovaný operační systém.

2.12.1.1 Postup instalace

- Získání aktuální verze jBoss Fuse z http://www.jboss.org/products/fuse
- Probíhse instalace dle https://access.redhat.com/site/documentation/en-US/JBoss_Fuse/6.0/html-single/Installation_Guide/index.html
- Následující kroky budou probíhat podle manuálu https://access.redhat.com/site/documentation/en-US/JBoss_Fuse/6.0/html-single/Configuring_and_Running_JBoss_Fuse/index.html
- Konfigurace a spuštění služby (kapitola 2)
- V případě že se jedná o první uzel, vytvoří se nový Fuse Fabric (kapitola 6)
- V opačném případě je uzel přidán do již existujícího Fuse Fabric (kapitola 7)
- Nasazení JPL systému a závislých komponent podle https://access.redhat.com/site/documentation/en-US/JBoss_Fuse/6.0/html-single/Deploying_into_the_Container/index.html

2.12.2 Instalace klientské aplikace

Instalace klientské aplikace bude realizována pomocí síťové instalace (tlustý klient i VDI server) prováděné standardními prostředky cílové platformy.

Na cílovém OS je nutné mít nainstalovánu Java JRE 1.7.0_45 nebo vyšší (Java Runtime Environment). Aplikace NSPTV se spouští zástupcem z plochy OS.

2.13 Aktualizace

2.13.1 Aktualizace serverové části

Aplikace nahraná v JBoss Fuse kontejneru je kontrolována Fabric agentem. Agent prozkoumává profily aplikované na kontejner, aby rozhodl, jaké verze aplikace má načíst. Update typicky obsahuje novou verzi jedné nebo více aplikací, proto je třeba upravit profil aplikovaný na tento kontejner. To způsobí načtení nové verze agentem. Doporučeným nástrojem pro update je využití Management console.

2.13.1.1 Postup aktualizace

- update (systémový nebo aplikační) je nahrán do maven repozitáře
- pomocí Management console je upraven profil verzí
- je zmigrován jeden nebo dva kontejnery pro ověření správné funkčnosti
- následně je zmigrován celý cluster

2.13.2 Aktualizace klientské aplikace

2.13.2.1 Aktualizace OS

Pro vzdálenou aktualizaci operačního systému klientské stanice a VDI budou využity standardní nástroje systému dle výsledku VŘ.

2.13.2.2 Aktualizace aplikace NSPTV

Pro instalaci nové verze aplikace je potřeba aktualizovat instalační složku s aplikací NSPTV novými soubory. Tento proces je nutné aplikovat pomocí standardního distribučního systému cílového systému dle výsledku VŘ.

2.14 Monitoring

2.14.1 Monitoring serverové části

JBoss Fuse nabízí pro správu a metriky svého použití přístup přes JMX (Java Management Extensions) lze tedy použít již existující aplikace (JConsole, MC4J), které lze pomocí pluginů rozšířit o vlastní pohledy, použít aplikaci Fuse HQ (komerční, monitoring včetně vlastního webového rozhraní), JBoss ON (JBoss Operations Network) nebo vytvořit vlastní monitorovací nástroj.

Bude se monitorovat aktuální stav jednotlivých kontejnerů, jejich vytížení a spotřeba prostředků.

2.14.2 Monitoring koncových pracovišť

Operátorské terminály se monitorují pomocí observerů definovaných v JTAPI. Aplikace NSPTV neustále monitoruje stavy všech terminálů a pracovišť, ke kterým jsou přihlášení operátoři. Zajišťuje tak, aby žádná nová událost nebyla směrována na pracoviště, kde není přihlášený operátor a telefon je schopen přijímat hovory.

Kromě indikace koncových pracovišť, které jsou schopny přijímat hovory, systém při každém přihlášení koncového pracoviště k IPL monitoruje aktuální verzi klienta.

2.15 Release a Incident Management

Nové verze a aktualizace aplikace NSPTV budou v předem oznámených intervalech za součinnosti zadavatele. Při nasazování nových verzí budou operátoři přihlášení z CDC, které je aktualizováno a další CDC. Po nasazení aktuální verze NSPTV na CDC bude CDC zapojeno do provozu a instalace proběhne analogicky na zbývajících CDC.

Při aktualizaci klientské části NSPTV budou operátoři postupně odstaveni, dle plánu aktualizace, od koncových pracovišť tak, aby nedošlo k obrození funkcionality příjmu tísňového volání. Aktualizace bude probíhat v dohodnutých časových intervalech se zadavatelem. Aktualizaci bude možné v případě rozhodnutí zadavatele přerušit a obnovit standardní provoz.

V případě výskytu chyby v aplikaci může operátor chybu zaznamenat do helpdeskového systému. Vedoucí pracoviště následně rozhodne o validaci požadavku na opravu a dle definovaného workflow dojde k opravení chyby a nasazení nové verze.

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

C. Síť

Dokument obsahuje:	Specifikaci dodávaného síťového řešení.
Verze:	5.1b
Schválil za Dodavatele:	RNDr. Vladimír Přibramský
Datum:	17/4/2014

Projekt Nováda informační systém integrovaného záchranného systému (NIS IZS) Registrační číslo projektu CZ.1.06/2.4.00/11.07707

Obsah

1 Cíle dokumentu ... 3
2 Požadavky na připojení k síti ITS (ITS NGN) ... 4
2.1 Harmonogram ... 4
2.2 Fyzické připojení lokalit CDC ... 5
2.3 Fyzické připojení lokalit KDC ... 7
2.4 Fyzické připojení lokalit NPSTV ... 10
3 Zapojení technologií NIS IZS ... 15
3.1 Zapojení CDC ... 16
3.2 Zapojení KDC ... 17
3.3 Zapojení NPSTV ... 19
3.3.1 Zapojení NPSTV HZS ... 19
3.3.2 Zapojení NSPTV ZZS ... 20
3.3.3 Zapojení NSPTV PČR ... 21
4 Použití VPN ... 22
5 Propojení s externími systémy ... 24
5.1 Připojení CDC/KDC k CMS (CMS 2.0) ... 24
6 Adresace ... 25
7 Specifikace dodávky síťové infrastruktury ... 32
7.1 Specifikace komponent CDC ... 32
7.1.1 CDC+KDC - CE směrovač ... 32
7.1.2 CDC - L2/L3 přepínač ... 36
7.1.3 CDC – load balancer ... 41
7.1.4 CDC - firewall ... 43
7.1.5 OOB - L2/L3 přepínač ... 45
7.2 Specifikace komponent KDC ... 48
7.2.1 KDC - CE směrovač ... 48
7.2.2 KDC - L2/L3 přepínač ... 53
7.3 Specifikace komponent NSPTV ... 56
7.3.1 NSPTV - CE směrovač pro ZZS ... 56
7.3.2 NSPTV - LAN přepínač ... 59
8 Seznam obrázků ... 63
9 Seznam tabulek ... 64

Podpis/signature:.....

1 Cíle dokumentu

Cílem tohoto dokumentu je

- popsat fyzická připojení lokalit, do kterých jsou dodávány technologie projektu NIS IZS
- definovat způsoby komunikace mezi jednotlivými systémovými prvky s odkazem na využití VPN pro složky IZS a jejich přístup ke službám v datových centrech NIS IZS
- popsat adresní plán k připojení všech potřebných systémových prvků NIS IZS a specifikovat požadavky na souběžný projekt ITS NGN, který má za cíl povýšit z hlediska přenosové kapacity a dostupnosti síťovou infrastrukturu propojující lokality složek IZS.

2 Požadavky na připojení k síti ITS (ITS NGN)

Síť ITS a její nástředovník ITS NGN je definována jako propojovací síť Ministerstva vnitra ČR. Pro projekt NIS IZS zajišťuje připojení jednotlivých složek IZS a jejich komětřivitu k datovým centrům a lokalitám NSPTV. Tento dokument neobsahuje informace o síti ITS NGN, jejíž dostavba je řešena samostatným projektem MV ČR, ale pouze definuje požadavky projektu NIS IZS na tuto přenosovou infrastrukturu.

Připojení k síti ITS NGN bude vždy realizováno na vazbě PE a CE vrstvy, kde bude pomocí dynamického směrovacího protokolu zajištěna rychlá konvergence sítě, automatická změna topologie sítě a volba optimální cesty mezi lokalitami NIS IZS. Propojení bude realizováno pomocí ethernetových rozhraní, na kterých bude možné předávat jednotlivé VPN složek IZS.

Výjimka v připojování bude tvořit připojení lokalit NSPTV HZS, které budou sdílet společnou síťovou infrastrukturu s KDC na úrovni CE směrovačů, ve dvou případech (Plzeň a Olomouc) bude využito jednotných CE směrovačů pro připojení technologií NPSTV, KDC i CDC. Sdílení CE směrovačů pro logické uzly systému NIS IZS, které spřovují ve shodných geografických lokalitách, nepřináší nová bezpečnostní rizika ani neomezuje propustnost systému, ale představuje efektivní vynaložení projektových prostředků s cílem minimalizovat budoucí náklady na provoz těchto technologií.

2.1 Harmonogram

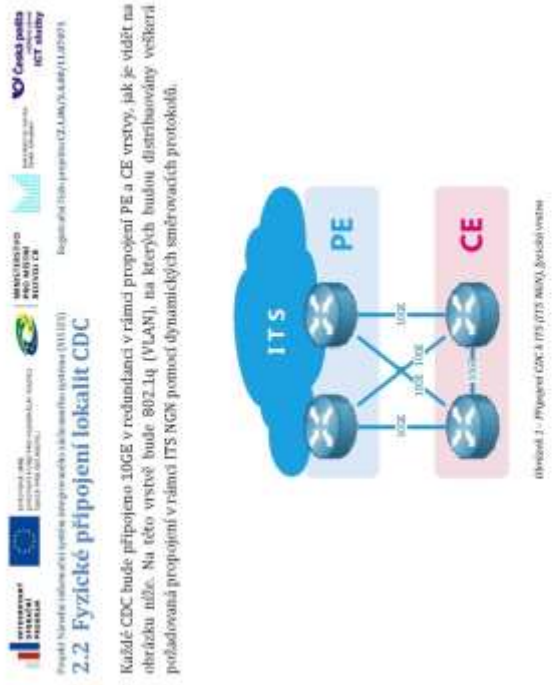
Požadavky na připojení jednotlivých CDC i KDC jsou rozděleny podle milníků, které odrážejí harmonogram projektu NIS IZS. Termíny a technické řešení propojení lokalit NIS IZS jsou v gesci projektu ITS NGN. Realizace ITS NGN je koordinována s NIS IZS a tato realizace odpovídá potřebám NIS IZS.

Fáze projektu NIS IZS	Datum zahájení
Pilotní testování	1.4.2014
Plošné testování	1.8.2014
Záčěžové testování	1.10.2014
Produkční provoz	28.2.2015

Tabulka 1 – Harmonogram jednotlivých připojení lokalit NIS IZS k síti ITS a ITS NGN

Bod připojení	Adresa	Stavba	Kraj	Šířka kanálu	Podporované APS (v kanálu kanálu)	Typ/Typ kanálu	Fixní kanál/ Dynamické kanálu	Fixní kanál/ Dynamické kanálu	Fixní kanál/ Dynamické kanálu	Fixní kanál/ Dynamické kanálu	Fixní kanál/ Dynamické kanálu	Fixní kanál/ Dynamické kanálu	Dostupnost	Fixní (Ano/Ne)	Fixní (Ano/Ne)	Max. Fixní Linka (%)
CDC 1	Praha, Olšanská 1	NIS	Praha	30 Mbps			Fixní kanál	5	/16	/16	/16	/16	Best effort	2	2	100 %
				360 Mbps			Fixní kanál	5	/16	/16	/16	/16	Best effort	2	2	100 %
				1,5 Gbps	10 Gbps		Dynamické kanálu	5	/16	/16	/16	/16	99,99 %	4	4	100 %
				1,5 Gbps	10 Gbps		Fixní kanál/ Dynamické kanálu	5	/16	/16	/16	/16	99,99 %	4	4	100 %
CDC 2	Plzeň, Kopečkova 273a/9	IIZS	Plzeňský	50 Mbps			Fixní kanál	5	/16	/16	/16	/16	Best effort	2	2	100 %
				480 Mbps			Fixní kanál	5	/16	/16	/16	/16	Best effort	2	2	100 %
				2 Gbps	10 Gbps		Dynamické kanálu	5	/16	/16	/16	/16	99,99 %	4	4	100 %
				2 Gbps	10 Gbps		Fixní kanál/ Dynamické kanálu	5	/16	/16	/16	/16	99,99 %	4	4	100 %
CDC 3	Olomouc, Schwarzova 924/11	IIZS	Olomoucký	50 Mbps			Fixní kanál	5	/16	/16	/16	/16	Best effort	2	2	100 %
				480 Mbps			Fixní kanál	5	/16	/16	/16	/16	Best effort	2	2	100 %
				2 Gbps	10 Gbps		Dynamické kanálu	5	/16	/16	/16	/16	99,99 %	4	4	100 %
				2 Gbps	10 Gbps		Fixní kanál/ Dynamické kanálu	5	/16	/16	/16	/16	99,99 %	4	4	100 %

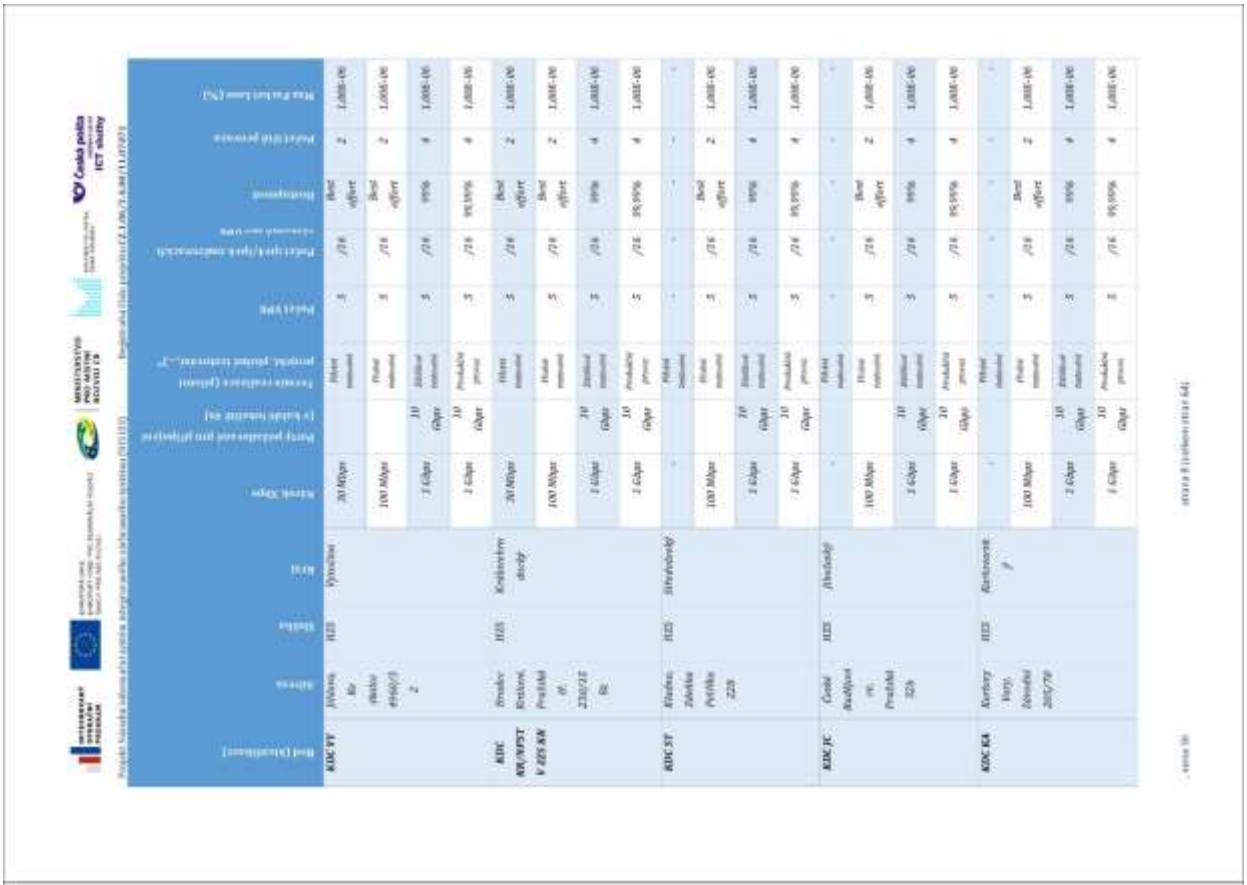
Tabulka 2 – Požadavky na připojení CDC



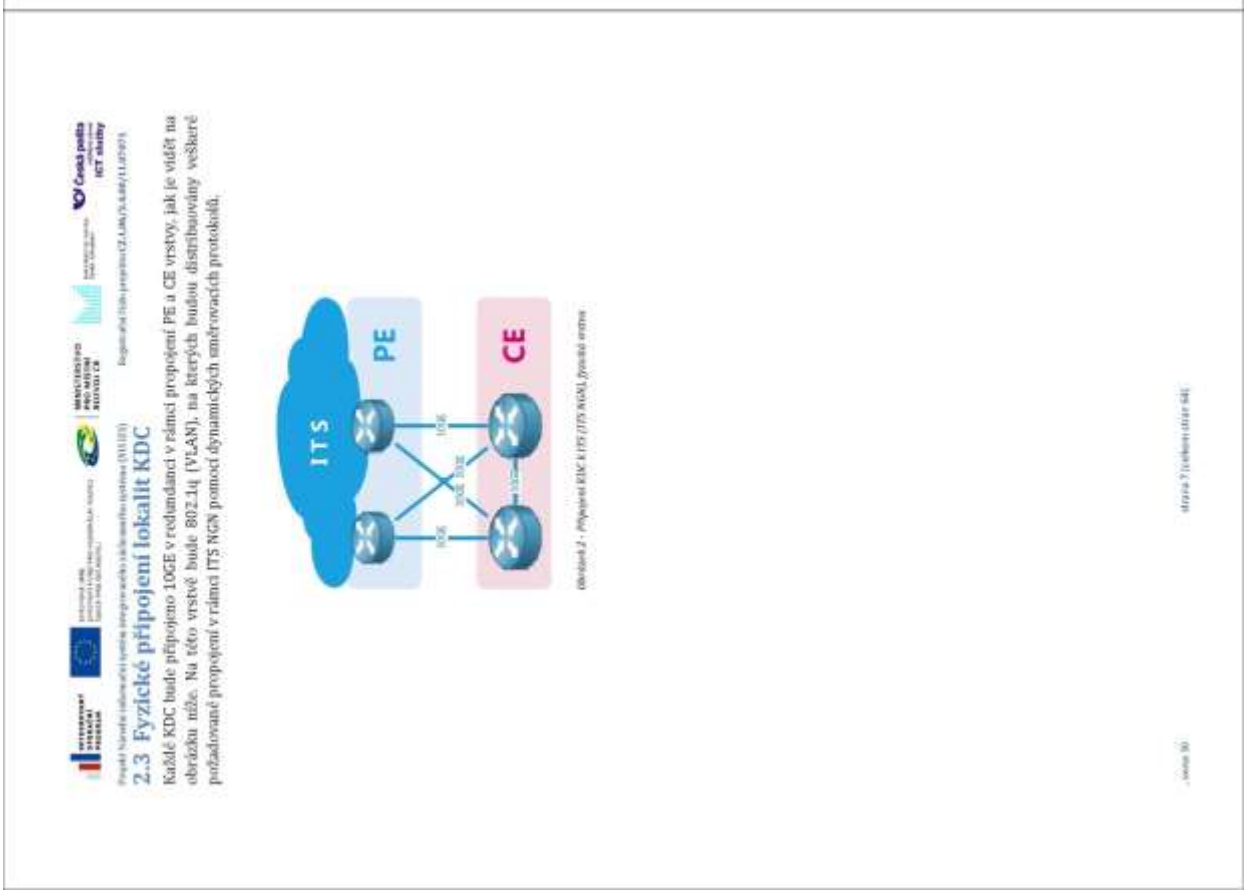
Obrázek 1 – Připojení CDC k ITS (ITS NGN), fyzická vrstva

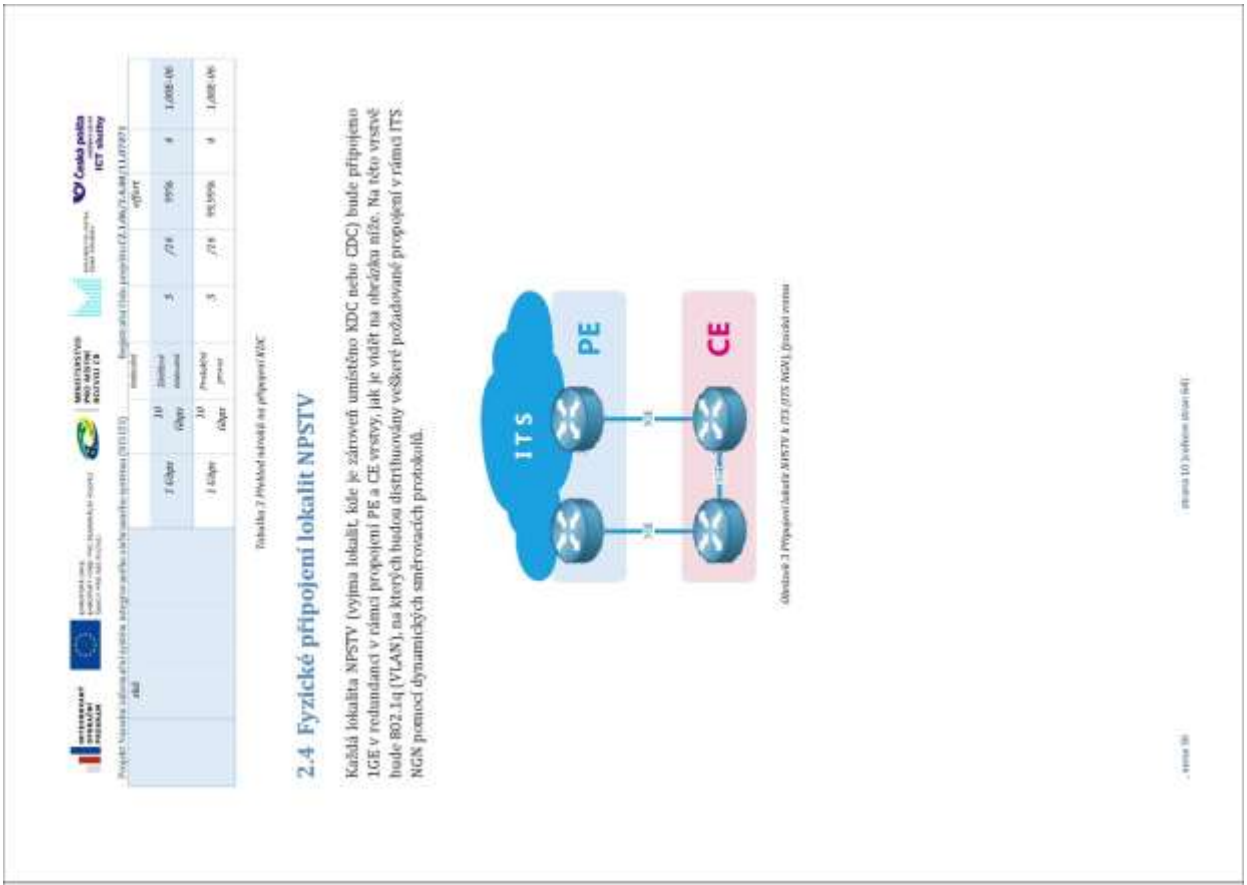
2.2 Fyzické připojení lokalit CDC

Každé CDC bude připojeno 10GE v redundanci v rámci propojení PE a CE vrstvy, jak je vidět na obrázku níže. Na této vrstvě bude 802.1q (VLAN), na kterých budou distribuovány veškeré požadovaná propojení v rámci ITS NGN pomocí dynamických směrovacích protokolů.

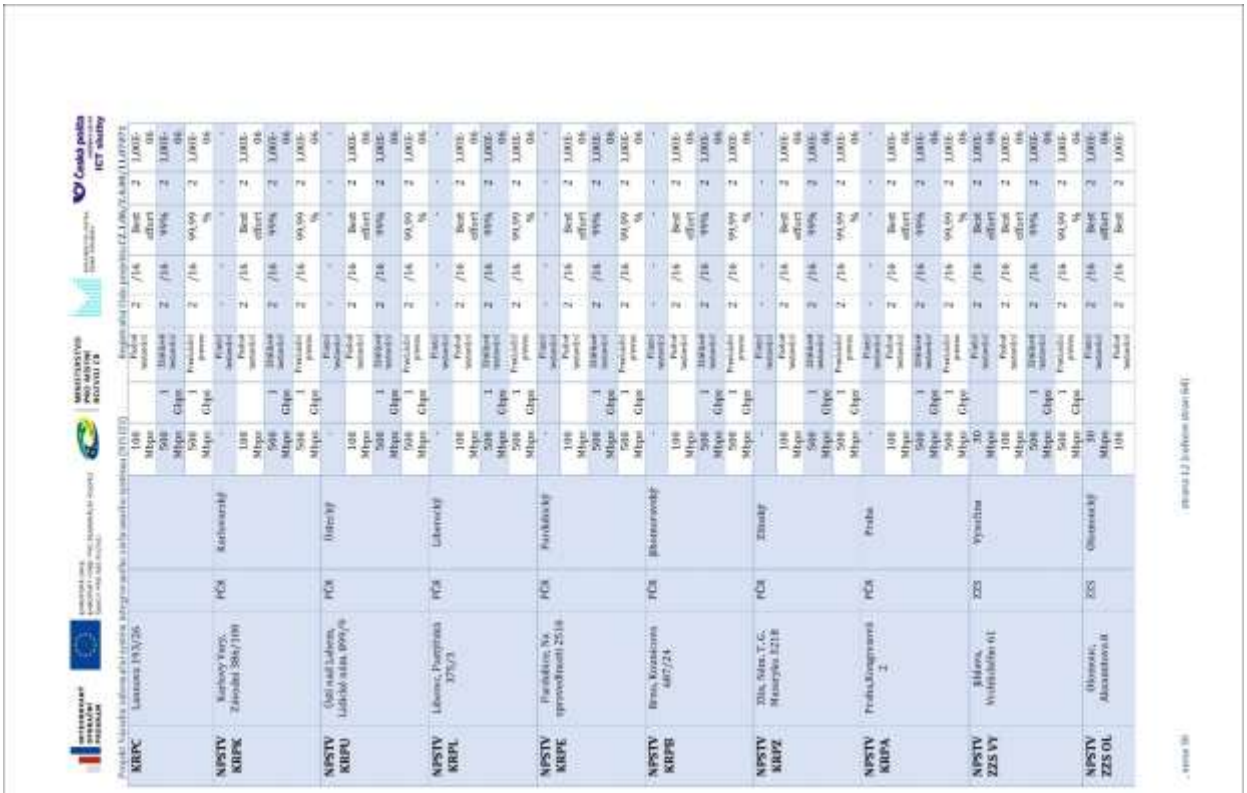


Bod (číslo/název)	Adresa	Stavba	Area	Rychlost linky	Délka trasy (km)	Počet vlaken	Počet vlaken/pás (nebo samostatná vlákna)	Počet typů	Bezpečnost	Počet vlaken pro provozu	Bez ochrany (%)
KDC VY	Jihlava, Ke Rybníku 4960/3 2	IZS	Vysočina	30 Mbps	Hlavní napájení	5	/16	Bod-bod optika	99%	2	1.00E-00
				100 Mbps	Hlavní napájení	5	/16	Bod-bod optika	99%	2	1.00E-00
KDC KR/NPST V IZS KR	Hradec Králové, Pražská ul. 230/2 IZ	IZS	Královéhradecký kraj	1 Gbps	10 Gbps / Produkční provoz	5	/16	Bod-bod optika	99%	4	1.00E-00
				30 Mbps	Hlavní napájení	5	/16	Bod-bod optika	99.9%	4	1.00E-00
				100 Mbps	Hlavní napájení	5	/16	Bod-bod optika	99%	2	1.00E-00
				1 Gbps	10 Gbps / Produkční provoz	5	/16	Bod-bod optika	99%	2	1.00E-00
				1 Gbps	10 Gbps / Produkční provoz	5	/16	Bod-bod optika	99.9%	4	1.00E-00
KDC ST	Kladno, Zámecká Petříkův 228	IZS	Středočeský kraj	-	Hlavní napájení	-	-	-	-	-	1.00E-00
				100 Mbps	Hlavní napájení	5	/16	Bod-bod optika	99%	2	1.00E-00
				1 Gbps	10 Gbps / Produkční provoz	5	/16	Bod-bod optika	99%	4	1.00E-00
				1 Gbps	10 Gbps / Produkční provoz	5	/16	Bod-bod optika	99.9%	4	1.00E-00
KDC JC	České Budějovice ul. Pražská 329	IZS	Jihočeský kraj	-	Hlavní napájení	-	-	-	-	-	1.00E-00
				100 Mbps	Hlavní napájení	5	/16	Bod-bod optika	99%	2	1.00E-00
				1 Gbps	10 Gbps / Produkční provoz	5	/16	Bod-bod optika	99%	4	1.00E-00
				1 Gbps	10 Gbps / Produkční provoz	5	/16	Bod-bod optika	99.9%	4	1.00E-00
KDC KA	Karlovy Vary, Závodní 205/79	IZS	Karlovarský kraj	-	Hlavní napájení	-	-	-	-	-	1.00E-00
				100 Mbps	Hlavní napájení	5	/16	Bod-bod optika	99%	2	1.00E-00
				1 Gbps	10 Gbps / Produkční provoz	5	/16	Bod-bod optika	99%	4	1.00E-00
				1 Gbps	10 Gbps / Produkční provoz	5	/16	Bod-bod optika	99.9%	4	1.00E-00

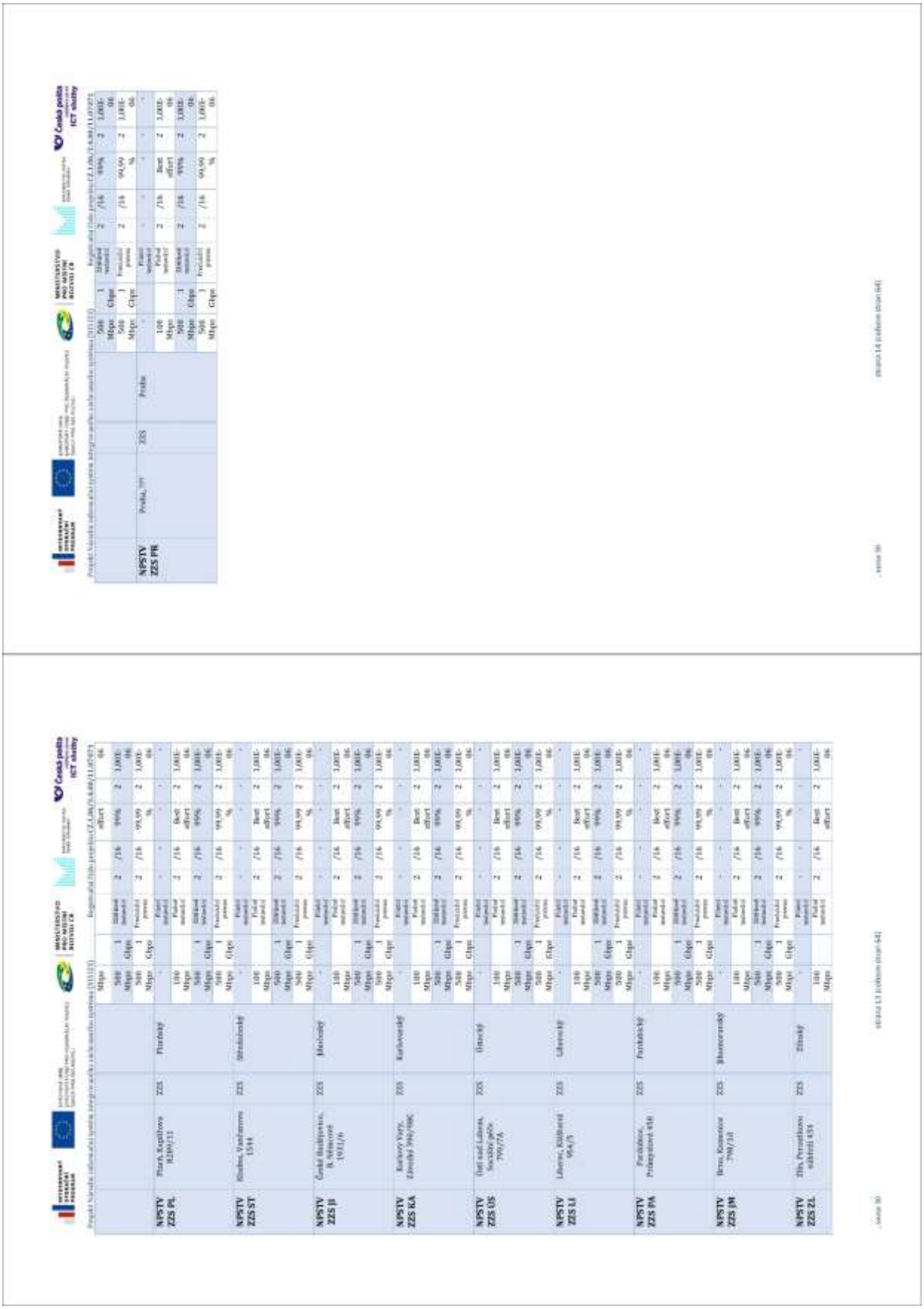




| | | |



| | | |

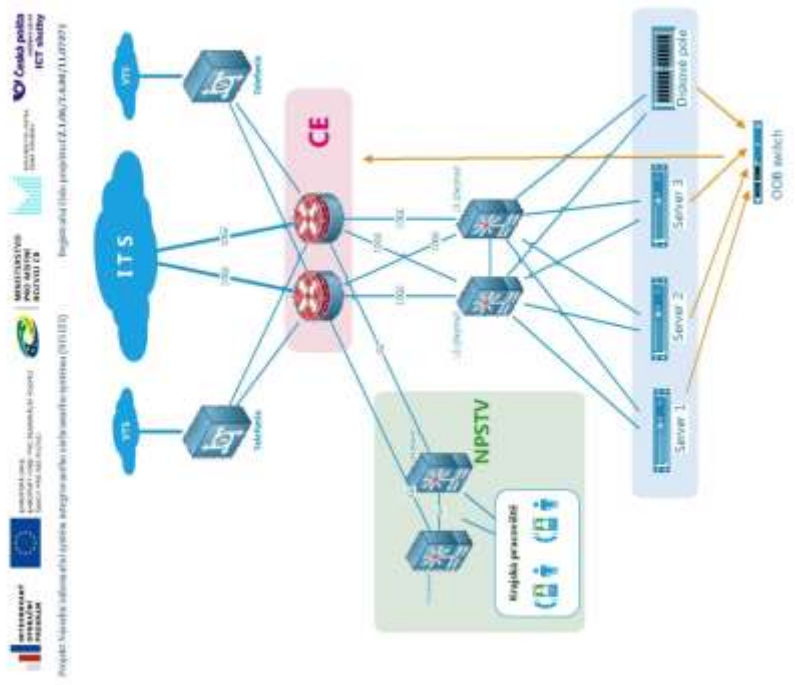


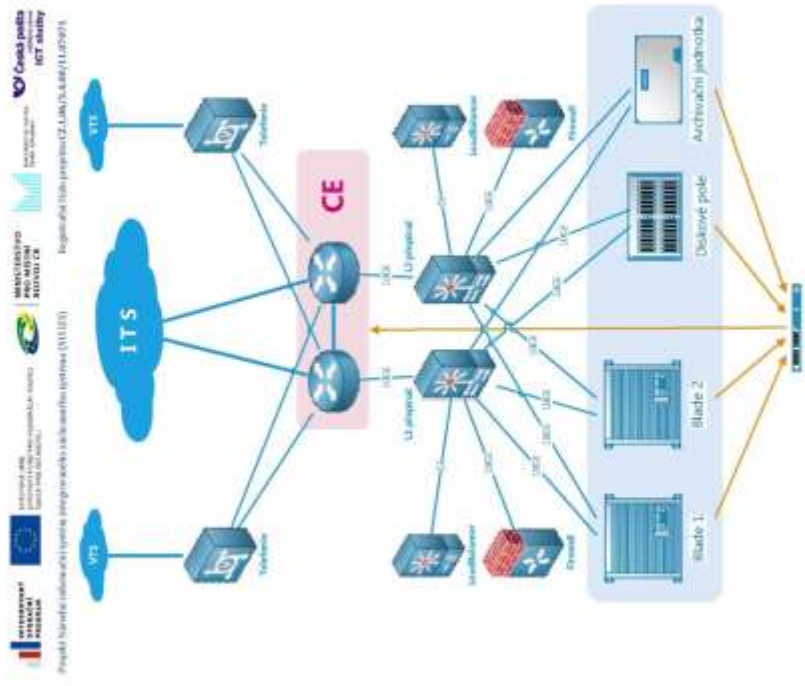
3 Zapojení technologií NIS IZS

Připojení technologií NIS IZS v každé z lokalit bude realizováno pomocí CE směrovačů připojených redundantně k PE směrovačům sítě ITS NGN. Připojení NPSTV PČR bude využívat CE směrovačů z projektu KSP PČR, lokalita HZS bude využívat k připojení CE směrovače KDC/CDC dodávané v rámci projektu NIS IZS. Složky ZZS budou v rámci projektu NIS IZS osazeny dvojicí CE směrovačů, které zajistí plnou funkcionalitu připojení.

3.1 Zapojení CDC

Technologie CDC budou připojeny k síti ITS (resp. ITS NGN) dvojicí CE směrovačů, zajišťující dynamické směrování do všech sítí NIS IZS a přístup k externím systémům (systémů OŘ a externím službám přes CMS, resp. CMS 2.0). Dále budou tyto CE směrovače plnit funkcionalitu CE směrovačů pro KDC a NPSTV HZS. Centrální redundantní L3 přepínače budou obstarávat směrování uvnitř centrálního datového centra. Součástí CDC bude i dvojice firewallů a load balancerů, které budou mít na starosti řízení a přístup jednotlivých datových toků ke službám poskytovaným z CDC. Centrální L3 přepínače budou zároveň obsluhovat komunikaci serverové farmy, diskového pole a archivační jednotky.

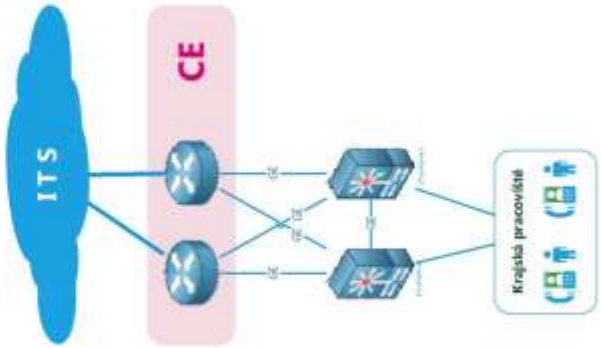




3.2 Zapojení KDC

Technologie KDC budou k síti ITS (resp. ITS NGN) připojeny dvojicí CE směrovačů s firewall funkcionalitou, které zajistí jak přístup datových toků mezi uzly NIS IZS, tak bezpečný přístup externích systémů, jako jsou například systémy OR. Dále budou tyto CE směrovače plnit funkcionalitu CE směrovačů pro NPSTV HZS. Dvojice centrálních L3 přepínačů bude zajišťovat směrování a přepínání uvnitř krajského datového centra.

3.3.2 Zapojení NSPTV ZZS

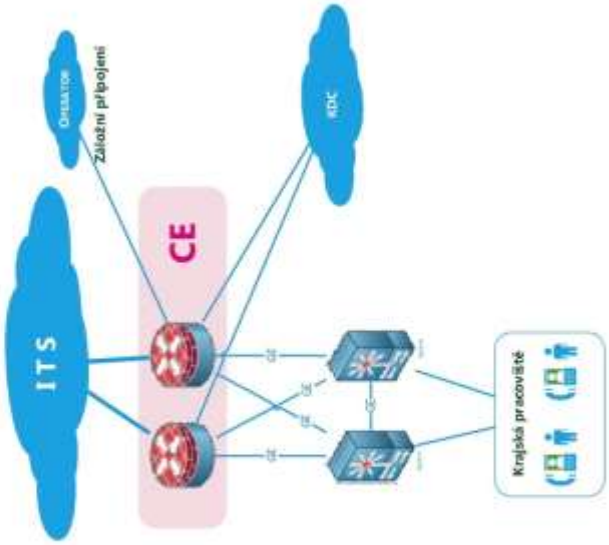


Obrázek 7 - Zapojení NPSTV PČR a ZZS

Připojení NSPTV ZZS bude realizováno dvojicí CE směrovačů. Dále bude následovat dvojice přepínačů s PoE funkcionalitou pro provoz telefonie. Všechna datová propojení budou na úrovni gigabit ethernetu.

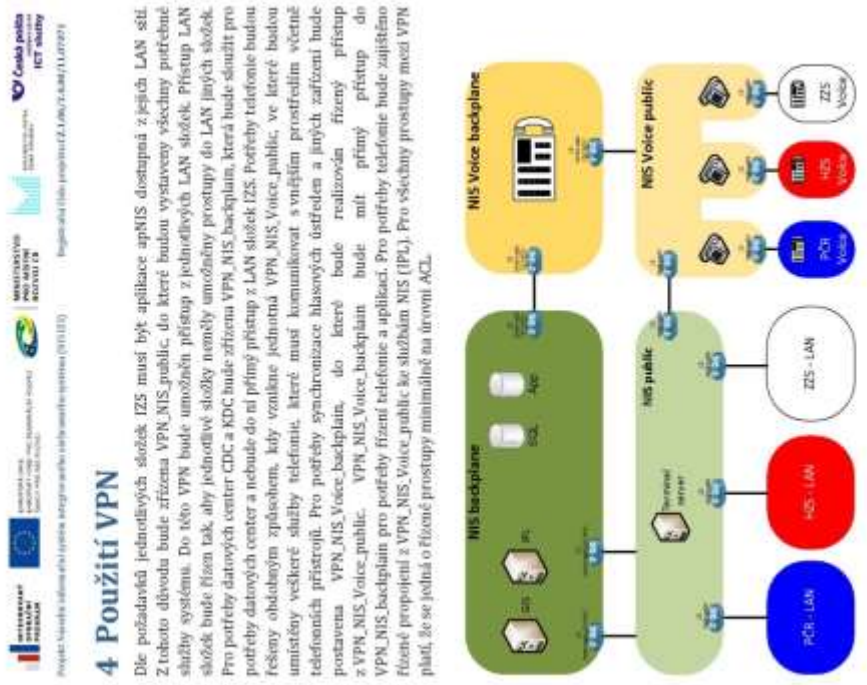
3.3 Zapojení NPSTV

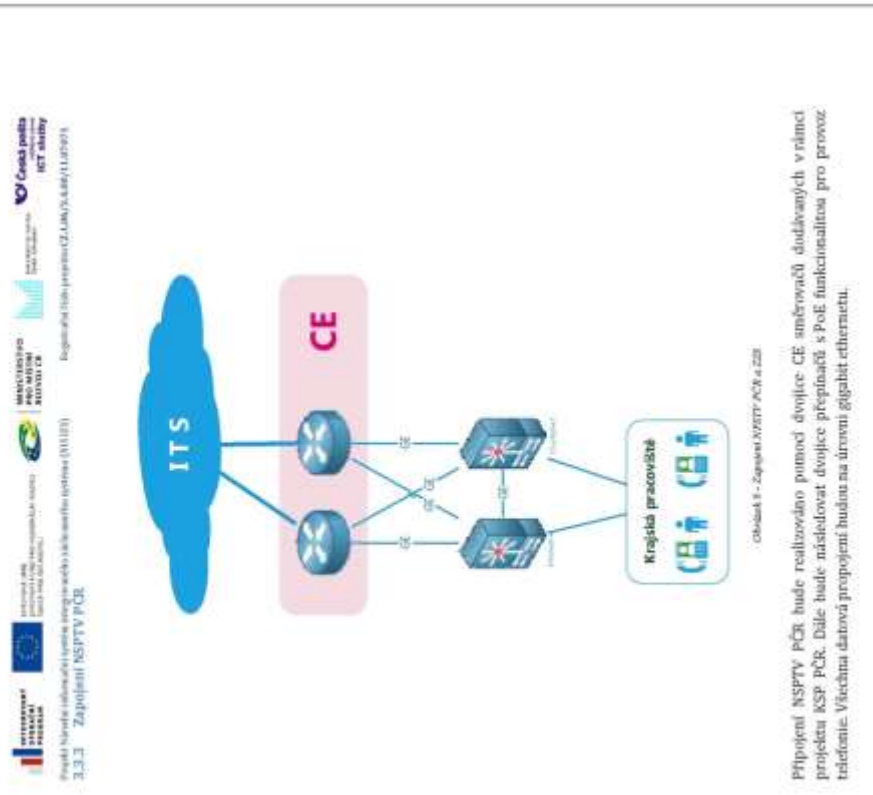
3.3.1 Zapojení NPSTV HZS



Obrázek 6 - Zapojení NPSTV HZS

Připojení technologií NPSTV HZS bude realizováno dvojicí CE směrovačů s funkcionalitou firewallu, které primárně slouží k připojení KDC a budou sloužit zároveň jako CE směrovače pro NPSTV HZS. Dále bude následovat dvojice přepínačů s PoE funkcionalitou pro provoz telefonie. Všechna datová propojení budou na úrovni gigabit ethernetu.


4 Použití VPN
Dle požadavků jednotlivých složek IZS musí být aplikace apNIS dostupná z jejich LAN sítí. Z tohoto důvodu bude zřízena VPN_NIS_public, do které budou vystaveny všechny potřebné služby systému. Do této VPN bude umožněn přístup z jednotlivých LAN složek. Přístup LAN složek bude řízen tak, aby jednotlivé složky neměly umožněny prostupy do LAN jiných složek. Pro potřeby datových center CDC a KDC bude zřízena VPN_NIS_backplain, která bude sloužit pro potřeby datových center a nebude do ní přímý přístup z LAN složek IZS. Potřeby telefonie budou řešeny obdobným způsobem, kdy vznikne jednotná VPN_NIS_Voice_public, ve které budou umístěny veškeré služby telefonie, které musí komunikovat s vnějším prostředím včetně telefonních přístrojů. Pro potřeby synchronizace hlasových ústředen a jiných zařízení bude postavena VPN_NIS_Voice_backplain, do které bude realizován řízený přístup z VPN_NIS_Voice_public. VPN_NIS_Voice_backplain bude mít přímý přístup do VPN_NIS_backplain pro potřeby řízení telefonie a aplikací. Pro potřeby telefonie bude zajištěno řízené propojení z VPN_NIS_Voice_public ke službám NIS (IPL). Pro všechny prostupy mezi VPN platí, že se jedná o řízené prostupy minimálně na úrovni ACL.
NIS backplane
NIS Voice backplane
NIS public
NIS Voice public
PČR - LAN
HZS - LAN
ZZS - LAN
PČR Voice
HZS Voice
ZZS Voice
Distribuci VPN pro jednotlivé složky bude zajišťovat infrastruktura sítě ITS NGN, kde jednotlivé VPN budou plně odděleny a prostup mezi jednotlivými VPN bude řízen CE směrovači NIS IZS na základě předem dohodnutých pravidel. Každá změna propagování jednotlivých podsítí/VPN NIS IZS na PE směrovači bude změněna na základě požadavků na změnu v rámci change management procesů systému NIS IZS. Z prostředí ApNIS bude možné přistupovat ke všem GIS


3.3.3 Zapojení NSPTV PČR
ITS
CE
Krajská pracoviště
Připojení NSPTV PČR bude realizováno pomocí dvojice CE směrovačů dodávaných v rámci projektu KSP PČR. Dále bude následovat dvojice přepínačů s PoE funkcionalitou pro provoz telefonie. Všechna datová propojení budou na úrovni gigabit ethernetu.

serverům a ke všem IPL jak v CDC tak KDC, jediné IPL může zprostředkovat datovou komunikaci mezi jednotlivými operátory a informačními systémy složek.

Toto vše znamená, že každá LAN složky IZS bude mít síťový přístup ke všem IPL a GIS serverům, ale nebude moci komunikovat s žádnou jinou VPN. Veškerou potřebnou datovou komunikaci mezi složkami IZS bude zajišťovat IPL, hlasová VPN bude pro všechny složky společná a bude zajišťovat jak obsluhu telefonu, tak i komunikaci mezi jednotlivými ústřednami.

5 Propojení s externími systémy

Přístup jakýchkoliv externích systémů do všech datových VPN bude umožněn pouze přes firewally v jednotlivých CDC a KDC na základě předem stanovených pravidel přístupu. Další přístup je možný přes služby vystavené NIS IZS v CMS (resp. CMS 2.0), kde se o bezpečné propojení stará bezpečnostní politika systému CMS (resp. CMS 2.0).

5.1 Připojení CDC/KDC k CMS (CMS 2.0)

Datová centra NIS IZS potřebují komunikovat s externími systémy jako je například JSDI, RÚIAN, INFO 35. Toto připojení bude prostřednictvím VPN NPSTV_CMS, která bude také terminována na InterConnect CMS (CMS 2.0), případně budou vytvořeny další propojovací VPN v závislosti na bezpečnostní politice CMS 2.0 (jelikož je projekt v přípravě, tyto politiky není možné předjímat), které budou šířeny k jednotlivým datovým centrům. Na těchto propojeních budou nejen přijímána data z externích systémů, ale zároveň budou sloužit k vystavění služeb NIS IZS do CMS (CMS 2.0). Další možností využití CMS (CMS 2.0) je zálohování připojení NPSTV k centrálním datovým centrům NIS IZS přes šifrované a zabezpečené připojení přes veřejný internet například pomocí IPSec.

NIS public	Datová centra VPN NIS public	10.8.32.0/19	10.8.28.0/24 Olomoucký kraj - KDC
			10.8.29.0/24
			10.8.30.0/24 Moravskoslezský kraj - KDC
			10.8.31.0/24
			10.8.32.0/24 Reserva
			10.8.33.0/24
			10.8.34.0/24
			10.8.35.0/24
			10.8.36.0/24
			10.8.37.0/24
			10.8.38.0/24
			10.8.39.0/24
			10.8.40.0/24
			10.8.41.0/24
			10.8.42.0/24
			10.8.43.0/24
			10.8.44.0/24
			10.8.45.0/24
			10.8.46.0/24
			10.8.47.0/24
			10.8.48.0/24
			10.8.49.0/24
			10.8.50.0/24
			10.8.51.0/24
			10.8.52.0/24
			10.8.53.0/24
			10.8.54.0/24
			10.8.55.0/24
			10.8.56.0/24
			10.8.57.0/24
			10.8.58.0/24
			10.8.59.0/24
			10.8.60.0/24
			10.8.61.0/24
			10.8.62.0/24
			10.8.63.0/24
		10.8.64.0/20	10.8.64.0/24
			10.8.65.0/24
			10.8.66.0/24 Středočeský kraj
			10.8.67.0/24 Jihočeský kraj
			10.8.68.0/24 Plzeňský kraj
			10.8.69.0/24 Karlovarský kraj

6 Adresace

Strukturální rozdělení IP adresního prostoru pro projekt NIS IZS je naznačen v tabulce IP adres. Tabulka naznačuje skupinové a účelové dělení a vytváří rezervy pro rozšiřování a modifikace.

Přidělení IP adres jednotlivým regionům a VPN podle místa a cíle určení vychází ze zvyklostí IP adresace používané v datových sítích MV a PČR (DSMV). Doporučuje se, aby segmenty serverů byly oddělené na úrovni LAN od segmentů uživatelů. Evidenci IP adres v jednotlivých uživatelských a serverových LAN segmentech vede příslušný lokální administrátor LAN. Evidence LAN a adresních skupin je vedena centrálně u provozovatele ČP OZ.

IP adresní rozsah pro NIS IZS je zvolen tak, aby pro datové sítě MV, PČR, HZS a ZZS byl nekolizní, takže v případě vzájemného propojení není potřeba provádět překlady adres.

VPN	Lokalita	Rozsah	Podsítě	Přidělení
VPN NIS backplain	Datová centra	10.8.0.0/19	10.8.0.0/24	Praha - CDC
			10.8.1.0/24	
			10.8.2.0/24	Plzeňský kraj - CDC
			10.8.3.0/24	
			10.8.4.0/24	Olomoucký kraj - CDC
			10.8.5.0/24	
			10.8.6.0/24	Středočeský kraj - KDC
			10.8.7.0/24	
			10.8.8.0/24	Jihočeský kraj - KDC
			10.8.9.0/24	
			10.8.10.0/24	Plzeňský kraj - KDC
			10.8.11.0/24	
			10.8.12.0/24	Karlovarský kraj - KDC
			10.8.13.0/24	
			10.8.14.0/24	Ústecký kraj - KDC
			10.8.15.0/24	
			10.8.16.0/24	Liberecký kraj - KDC
			10.8.17.0/24	
			10.8.18.0/24	Královehradecký kraj - KDC
			10.8.19.0/24	
			10.8.20.0/24	Pardubický kraj - KDC
			10.8.21.0/24	
			10.8.22.0/24	Kraj Vysočina - KDC
			10.8.23.0/24	
			10.8.24.0/24	Jihomoravský kraj - KDC
			10.8.25.0/24	
			10.8.26.0/24	Zlínský kraj - KDC
			10.8.27.0/24	

Voice backplain	10.B.112.0/20	10.B.112.0/24	
		10.B.113.0/24	
		10.B.114.0/24	Středočeský kraj
		10.B.115.0/24	Jihočeský kraj
		10.B.116.0/24	Plzeňský kraj
		10.B.117.0/24	Karlovarský kraj
		10.B.118.0/24	Ústecký kraj
		10.B.119.0/24	Liberecký kraj
		10.B.120.0/24	Královehradecký kraj
		10.B.121.0/24	Pardubický kraj
		10.B.122.0/24	Kraj Vysočina
		10.B.123.0/24	Jihomoravský kraj
		10.B.124.0/24	Zlínský kraj
		10.B.125.0/24	Olomoucký kraj
		10.B.126.0/24	Moravskoslezský kraj
		10.B.127.0/24	Praha
	10.B.128.0/17	10.B.128.0/24	Rezerva
		10.B.129.0/24	
		10.B.130.0/24	
		10.B.131.0/24	
		10.B.132.0/24	
		10.B.133.0/24	
		10.B.134.0/24	
		10.B.135.0/24	
		10.B.136.0/24	
		10.B.137.0/24	
		10.B.138.0/24	
		10.B.139.0/24	
		10.B.140.0/24	
		10.B.141.0/24	
		10.B.142.0/24	
		10.B.143.0/24	
NIS Voice public		10.B.144.0/24	PČR Voice
		10.B.145.0/24	Reserva PČR Voice
		10.B.146.0/24	ZZS Voice
		10.B.147.0/24	Reserva ZZS Voice
		10.B.148.0/24	
		10.B.149.0/24	
		10.B.150.0/24	
		10.B.151.0/24	
Jihočeský kraj		10.B.152.0/24	PČR Voice
		10.B.153.0/24	Reserva PČR Voice

	10.B.80.0/20	10.B.70.0/24	Ústecký kraj
		10.B.71.0/24	Liberecký kraj
		10.B.72.0/24	Královehradecký kraj
		10.B.73.0/24	Pardubický kraj
		10.B.74.0/24	Kraj Vysočina
		10.B.75.0/24	Jihomoravský kraj
		10.B.76.0/24	Zlínský kraj
		10.B.77.0/24	Olomoucký kraj
		10.B.78.0/24	Moravskoslezský kraj
		10.B.79.0/24	Praha
		10.B.80.0/24	Rezerva
		10.B.81.0/24	
		10.B.82.0/24	
		10.B.83.0/24	
		10.B.84.0/24	
		10.B.85.0/24	
		10.B.86.0/24	
		10.B.87.0/24	
		10.B.88.0/24	
		10.B.89.0/24	
		10.B.90.0/24	
		10.B.91.0/24	
		10.B.92.0/24	
		10.B.93.0/24	
		10.B.94.0/24	
		10.B.95.0/24	
	10.B.96.0/20	10.B.96.0/24	
		10.B.97.0/24	
		10.B.98.0/24	
		10.B.99.0/24	
		10.B.100.0/24	
		10.B.101.0/24	
		10.B.102.0/24	
		10.B.103.0/24	
		10.B.104.0/24	
		10.B.105.0/24	
		10.B.106.0/24	
		10.B.107.0/24	
		10.B.108.0/24	
		10.B.109.0/24	
		10.B.110.0/24	
		10.B.111.0/24	

Pardubický kraj	10.B.196.0/24		
	10.B.197.0/24		
	10.B.198.0/24		
	10.B.199.0/24		
	10.B.200.0/24	PČR Voice	
	10.B.201.0/24	Reserva PČR Voice	
	10.B.202.0/24	ZZS Voice	
	10.B.203.0/24	Reserva ZZS Voice	
	10.B.204.0/24		
	10.B.205.0/24		
	10.B.206.0/24		
	10.B.207.0/24		
Kraj Vysočina	10.B.208.0/24	PČR Voice	
	10.B.209.0/24	Reserva PČR Voice	
	10.B.210.0/24	ZZS Voice	
	10.B.211.0/24	Reserva ZZS Voice	
	10.B.212.0/24		
	10.B.213.0/24		
	10.B.214.0/24		
	10.B.215.0/24		
Jihomoravský kraj	10.B.216.0/24	PČR Voice	
	10.B.217.0/24	Reserva PČR Voice	
	10.B.218.0/24	ZZS Voice	
	10.B.219.0/24	Reserva ZZS Voice	
	10.B.220.0/24		
	10.B.221.0/24		
	10.B.222.0/24		
	10.B.223.0/24		
Zlínský kraj	10.B.224.0/24	PČR Voice	
	10.B.225.0/24	Reserva PČR Voice	
	10.B.226.0/24	ZZS Voice	
	10.B.227.0/24	Reserva ZZS Voice	
	10.B.228.0/24		
	10.B.229.0/24		
	10.B.230.0/24		
	10.B.231.0/24		
Olomoucký kraj	10.B.232.0/24	PČR Voice	
	10.B.233.0/24	Reserva PČR Voice	
	10.B.234.0/24	ZZS Voice	
	10.B.235.0/24	Reserva ZZS Voice	
	10.B.236.0/24		
	10.B.237.0/24		

Přerovský kraj	10.B.154.0/24	ZZS Voice	
	10.B.155.0/24	Reserva ZZS Voice	
	10.B.156.0/24		
	10.B.157.0/24		
	10.B.158.0/24		
	10.B.159.0/24		
Karlovarský kraj	10.B.160.0/24	PČR Voice	
	10.B.161.0/24	Reserva PČR Voice	
	10.B.162.0/24	ZZS Voice	
	10.B.163.0/24	Reserva ZZS Voice	
	10.B.164.0/24		
	10.B.165.0/24		
	10.B.166.0/24		
	10.B.167.0/24		
Ústecký kraj	10.B.168.0/24	PČR Voice	
	10.B.169.0/24	Reserva PČR Voice	
	10.B.170.0/24	ZZS Voice	
	10.B.171.0/24	Reserva ZZS Voice	
	10.B.172.0/24		
	10.B.173.0/24		
	10.B.174.0/24		
	10.B.175.0/24		
Liberecký kraj	10.B.176.0/24	PČR Voice	
	10.B.177.0/24	Reserva PČR Voice	
	10.B.178.0/24	ZZS Voice	
	10.B.179.0/24	Reserva ZZS Voice	
	10.B.180.0/24		
	10.B.181.0/24		
	10.B.182.0/24		
	10.B.183.0/24		
Královéhradecký kraj	10.B.184.0/24	PČR Voice	
	10.B.185.0/24	Reserva PČR Voice	
	10.B.186.0/24	ZZS Voice	
	10.B.187.0/24	Reserva ZZS Voice	
	10.B.188.0/24		
	10.B.189.0/24		
	10.B.190.0/24		
	10.B.191.0/24		
	10.B.192.0/24	PČR Voice	
	10.B.193.0/24	Reserva PČR Voice	
	10.B.194.0/24	ZZS Voice	
	10.B.195.0/24	Reserva ZZS Voice	

7 Specifikace dodávky síťové infrastruktury

7.1 Specifikace komponent CDC

7.1.1 CDC+KDC - CII směrovač

Počet ks v jedné lokalitě: 2

Počet lokalit celkem (2xCDC+KDC, 1x CDC): 3

7.1.1.1 Závazné parametry

č.	Hardware
1	Formát zařízení - modulární
2	Maximální velikost 2RU
3	Minimálně 2x 10GE s volitelným fyzickým rozhraním
4	Minimálně 2 volné sloty pro rozšíření
5	Nehlokující architektura přepínaru/bo/směrovačbo subsystému (wire speed)
6	Nehlokující architektura převodu interface - přepínací/směrovací subsystém min. pro všechny popisované interface současně (platí zejména pro modulární zařízení)
7	Redundantní napájení (zařízení musí být schopno plné funkce při poruše jednoho napájecího zdroje).
8	Možnost výměny napájecích zdrojů za provozu (hot-swap) bez ovlivnění funkce zařízení jako celku
9	Duální podpora IPv4 a IPv6 (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, tzv. dual stack)
10	Hardwarová podpora L3 přepínání/směrování protokolů IPv4 a IPv6
11	Filtrování TCP a UDP bez nepříznivého vlivu na řádnou funkčnost zařízení
12	Nehlokující (wire speed) replikace multicastu v HW
13	Kontrola přípustnosti zdrojové IPv4 a IPv6 adresy na všech (fyzických i logických) L3 rozhraních podle aktuální směrovací tabulky (antispoofingová kontrola ekvivalentní funkci RPF check, reverse path forwarding check dle RFC 3704)
14	Hardwarová podpora bezstavové bezpečnostní filtrace provozu podle L2/L3/L4 atributů na úrovni linkové/síťové/transportní vrstvy aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní (VLAN)
15	Hardwarová podpora dlouhých ethernetových rámců (tzv. jumbo frames) datový obsah rámce (payload) alespoň 9000 B
16	Hardwarová podpora omezení (procentuálního poměru) broadcastového provozu na rozhraní (broadcast storm control)
17	Statické směrování pro IPv4 a IPv6 unicast i multicast
18	Rozkládání zátěžení na L3 paralelních cestách (ECMP)
19	OSPF v2 dle RFC 2328
20	OSPF v3 dle RFC 5340
21	Kontrolovaná redistribuce směrovacích informací mezi protokoly
22	Podpora L2 paralelních cest dle IEEE 802.3ad
23	Podpora IEEE 802.3ad přes více karet

Moravskoslezký kraj		10.B.238.0/24	
		10.B.239.0/24	
		10.B.240.0/24	PČR Voice
		10.B.241.0/24	Reserva PČR Voice
		10.B.242.0/24	ZZS Voice
		10.B.243.0/24	Reserva ZZS Voice
		10.B.244.0/24	
		10.B.245.0/24	
		10.B.246.0/24	
		10.B.247.0/24	
Praha		10.B.248.0/24	PČR Voice
		10.B.249.0/24	Reserva PČR Voice
		10.B.250.0/24	ZZS Voice
		10.B.251.0/24	Reserva ZZS Voice
		10.B.252.0/24	
		10.B.253.0/24	
		10.B.254.0/24	
		10.B.255.0/24	

Tabulka 4 – Tabulka adresace NPSTV

24	Podpora detekce jednosměrné komunikace na lince (např. BFD)
25	Možnost omezení počtu naučených MAC adres na rozhraní (ochrana proti útokům typu zaplavení vnitřní tabulky MAC adres přepínače/mostu).
26	Podpora výměnných DWDM rozhraní (dosah až 80km)
27	Fyzická specifikace
28	Redundantní FAN a PSU
29	Modularní chassis
30	Výkon
31	Non-blocking architektura
32	Distribuovaný „control" a „forwarding" plane
33	L2 funkcionality
34	Minimálně 500k MAC na systém
35	Minimálně 128k ARP záznamů na systém
36	Jumbo frames 9000B
37	Podpora IEEE 802.1Q
38	Plný rozsah VLAN (4k)
39	Podpora IEEE 802.1QinQ
40	Inner / Outer VLAN rozsáhlá manipulace
41	podpora LACP
42	Multi Chassis LAG
43	Detekce protiběžného zařízení LLDP (IEEE 802.1AB)
44	Interface spec. funkce
45	per subinterface encapsulation
46	per subinterface Vlan tag type (kombinace single VLAN, QinQ, non-tag (native VLAN))
47	Routed L3 interface, (každý subinterface má subnet
48	Routed VLAN (Bridge) interface
49	L3 capability
50	Minimálně IPv4 20kB route v RIB
51	IPv4 HW support
52	RIP, OSPF, ISIS, BGPv4
53	Podpora GRE (Generic Routing Encapsulation)
54	Static routing
55	VRF lite (IPv4/6)
56	Minimálně IPv6 20kB route v RIB
57	IPv6 HW support
58	RIPng, OSPFv3, MBGP, ISIS pro IPv6
59	BFD pro BGP, OSFPv2, OSPFv3, ISIS
60	Policy based routing / filter based routing
61	Multicast
62	IGMP snooping v1/2/3
63	IGMP v1/2/3
64	PIM SM/SSM/DM

65	MSDP
66	Podpora IPv6 Multicast (MLDv1 & v2)
67	Podpora IPv6 Multicast (PIM SM)
68	Podpora IPv6 Multicast (PIM SSM)
69	MPLS
70	Hardwarová podpora MPLS
71	LDP / RSVP signalizace
72	RSVP ping/path
73	RSVP-TE (FRR, Link/node protection)
74	L2VPN
75	VPLS LDP based
76	VPLS BGP based
77	L3VPN (RFC 4364)
78	Mcast in L3VPN - draft Rosen
79	Podpora Label Imposition a Label Disposition (MPLS Provider Edge)
80	Podpora Label Swapping (MPLS Provider Core)
81	Podpora LDP (Label Distribution Protocol)
82	Podpora MPLS TE
83	Podpora P2MP TE
84	Podpora mLDP
85	Podpora IPv6 over MPLS (6PE)
86	Podpora IPv6 VPN over MPLS (6VPE)
87	Bezpečnost
88	Policing / rate limit pro provoz směrem k CPU
89	ACLka na provoz směrem k CPU
90	Podpora IPv6 ACL
91	Podpora reverse path check (uRPF) v hardwaru
92	ACL pro IP
93	Bezstavová Kontrola / Řízení provozu L2-L7 (tzv. ACLka)
94	ACLka v HW (TCAM / CAM)
95	Port ACLka (vstup / výstup)
96	VLAN (Bridge) ACLka (vstup / výstup)
97	Routed ACLka (vstup / výstup)
98	Policing pod interface
99	CoS
100	Klasifikace provozu
101	802.1p
102	DSCP
103	IP precedence
104	MPLS exp.
105	Založeno na bezstavovém vyhodnocení paketů v L2-L4
106	Port shaping / Queue shaping

107	Policing
108	Minimálně 8x Queues na port
109	Minimálně 8x forwarding class
110	Minimálně 4 priority per Scheduler
111	Strict priority implementace
112	WRED
113	Rewrite rules – přepsání CoS bitů
114	Podpora IPv6 QoS
115	Vysoká dostupnost
116	Forwarding známých paketů bez asistence „control plane"
117	Management
118	Modularní operační systém
119	Command line interface (CLI)
120	Minimálně 10 konfiguračních záloh přímo na zařízení s možností jejich návratu příkazem z CLI
121	Aktivní a „batch" konfigurace = změny se promítnou do funkce až po potvrzení = časované změny, masivní změny nastav atd
122	Archivace konfigurací do souborů přímo na boxu
123	Archivace konfigurací na vzdáleném FTP / SCP - i automatická
124	Local přístup do CLI přes konsole port
125	Management zařízení Telnet / SSH
126	FTP, TFTP client a server
127	Podpora NETCONF
128	Syslog
129	Centralizovaná authentikace pro přístup na zařízení Radius/Tacacs+
130	Omezení práv přístupu dle uživatelských rolí
131	Možnost omezení přístupu k managementu (SSH, SNMP)
132	Konfigurační soubory v čitelném formátu (například ASCII, TXT, XML)
133	Možnost nahrání/zálohování konfigurace zařízení po síti pomocí alespoň jednoho z protokolů TFTP, FTP, HTTP, SCP nebo SFTP
134	Možnost povýšení operačního systému zařízení po síti pomocí alespoň jednoho z protokolů TFTP, FTP, HTTP, SCP nebo SFTP
135	Secure Shell (SSHv2)
136	Podpora centrální autorizace příkazů prostřednictvím protokolu TACACS+ nebo RADIUS
137	Out-of-Band Management
138	Tx a Rx optical power monitoring (DOM)
139	Podpora synchronizace času protokolem NTP, minimálně verze 3.
140	Podpora protokolů SNMPv2, SNMPv3 (včetně schopnosti generovat trapy při detekci významných událostí) a syslog.
141	Podpora SNMPv2/v3 MIBs a traps
142	Možnost omezit oprávněné zdrojové IP adresy manažerských stanic pro vzdálený konfigurační přístup
143	Možnost omezit oprávněné zdrojové IP adresy SNMP manažerských stanic
144	Network Management a monitoring

145	Port mirroring
146	Real-time performance monitoring
147	NetFlow v9 IPFIX RFC 3917, 3955 nebo obdobné
148	Ping / traceroute
149	Debug na úrovni protokolů interface a procesů
150	NTP klient
151	DNS klient
152	Podpora interních nástrojů pro debugging provozního provozu
153	Podpora interních nástrojů pro on-line měření kvality síťové infrastruktury
154	Výkon
155	Minimální propustnost jednoho šasi 800Gbps
156	Rozšiřující rozhraní
157	Minimálně 2x 10GE s volitelným fyzickým rozhraním
158	Minimálně 20x 1GE SFP s volitelným fyzickým rozhraním
159	Interface moduly (přesnou vlnovou délku a přesný počet modulů zadavatel stanoví v objednávce)
160	Minimálně 1x 10GE Multimode SR optický modul (originál od výrobce)
161	Minimálně 1x 10GE SingleMode LR optický modul (originál od výrobce)
162	Minimálně 1x 10GE SingleMode ER optický modul (originál od výrobce)
163	Minimálně 1x 10GE DWDM SingleMode optický modul C Band Tunable (100-GHz ITU grid)
164	Minimálně 1x 100GBASE-DWDM 1550XXX nm (100-GHz ITU grid)
165	Minimálně 1x 1GE Multimode SX optický modul (originál od výrobce)
166	Minimálně 1x 1GE Singlemode LX/LH optický modul (originál od výrobce)
167	Minimálně 1x 1GE Metalický modul s konnektorem RJ45(originál od výrobce)
168	Servisní a doplňkové požadavky
169	Záruka a produktová podpora min. 5 let
170	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zaškolení
171	Veškeré licence SW potřebné ke specifikovanému řešení
172	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

7.1.2 CDC - L2/L3 přepínač

Počet ks v jedné lokalitě: 2

Počet lokalit celkem (1xCDC, 2xCDC+KDC): 3

- Tento vysokorychlostní přepínač bude využíván jako centrální komunikační prvek v CDC a bude zajišťovat datové propojení s ostatními CDC a KDC. Do každého z nich bude dodáváno ve dvou instancích pro zajištění požadované redundantní řešení.

7.1.2.1 Závazné parametry

Č.	Základní vlastnosti
1	Typ zařízení přepínač

2	Formát zařízení modulární
3	Redundantní řídící modul
4	Redundantní zdroj
5	Minimálně 7 slotů v šasi
6	Minimálně 48 portů ethernet 10/100/1000 (RJ-45)
7	Podpora modulů s minimálně 24 portů 1GE s volitelným fyzickým rozhraním
8	Minimálně 10 neblokujících portů 10GE s volitelným fyzickým rozhraním
9	Podpora modulů s minimálně 16 porty 10GE s volitelným fyzickým rozhraním
10	Podpora modulů s 40GE s volitelným fyzickým rozhraním
11	Podpora GRE tunelování v hardware
12	Podpora IPv4 a IPV6 v hardware
13	Podpora MPLS a VPLS v hardware
14	Podpora virtualizace – možnost sloučit dvě fyzická šasi do jednoho logického
15	Výkonnostní parametry
16	Minimální dostupná kapacita na slot 220Gbps
17	Minimálně 256k záznamů ve směrovací tabulce - IPv4 unicast
18	Minimálně 128k záznamů ve směrovací tabulce – IPv6 unicast
19	Minimálně 128k záznamů ve směrovací tabulce - IPv4 multicast
20	Minimálně 128k záznamů ve směrovací tabulce – IPv6 multicast
21	Protokoly fyzické vrstvy
22	IEEE 802.3ad
23	IEEE 802.3ad přes více karet
24	Podpora IEEE 802.3ad přes více šasí (Multichassis Etherchannel)
25	Podpora "jumbo rámců"
26	Protokoly 2. vrstvy
27	IEEE 802.1D
28	IEEE 802.1Q
29	Minimálně 4000 aktivních VLAN
30	IEEE 802.1s - multiple spanning trees
31	IEEE 802.1w - Rapid Tree Spanning Protocol
32	Detekce protilehlého zařízení (např. CDP nebo LLDP)
33	Protokol pro definici šířených VLAN (např. GVRP nebo ekvivalentní)
34	Detekce jednosměrnosti optické linky (např. OAM link fault management nebo ekvivalentní)
35	STP root guard nebo ekvivalentní
36	STP loop guard nebo ekvivalentní
37	Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)
38	Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech
39	Protokol IP
40	Podpora router redundancy protokol (např. VRRP, HSRP)
41	Podpora BGPv4
42	Podpora OSPFv2

43	Podpora IS-IS
44	Podpora IGMPv2, IGMPv3
45	Podpora Multicast (PIM SSM, PIM SM)
46	Podpora funkce Non-Stop Forwarding nebo ekvivalentní pro protokoly OSPF, BGP a IS-IS
47	Podpora DHCP relay
48	Policy-based routing podle ACL
49	Podpora reverse path check (uRPF)
50	Podpora GRE (Generic Routing Encapsulation)
51	Podpora Policy-based routing podle ACL
52	MPLS
53	Podpora MPLS
54	Podpora virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)
55	Podpora L3 MPLS VPN
56	Minimálně 500 podporovaných MPLS VPN
57	Podpora Label Edge Router (LER) funkce
58	Podpora QoS s využitím EXP bitů
59	Podpora MPLS TE (Traffic Engineering)
60	Podpora Multicast MPLS VPN (MVPN)
61	Podpora 6VPE (IPv6 VPN over MPLS)
62	Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)
63	Podpora MPLS TE FRR (MPLS Traffic Engineering Fast Reroute)
64	Podpora EoMPLS
65	Podpora VPLS
66	QoS
67	Podpora QoS classification – ACL, DSCP, CoS based
68	Podpora QoS marking - DSCP, CoS
69	Podpora QoS Policing
70	Podpora QoS - Strict Priority Queue pro ukládání paketů IP telefonního provozu
71	Podpora rate limiting
72	Protokol IPv6
73	Podpora VRRP nebo ekvivalentní pro IPv6
74	Podpora OSPFv3
75	Podpora MP BGP
76	Podpora IS-IS pro IPv6
77	Podpora IPv6 QoS
78	Podpora IPv6 ACL
79	Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP, DHCP)
80	Podpora IPv6 Multicast (MLDv1 & v2)
81	Podpora IPv6 Multicast (PIM SM)
82	Podpora IPv6 Multicast (PIM SSM)
83	Podpora IPv6 nástrojů pro měření kvality sítě (např. SLA, NQA)
84	Podpora IPv6 over GRE v HW

Podpis/signature:.....

85	Podpora DHCPv6 Relay
86	Podpora oddělených částí paketů pro IPv4 a IPv6 provoz
87	Podpora NetFlow pro IPv6
88	Podpora uRPF pro IPv6
89	Bezpečnost
90	ACL na rozhraní IN/OUT (včetně virtuálních - VLAN)
91	Možnost provádět změny ACL bez ztráta narušení provozu
92	Možnost definovat povolené MAC adresy na portu
93	Možnost definovat maximální počet MAC adres na portu
94	Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)
95	Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)
96	Podpora bezpečnostních funkcí umožňujících ochranu proti podvržení zdrojové IP adresy – IP source guard nebo ekvivalentní
97	Podpora bezpečnostních funkcí umožňujících ochranu proti připojení neautorizovaného DHCP serveru – DHCP snooping nebo ekvivalentní
98	Podpora bezpečnostních funkcí umožňujících inspekci provozu protokolu ARP – ARP inspection nebo ekvivalentní
99	Konfigurovatelné prostředky L3 přepínače před útoky typu odepření služby (DoS) formou vhodného omezení frekvence určitých typů rámců/paketů, které jsou zpracovávány procesorem zařízení
100	Podpora koncových zařízení
101	Podpora automatické detekce IP telefonu připojeného k portu LAN přepínače a automatické nastavení vhodných QoS parametrů daného portu
102	Podpora automatické detekce IP telefonu připojeného k portu LAN přepínače a jeho automatické přiřazení do dedikované voice VLAN
103	Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu
104	Management
105	CLI rozhraní
106	SSHv2
107	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
108	SNMPv2
109	SNMPv3
110	DNS klient
111	NTP klient s MD5 autentizací
112	RADIUS klient pro AAA (autentizace, autorizace, accounting)
113	TACACS+ klient
114	Port mirroring (SPAN)
115	Vzdálený port mirroring (RSPAN)
116	Syslog
117	Podpora interních nástrojů pro debugging procházejícího provozu
118	Monitorování aplikačních toků
119	Podpora monitorování aplikačních toků (všech paketů) s využitím technologie NetFlow
120	Možnost definice široké škály klíčových atributů a parametrů monitorovaných toků včetně parametrů, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód
121	Podpora exportu NetFlow dat dle formátu NetFlow v9 nebo IPFIX
122	Administrátorem definovatelné monitory datových toků, které mohou být aplikovány na jednotlivá fyzická nebo virtuální rozhraní L3 přepínače
123	Možnost definovat minimálně dva různé monitory datových toků současně, jeden monitor pro sběr parametrů datových toků potřebných pro analýzu aplikačních toků, druhý monitor pro sběr parametrů datových toků potřebných pro detekci bezpečnostních incidentů
124	Minimálně 512000 NetFlow záznamů
125	Podpora interních nástrojů pro on line měření kvality síťové infrastruktury, např. IP SLA
126	Ostatní funkce a služby
127	DHCP server
128	Podpora interních nástrojů pro automatické spouštění předem definovaných akcí na základě detekce různých síťových událostí
129	Dostupné moduly
130	Modul s minimálně 20 GigabitEthernet rozhraní 10/100/1000 Base-TX
131	Modul s minimálně 40 GigabitEthernet rozhraní 10/100/1000 Base-TX
132	Modul s minimálně 20x 1GE s volitelným fyzickým rozhraním
133	Modul s minimálně 4x 10GE s volitelným fyzickým rozhraním
134	Modul s minimálně 8x 10GE s volitelným fyzickým rozhraním
135	Modul s minimálně 12x 10GE s volitelným fyzickým rozhraním

5	Redundantní AC napájení
6	Možnost výměny zdroje za chodu (hot swap)
7	Minimálně 4x 1GE rozhraní
8	Minimálně 4x 10GE rozhraní (SFP+)
9	Možnost nasazení více zařízení (aktivní / záložní)
10	Virtualizace
11	Počet virtuálních load balancerů minimálně 8
12	Plné oddělení virtuálních instancí (L2-L7, management, ...)
13	Garantovaný výkon pro virtuální load balancer
14	Oddělený management (každá instance má svého administrátora)
15	Výkon
16	Propustnost minimálně 15Gbps
17	Počet současných spojení na L4 minimálně 5M
18	Počet nových spojení za vteřinu (CPS) na L7 minimálně 800K
19	Počet nových spojení za vteřinu (CPS) na L4 minimálně 500K
20	SSL offloading propustnost minimálně 10Gbps
21	SSL transakcí za vteřinu (TPS) minimálně 10K
22	Síťová podpora
23	Podpora VRRP nebo ekvivalentní mechanismus
24	IPv6
25	VLAN (802.1Q) minimálně 900
26	Směrovací protokoly - RIP, OSPF, BGP
27	LACP (802.3ad
28	Monitorování stavu serverů (Health monitoring)
29	Monitorování stavu serverů - ICMP
30	Monitorování stavu serverů - TCP
31	Monitorování stavu serverů - UDP
32	Monitorování stavu serverů - SSL Hello
33	Monitorování stavu serverů - HTTP obsah
34	Monitorování stavu serverů - POP3
35	Monitorování stavu serverů - IMAP4
36	Monitorování stavu serverů - SMTP
37	Monitorování stavu serverů - SIP
38	Monitorování stavu serverů - Možnost kombinace metod
39	Monitorování stavu serverů - Možnost definovat interval ověřování
40	Monitorování stavu serverů - Možnost definovat timeout
	Monitorování stavu serverů - Možnost definovat počet opakování před prohlášením služby za dostupnou
41	Loadbalancing - Na základě L3 - L7 parametrů
42	Loadbalancing - IP hash
43	Loadbalancing - HTTP cookies
44	Loadbalancing - SSL session ID
45	

5	
136	Interface moduly (přesnou vlnovou délku a přesný počet modulů zadavatel stanoví v objednávce)
137	Minimálně 1x 10GE Multimode SR optický modul (originál od výrobce)
138	Minimálně 1x 10GE SingleMode LR optický modul (originál od výrobce)
139	Minimálně 1x 10GE SingleMode ER optický modul (originál od výrobce)
140	Minimálně 1x 10GBASE-DWDM 15XX.XX nm (100-GHz ITU grid)
141	Minimálně 1x 1GE Multimode SX optický modul (originál od výrobce)
142	Minimálně 1x 1GE Singlemode LX/LH optický modul (originál od výrobce)
143	Minimálně 1x 1GE Metalický modul s konectorem RJ45(originál od výrobce)
144	Minimálně 1x 10GE DAC kabel, délka 1m (originál od výrobce)
145	Minimálně 1x 10GE DAC kabel, délka 3m (originál od výrobce)
146	Minimálně 1x 10GE DAC kabel, délka 5m (originál od výrobce)
147	Servisní a doplňkové požadavky
148	Záruka a produktová podpora min. 5 let
149	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zaškolení
150	Veškeré licence SW potřebné ke specifikovanému řešení
151	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

7.1.3 CDC – load balancer

Počet ks v jedné lokalitě: 2

Počet lokalit celkem (LxCDC, 2xCDC+KDC): 3

- Load balancer bude zajišťovat potřebné aplikační funkce a požadované reakční záložte na zařízení umístěná v rámci jednoho CDC. Do každého CDC bude dodáván zdvojené.

7.1.3.1 Závazné parametry

Č.	Základní vlastnosti
1	Loadbalancer - HW Appliance
2	Dedikovaný management port
3	Konzolový port pro správu
4	Rozměry maximálně 4RU

46	Loadbalancing - Hodnoty obsažené v HTTP hlavičce
47	Loadbalancing - Možnost vkládání cookies pro perzistenci spojení
48	Loadbalancing - Možnost modifikace URL
49	Loadbalancing - Aplikačního provozu na základě vrstev L3 – L7
50	Loadbalancing - Možnost balancingu na základě provozu (v příchozím i odchozím směru)
51	Management
52	Centrální management
53	Možnost definovat uživatele s různým oprávněním
54	Management přes protokol SSH
55	Management přes protokol HTTPS (GUI)
56	Podpora protokolu SNMP
57	Ukládání konfigurace v textovém formátu
58	Podpora Syslog
59	Podpora protokolu NTP pro synchronizaci času
60	Interface moduly (přesnou vhodnou délku a přesný počet modulů zadavatel stanoví v objednávce)
61	Minimálně 1x 10GE Multimode SR optický modul
62	Minimálně 1x 10GE SingleMode LR optický modul
63	Minimálně 1x 1GE Multimode SX optický modul
64	Minimálně 1x 1GE Singlemode LX/ULH optický modul
65	Minimálně 1x 1GE Metalický modul s konektorem RJ45
66	Servisní a doplňkové požadavky
67	Záruka a produktová podpora min. 5 let
68	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zaškolení
69	Veškeré licence SW potřebné ke specifikovanému řešení
70	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

7.1.4 CDC - Firewall

Počet ks v jedné lokalitě 2

Počet lokalit celkem (1xCDC, 2xCDC+RDC): 3

- Firewall bude zajišťovat potřebné zabezpečení zařízení umístěných v rámci jednoho CDC. Do každého CDC bude dodáván zdvojené.

7.1.4.1 Závazné parametry

Č.	Základní parametry
1	Formát zařízení - modulární firewall
2	Minimálně 6x 10G s volitelným fyzickým rozhraním
3	Out-of-Band management interface 10/100 nebo 10/100/1000
4	Redundantní zapojení
5	Minimální počet současně otevřených spojení 5M
6	Minimální počet nově otevřených spojení za vteřinu (init/close) 245K
7	Podpora stateful failover
8	Podpora Active/Passive, Active/Active failoveru
9	Propustnost firewallu 30Gb/s
10	Propustnost IPS 10Gb/s
11	Propustnost VPN (IPSec AES/3DES) 5Gb/s
12	Minimální počet IPSec VPN 7500
13	Multicore architektura s interním loadbalancingem
14	Podpora logických systémů s garantováním výpočetních prostředků
15	Zónový firewall
16	Do jedné zóny je možné přiřadit více interfaců
17	Podpora stateful IPv4 firewallu
18	Podpora stateful IPv6 firewallu
19	Podpora IPv6 IPS
20	L3 funkce
21	Minimální počet IPv4 záznamů ve směrovací tabulce (unicast) 700K
22	Minimální počet IPv6 záznamů ve směrovací tabulce (unicast) 500K
23	Podpora routovacího protokolu OSPFv2, OSPFv3
24	Podpora routovacího protokolu BIP
25	Podpora multicast směrovacího protokolu PIM
26	Podpora protokolu IGMP
27	Podpora virtuálních směrovacích tabulek min. 250 (VRF, Virtuální router...)
28	L2 funkce
29	Podpora Link agregation 802.3ad (LACP)
30	Podpora Agregace portu přes celý Firewall Cluster
31	Podpora 802.1Q (VLAN)
32	Minimální počet aktivních VLAN 1024
33	Security funkce
34	Podpora NAT/PAT
35	Podpora NAT66
36	Podpora NAT64
37	Podpora Static NAT
38	Podpora Aplikačního Firewallu (rozpoznání aplikací nezávisle na TCP/UDP portech)
39	Dostupnost výrobcem definované aplikační signatury
40	Zobrazení statistik Aplikačního firewallu
41	Podporad Dos, DDoS ochrany
42	Možnost nastavení maximálního počtu spojení za časovou jednotku
43	Množství bezpečnostních pravidel (celkem) 40k
44	Podpora dynamických pravidel (doplňkovaných např. z AAA serveru)
45	Podporad ALG (inspekce) pro protokoly DNS, H.323, IKE, SIP, SCCP, RPC, FTP
46	IPS pro IPv4
47	IPS pro IPv6

5	Minimální počet zařízení ve stohu 8
6	Minimální kapacita sběrnice stohu 80Gbps
7	Dostupná provedení – minimálně následující varianty
8	24 portů 10/100/1000, 4 porty GE (SFP)
9	Výkonnostní parametry
10	Propustnost přepínacího subsystému minimálně 56Gbps
11	Protokoly fyzické vrstvy
12	Podpora standardu IEEE 802.3ad
13	Minimálně 24 konfigurovatelných portchannel skupin
14	Podpora IEEE 802.3ad přes více přepínačů ve stohu
15	Podpora "jumbo rámců"
16	Protokoly 2. vrstvy
17	IEEE 802.1D
18	IEEE 802.1Q
19	Podpora Private VLAN nebo ekvivalentní
20	Minimální 1000 aktivních VLAN
21	IEEE 802.1x
22	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)
23	Podpora integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)
24	IEEE 802.1s - multiple spanning trees
25	IEEE 802.1w - Rapid Tree Spanning Protocol
26	Detekce protilehlého zařízení (např. CDP nebo LLDP)
27	Protokol pro definici šířených VLAN (např. GVRP nebo ekvivalentní)
28	Detekce jednosměrnosti optické linky (např. OAM link fault management nebo ekvivalentní)
29	STP root guard nebo ekvivalentní
30	STP loop guard nebo ekvivalentní
31	Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)
32	Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech
33	Protokol IP
34	Podpora IGMP snooping
35	Podpora IPv6 MLD snooping
36	Podpora IPv6 port ACL
37	Podpora IPv6 QoS
38	Podpora IPv6 RA guard
39	Podpora IPv6 source guard
40	Popdora DHCPv6 snooping
41	Podpora IPv6 ND inspection
42	QoS
43	Podpora QoS classification – ACL, DSCP, CoS based

48	QoS funkce
49	Omezení maximální šířky pásma
50	Shaping
51	Policing
52	Management
53	CLI rozhraní (sériová konzole, telnet, sshž)
54	SNMPv2
55	Podpora sběru Flow informací
56	Autentizace proti AAA serveru protokolem RADIUS, TACAS+
57	Syslog
58	Podpora DHCP relay
59	Podpora DHCPv6 relay
60	Interface moduly (přesnou vlnovou délku a přesný počet modulů zadavatel stanoví v objednávce)
61	Minimálně 1x 10GE Multimode SR optický modul (originál od výrobce)
62	Minimálně 1x 10GE SingleMode LR optický modul (originál od výrobce)
63	Minimálně 1x 10GE SingleMode ER optický modul (originál od výrobce)
64	Minimálně 1x 1GE Multimode SX optický modul (originál od výrobce)
65	Minimálně 1x 1GE Singlemode LX/LH optický modul (originál od výrobce)
66	Minimálně 1x 1GE Metalický modul s koncovkou RJ45(originál od výrobce)
67	Licence (množství a typ požadovaných licencí bude upřesněn v minitendru)
68	Jednoletý upgrade signatůr pro IPS
69	Servisní a doplňkové požadavky
70	Záruka a produktová podpora min. 5 let
71	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zahoření
72	Veškeré licence SW potřebné ke specifikovanému řešení
73	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

1.

7.1.5 OOB - L2/L3 přepínač

Počet instancí v rámci 1 CDC/KDC: 1

Počet lokalit celkem (1xCDC, 2xCDC+KDC, 12xKDC): 15

7.1.5.1 Tento přepínač bude sloužit k vytvoření oddělené Out-Off-Band management sítě. Závazné parametry

č.	Základní vlastnosti
1	Třída zařízení přepínač
2	Formát zařízení pro instalaci do Racku maximální velikost 1RU
3	Možnost rozšíření o redundantní zdroj
4	Možnost stohování

Podpis/signature:.....

44	Podpora QoS marking - DSCP, CoS
45	Podpora QoS Policing
46	Podpora QoS - Strict Priority Queue pro ukládání paketů IP telefonního provozu
47	Podpora rate limiting
48	Bezpečnost
49	ACL na rozhraní IN/OUT (včetně virtuálních - VLAN)
50	Možnost definovat povolené MAC adresy na portu
51	Možnost definovat maximální počet MAC adres na portu
52	Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)
53	Podpora bezpečnostních fun kcí umožňujících ochranu proti podvržení zdrojové IP adresy – IP source guard nebo ekvivalentní
54	Podpora bezpečnostních funkcí umožňujících ochranu proti připojení neautorizovaného DHCP serveru – DHCP snooping nebo ekvivalentní
55	Podpora bezpečnostních funkcí umožňujících inspekci provozu protokolu ARP – ARP inspection nebo ekvivalentní
56	Podpora koncových zařízení
57	Podpora IEEE 802.3az
58	Podpora automatické detekce IP telefonu připojeného k portu LAN přepínače a automatické nastavení vhodných QoS parametrů daného portu
59	Podpora automatické detekce IP telefonu připojeného k portu LAN přepínače a jeho automatické přiřazení do dedikované voice VLAN
60	Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu
61	Management
62	CLI rozhraní
63	SSHv2
64	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
65	SNMPv2
66	SNMPv3
67	DNS klient
68	NTP klient s MD5 autentizací
69	RADIUS klient pro AAA (autentizace, autorizace, accounting)
70	TACACS+ klient
71	Port mirroring (SPAN)
72	Vzdálený port mirroring (RSPAN)
73	Syslog
74	Podpora interních nástrojů pro debugging procházejícího provozu
75	Monitorování aplikačních toků
76	Podpora monitorování aplikačních toků s využitím Sampled NetFlow nebo sFlow
77	Podpora monitorování aplikačních toků na fyzických i VLAN rozhraních
78	Možnost nastavení vzorkovací rychlosti

79	Požadované interface moduly součástí prvku (přesnou vlnovou délku a přesný počet modulů zadavatel stanoví v minitendru)
80	Minimálně 1x 1GE Multimode SX optický modul (originál od výrobce)
81	Minimálně 1x 1GE Singlemode LX/LH optický modul (originál od výrobce)
82	Minimálně 1x 1GE Metalický modul s koncovkou RJ45(originál od výrobce)
83	Servisní a dopětkové požadavky
84	Záruka a produktová podpora min. 5 let
85	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zahoření
86	Veškeré licence SW potřebné ke specifikovanému řešení
87	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

7.2 Specifikace komponent KDC

7.2.1 KDC - CE směrovač

Počet ks v jedné lokalitě 2

Počet lokalit celkem (12 lokalit KDC bez fce CDC): 12

7.2.1.1 Závazné parametry

č.	Hardware
1	Formát zařízení - modulární
2	Maximální velikost 2RU
3	Minimálně 2x 10GE s volitelným fyzickým rozhraním
4	Minimálně 2 volné sloty pro rozšíření
5	Nehlokující architektura přepínacího/směrovacího subsystému (wire speed)
6	Nehlokující architektura přechodu interface - přepínací/směrovací subsystém min. pro všechny podávané interface současně (platí zejména pro modulární zařízení)
7	Redundantní napájení (zařízení musí být schopno plné funkce při poruše jednoho napájecího zdroje).
8	Možnost výměny napájecích zdrojů za provozu (hot-swap) bez ovlivnění funkce zařízení jako celku
9	Duální podpora IPv4 a IPv6 (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, tzv. dual stack)
10	Hardwarová podpora L3 přepínání/směrování protokolů IPv4 a IPv6
11	Filtrování TCP a UDP bez negativního vlivu na řádnou funkčnost zařízení
12	Nehlokující (wire speed) replikace multicastu v HW
13	Kontrola přípustnosti zdrojové IPv4 a IPv6 adresy na všech (fyzických i logických) L3 rozhraních podle aktuální směrovací tabulky (antispoofingová kontrola ekvivalentní funkci RPF check, reverse path forwarding check dle RFC 3704)
14	Hardwarová podpora bezstavové bezpečnostní filtrace provozu podle L2/L3/L4 atributů na úrovni linkové/síťové/transportní vrstvy aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní (VLAN)

Příloha č. 8 zadávací dokumentace – Specifikace systémů NIS IZS a NSTPV

15	Hardwarová podpora dlouhých ethernetových rámců (tzv. jumbo frames) datový obsah rámce (payload) alespoň 9000 B
16	Hardwarová podpora omezení (geocentrálního poměru) broadcastového provozu na rozhraní (broadcast storm control)
17	Statické směrování pro IPv4 a IPv6 unicast i multicast
18	Rozkládání zátěžení na L3 paralelních cestách (ECMP)
19	OSPF v2 dle RFC 2328
20	OSPF v3 dle RFC 5340
21	Kontrolované rozšiřování směrovacích informací mezi protokoly
22	Podpora L2 paralelních cest dle IEEE 802.3ad
23	Podpora IEEE 802.3ad přes více karet
24	Podpora detekce jednosměrné komunikace na lince (např. BFD)
25	Možnost omezení počtu naučených MAC adres na rozhraní (obrana proti útokům typu zahlcení vnitřní tabulky MAC adres přepínače/mostu).
26	Podpora výměnných IWDM rozhraní (dosah až 80km)
27	Fyzická specifikace
28	Redundantní FAN a PSU
29	Modularní chassis
30	Výkon
31	Non-blocking architektura
32	Distribuovaný „control" a „forwarding" plane
33	L2 funkcionality
34	Minimálně 500k MAC na systém
35	Minimálně 128k ARP záznamů na systém
36	Jumbo frames 9000B
37	Podpora IEEE 802.1Q
38	Plný rozsah VLAN (4k)
39	Podpora IEEE 802.1Q(inQ
40	Inner / Outer VLAN rozsáhlá manipulace
41	podpora LACP
42	Multi Chassis LAG
43	Detekce protiklidného zařízení LLDP (IEEE 802.1AB)
44	Interface spec. funkce
45	per subinterface encapsulation
46	per subinterface Vlan tag type (kombinace single VLAN, Qinq, non-tag (native VLAN))
47	Routed L3 interface, tj.každý subinterface má subnet
48	Routed VLAN (Bridge) interface
49	L3 capability
50	Minimálně IPv4 384k route v RIB
51	IPv4 HW support
52	RIP, OSPF, ISIS, BGPv4
53	Podpora GRE (Generic Routing Encapsulation)

54	Static routing
55	VRF lite (IPv4/6)
56	Minimálně IPv6 2Mil. route v RIB
57	IPv6 HW support
58	RIPng, OSPFv3, MBGP, ISIS pro IPv6
59	BFD pro BGP, OSPFv2, OSPFv3, ISIS
60	Policy based routing / filter based routing
61	Multicast
62	IGMP snooping v1/2/3
63	IGMP v1/2/3
64	PIM SM/SSM/DM
65	MSDP
66	Podpora IPv6 Multicast (MLDv1 & v2)
67	Podpora IPv6 Multicast (PIM SM)
68	Podpora IPv6 Multicast (PIM SSM)
69	MPLS
70	Hardwarová podpora MPLS
71	LDP / RSVP signalizace
72	RSVP ping path
73	RSVP-TE (FRR, Link/node protection)
74	L2VPN
75	VPLS LDP based
76	VPLS BGP based
77	L3VPN (RFC 4364)
78	Mcast in L3VPN - draft Rosen
79	Podpora Label Imposition a Label Disposition (MPLS Provider Edge)
80	Podpora Label Swapping (MPLS Provider Core)
81	Podpora LDP (Label Distribution Protocol)
82	Podpora MPLS TE
83	Podpora P2MP TE
84	Podpora mLDP
85	Podpora IPv6 over MPLS (6PE)
86	Podpora IPv6 VPN over MPLS (6VPE)
87	Bezpečnost
88	Policing / rate limit pro provoz směrem k CPU
89	ACLka na provoz směrem k CPU
90	Podpora IPv6 ACL
91	Podpora reverse path check (uRPF) v hardwaru
92	ACL pro IP
93	Bezstavová Kontrola / Hlavní provozu L2-L7 (tzv. ACLka)
94	ACLka v HW (TCAM / CAM)
95	Port ACLka (vstup / výstup)

Podpis/signature:……

96	VLAN (Bridge) ACLka (vstup / výstup)
97	Routed ACLka (vstup / výstup)
98	Policing pod interface
99	CoS
100	Klasifikace provozu
101	802.1p
102	DSCP
103	IP precedence
104	MPLS exp.
105	Zaručeno na bezstavovém vyhodnocení paketů v L2-L4
106	Port shaping / Queue shaping
107	Policing
108	Minimálně 8x Queues na port
109	Minimálně 8x forwarding class
110	Minimálně 4 priority per Scheduler
111	Strict priority implementace
112	WRED
113	Rewrite rules – přepsání CoS bitů
114	Podpora IPv6 QoS
115	Vysoká dostupnost
116	Forwarding známých paketů bez asistence „control plane"
117	Management
118	Modulární operační systém
119	Command line interface (CLI)
120	Minimálně 10 konfiguračních úloh přímo na zařízení s možností jejich návratu příkazem z CLI
121	Aktivní a „batch" konfigurace = změny se promítnou do funkce až po potvrzení = časované změny, masivní změny naráz atd
122	Archivace konfigurací do souborů přímo na boxu
123	Archivace konfigurací na vzdáleném FTP / SCP – i automatická
124	Local přístup do CLI přes konsole port
125	Management zařízení Telnet / SSH
126	FTP, TFTP client a server
127	Podpora NETCONF
128	Syslog
129	Centralizovaná autentikace pro přístup na zařízení Radius/Tacacs+
130	Omezení práv přístupu dle uživatelských rolí
131	Možnost omezení přístupu k managementu (SSH, SNMP)
132	Konfigurační soubory v čitelném formátu (například ASCII, TXT, XML)
133	Možnost nahrání/zálohování konfigurace zařízení po síti pomocí alespoň jednoho z protokolů TFTP, FTP, HTTP, SCP nebo SFTP
134	Možnost povýšení operačního systému zařízení po síti pomocí alespoň jednoho z protokolů TFTP, FTP, HTTP, SCP nebo SFTP

135	Secure Shell (SSHv2)
136	Podpora centrální autorizace příkazů prostřednictvím protokolu TACACS+ nebo RADIUS
137	Out-of-Band Management
138	Tx a Rx optical power monitoring (DOM)
139	Podpora synchronizace času protokolem NTP, minimálně verze 3
140	Podpora protokolů SNMPv2c, SNMPv3 (včetně schopnosti generovat trapy při detekci významných událostí) a syslog.
141	Podpora SNMPv2c/v3 Mills a traps
142	Možnost omezit oprávněné zdrojové IP adresy manažerských stanic pro vzdálený konfigurační přístup
143	Možnost omezit oprávněné zdrojové IP adresy SNMP manažerských stanic
144	Network Management a monitoring
145	Port mirroring
146	Real-time performance monitoring
147	Netflow v9 IPFIX RFC 3917, 3955 nebo obdobné
148	Ping / traceroute
149	Debug na úrovni protokolů interface a procesů
150	NTP klient
151	DNS klient
152	Podpora internich nástrojů pro debugging prochazejícího provozu
153	Podpora internich nástrojů pro on-line měření kvality síťové infrastruktury
154	Vylcm
155	Minimální propustnost jednoho kusu 80Gbps
156	Rozšiřující rozhraní
157	Minimálně 2x 10GE s volitelným fyzickým rozhraním
158	Minimálně 20x 1GE SFP s volitelným fyzickým rozhraním
159	Interface moduly (převzetí vlnovou délku a přesný počet modulů zadavatel stanoví v objednávce)
160	Minimálně 1x 10GE Multimode SR optický modul (original od výrobce)
161	Minimálně 1x 10GE SingleMode LR optický modul (original od výrobce)
162	Minimálně 1x 10GE SingleMode ER optický modul (original od výrobce)
163	Minimálně 1x 10GE DWDM SingleMode optický modul C Band Tunable (100-GHz ITU grid)
164	Minimálně 1x 10GBASE-AWDM 1550XX nm (100-GHz ITU grid)
165	Minimálně 1x 1GE Multimode SX optický modul (original od výrobce)
166	Minimálně 1x 1GE Singlemode LX/LH optický modul (original od výrobce)
167	Minimálně 1x 1GE Metalický modul s konovkou RJ45(original od výrobce)
168	Servisní a doplňkové požadavky
169	Záruka a prodloužená podpora min. 5 let
170	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zaškolení
171	Veškeré licence SW potřebné ke specifikovanému řešení
172	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

30	IEEE 802.1
31	IEEE 802.1p
32	IEEE 802.1Qau
33	RFC 951, 1542 BootP
34	L3 Funkce
35	RVI (Routed VLAN Interface)
36	Layer 3 features (IPv4)
37	Static Routing
38	Route maps
39	Dynamické směrovací protokoly (OSPF, BGP, ISIS)
40	Podpora BFD
41	Podpora VRRP /HSRP nebo podobné
42	VRF-lite (multicast, unicast)
43	DHCP Relay (RFC 3046)
44	Podpora IPv6 v HW - bez impactu
45	RFC 768 UDP
46	RFC 791 IP
47	RFC 792 ICMP
48	RFC 793 TCP
49	RFC 826 ARP
50	RFC 894 IP over Ethernet
51	RFC 1122 Host requirements
52	RFC 1256 IPv4 ICMP Router Discovery (IRDP)
53	RFC 1519 Classless Interdomain Routing (CIDR)
54	RFC 1812 Requirements for IP Version 4 routers
55	ICMP
56	Multicast features
57	IGMP v2/v3 (RFC 3376)
58	Anycast RP
59	PIM-SM
60	Static RP
61	Security and ACL
62	Secure interface login and password
63	Ingress and Egress ACLs: allow and deny. Port ACLs, VLAN ACLs, Routed ACLs
64	Local proxy Address Resolution Protocol (ARP)
65	Static ARP support
66	Storm Control, Port error disable and auto-recovery
67	Control Plane denial-of-service (DoS) protection
68	Port Security
69	Traffic Storm Control
70	Unicast RPF
71	Control Plane Policing

7.2.2 KDC - L2/L3 přepínač

Počet ks v jedné lokalitě: 2

Počet lokalit celkem (12 lokalit KDC bez fce CDC): 12

- Tento vysokorychlostní přepínač bude využíván jako centrální komunikační prvek v KDC a bude zajišťovat datové propojení s ostatními DC. Do každého KDC bude dodáváno ve dvou instancích pro zajištění požadované redundance řešení.

7.2.2.1 Závazné parametry:

č.	Hardware
1	Nebloknjící architektura přepínacího subsystému (wire speed)
2	Velikost IRU
3	Latence pod 2mikro sekundy
4	Propustnost minimálně 1,28 Tbps
5	Přepínací systém minimálně 960 Mpps
6	FCoE na všech portech
7	Minimálně 48 portů 1/10GE/FCoE s volitelným fyzickým rozhraním
8	Minimálně 4 porty 40GE/FCoE s volitelným fyzickým rozhraním
9	Možnost konverze 40GE rozhraní na 4x 10GE rozhraní s podporou FCoE
10	Podpora standardu TRILL nebo ekvivalentní technologie
11	Možnost výměny napájecích zdrojů za provozu (hot-swap) bez ovlivnění funkce zařízení jako celku
12	Bezvýpadkový upgrade přepínače (ISSU)
13	Redundantní napájení (zařízení musí být schopno plné funkce při poruše jednoho napájecího zdroje)
14	Možnost výměny ventilátorů za provozu (hot-swap) bez ovlivnění funkce zařízení jako celku (N+1)
15	L2 Funkce
16	Podpora IEEE 802.1Q minimálně 4K VLAN
17	Port Based VLAN
18	Podpora filtrování MAC adres
19	Možnost definování statické MAC adresy na port
20	Podpora statické Link Agregace
21	Podpora protokolu LACP (IEEE 802.3ad)
22	Podpora protokolu LLDP (IEEE 802.1AB)
23	Podpora Jumbo Frame minimálně 9K bytes
24	Podpora protokolu Spanning Tree (IEEE 802.1D)
25	Podpora protokolu Rapid Spanning Tree (IEEE 802.1w)
26	Podpora protokolu Multiple Spanning Tree (IEEE 802.1s)
27	Podpora Spanning Tree BPDU Protect, BPDU Filtering, Loop Protect, Root Protect
28	Uplink Failure Detection
29	Podpora MC-LAG

72	Rate Limits
73	Quality of service (QoS)
74	Layer 2 QoS: classification, rewrite, queuing
75	Layer 3 QoS
76	Rate Limiting
77	Ingress policing: Irate2color - Egresspolicer,policermarkdownaction
78	8 hardware queues per port
79	Strict priority queuing (LLQ), DWRR
80	802.1p remarking
81	Layer 2 classification criteria: Interface, MAC address, Ethertype, 802.1p, VLAN,
82	Trust IEEE 802.1p/DSCP (ingress)
83	Remarking of bridged packets
84	Traffic Mirroring
85	Port-based
86	Možnost definovat směr zrcadleného provozu (vstupní/ výstupní)
87	Možnost zrcadlení celého LAG portu
88	VLAN-based
89	SPAN and RSPAN are supported
90	Minimálně 2 instance
91	Data center bridging (DCB)
92	PFC (Priority Flow Control) - IEEE 802.1Qbb
93	ETS (Enhanced Transmission Selection) - IEEE 802.1Qaz
94	DCBX (Data Center Bridging Exchange Protocol
95	IEEE 802.3x - Link-level flow control
96	FC-BB-5
97	Podpora technologie N-Port Identifier Virtualization (NPIV)
98	Management
99	Sériová konzole (RJ45)
100	USB port
101	Podpora správy přepínače přes NETCONF
102	Out-Of-band management
103	Podpora SSHv2
104	Podpora SNMPv2, SNMPv3
105	Podpora odesílání logů na syslog server
106	sFlow nebo NetFlow/IPFIX
107	Omezení práv přístupu dle uživatelských rolí
108	RFC 854 Telnet client and server
109	Podpora synchronizace času z centrálního časového serveru, NTP protokol
110	Možnost správy přepínače přes HTTP/HTTPS (GUI)
111	RFC 1492 TACACS+
112	RFC 2138 RADIUS Authentication
113	RFC 2139 RADIUS Accounting

114	Interface moduly (přesnou vlnovou délku a přesný počet modulů zadavatel stanoví v objednávce)
115	Minimálně 1x 10GE Multimode SR optický modul (originál od výrobce)
116	Minimálně 1x 10GE SingleMode LR optický modul (originál od výrobce)
117	Minimálně 1x 10GE SingleMode ER optický modul (originál od výrobce)
118	Minimálně 1x 1GE Multimode SX optický modul (originál od výrobce)
119	Minimálně 1x 1GE Singlemode LX/LH optický modul (originál od výrobce)
120	Minimálně 1x 1GE Metalický modul s koncovkou RJ45(originál od výrobce)
121	Minimálně 1x 10GE DAC kabel, délka 1m (originál od výrobce)
122	Minimálně 1x 10GE DAC kabel, délka 3m (originál od výrobce)
123	Minimálně 1x 10GE DAC kabel, délka 5m (originál od výrobce)
124	Minimálně 1x 40GE Multimode SR optický modul (originál od výrobce)
125	Minimálně 1x 40GE SingleMode LR optický modul (originál od výrobce)
126	Minimálně 1x 40GE DAC kabel, délka 1m (originál od výrobce)
127	Minimálně 1x 40GE DAC kabel, délka 3m (originál od výrobce)
128	Minimálně 1x 40GE DAC kabel, délka 5m (originál od výrobce)
129	Minimálně 1x 40GE na 4x 10GE DAC kabel, délka 1m
130	Minimálně 1x 40GE na 4x 10GE DAC kabel, délka 3m
131	Servisní a doplňkové požadavky
132	Záruka a produktová podpora min. 5 let
133	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zaškolení
134	Veškeré licence SW potřebné ke specifikovanému řešení
135	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

7.3 Specifikace komponent NSPTV

7.3.1 NSPTV - CE směrovač pro ZZS

Počet ks v jedné lokalitě: 2

Počet lokalit celkem (14xNSPTV ZZS, 1xGŘ HZS): 15

7.3.1.1 Závazné parametry:

č.	Základní vlastnosti
1	Třída zařízení směrovač
2	Formát zařízení modulární
3	Minimálně 3x 10/100/1000BaseT WAN port
4	Minimálně 4x 10/100BaseT portů
5	Podpora virtualizace směrovacích tabulek (VRF) minimálně 20
6	Minimální paketový výkon celého systému 200Kpps
7	Minimální propustnost systému 500Mbps / IMIX
8	Minimální počet route ve směrovací tabulce 16000

9	Minimální velikost Flash paměti 256 MB
10	Minimální velikost DRAM paměti 512 MB
11	Směrování IPv4
12	Směrování IPv6
13	Protokoly 2. vrstvy
14	IEEE 802.1Q (minimálně 16 VLAN)
15	IEEE 802.1X
16	Detekce protiklidného zařízení (např. LLDP)
17	Podpora "jumbo rámců"
18	Protokol IP
19	IP alias (více IP sítí na jednom rozhraní)
20	QoS
21	Random Early Detection (RED)
22	DHCP relay
23	router redundancy protokol (např. VRRP, HSRP)
24	Podpora GRE (Generic Routing Encapsulation)
25	Protokol IPv6
26	Podpora VRRP nebo ekvivalentní pro IPv6
27	Podpora IPv6 ACL
28	Podpora IPv6 QoS
29	Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP, DHCP)
30	Podpora IPv6 Multicast (MLDv1 & v2)
31	Podpora IPv6 Multicast (PIM SSM)
32	Podpora IPv6 Multicast (PIM SM)
33	Podpora OSPFv3
34	Podpora MP BGP
35	Podpora IS-IS pro IPv4 a IPv6
36	Podpora IPv6 MLDv2 snooping
37	Podpora IPv6 nástrojů pro měření kvality sítě (např. SLA, NQA)
38	Podpora IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels
39	Podpora IPv6 Tunneling: ISATAP Tunnel
40	Podpora DHCPv6 Relay
41	Podpora IPv6 dynamických VPN (např. DMVPN nebo ekvivalentní)
42	Podpora IPv6 VPN over MPLS (6VPE)
43	Podpora IPv6 firewall with statefull inspection
44	Šifrovací protokoly
45	Podpora IPSec VPN (3DES i AES 256)
46	Podpora IPSec NAT transparency
47	Podpora pre-fragmentace pro IPSec VPN
48	QoS
49	Podpora QoS classification – ACL, DSCP, MPLS EXP, CoS based
50	Podpora QoS marking – DSCP, MPLS EXP, CoS

51	Podpora QoS Shaping and Policing
52	Podpora Class Based and Priority queuing
53	Podpora Rate Limiting
54	Podpora Hierarchical Queuing Function
55	Směrovací protokoly
56	MPLS
57	BGPv4
58	BGP pro IPv6
59	OSPFv2, OSPFv3
60	OSPF s MD5 a NSSA
61	IS-IS
62	RIPv2
63	RIP pro IPv6
64	Policy-based routing podle ACL
65	Podpora detekce funkčnosti linky (např. BFD nebo funkčně ekvivalentní)
66	MPLS
67	MPLS
68	LDP (Label Distribution Protocol)
69	Podpora Label Edge Router (LER) funkce
70	MPLS VPN
71	MPLS TE
72	EoMPLS
73	Podpora QoS s využitím EXP bitů
74	Směrování multicastu
75	PIM (dense i sparse mód)
76	PIM pro IPv6
77	IGMPv2
78	IGMPv3
79	Bezpečnost
80	Statefull firewall
81	Podpora reverse path check (uRPF)
82	ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback)
83	ACL pro IP
84	ACL pro ethernetové rámce
85	IPSec VPN
86	Detekce nefunkčnosti protějšího IPSec směrovače (dead peer detection)
87	Dynamické sestavování IPSec VPN tunelů pro automatické vytváření full-mesh topologie
88	IPSec VPN bez potřeby vytvářet tunely
89	Podpora NAT/PAT
90	Podpora Static NAT
91	Management
92	CLI rozhraní

Příloha č. 8 zadávací dokumentace – Specifikace systémů NIS IZS a NSTPV

7	Minimálně na 24 rozhraních 300W PoE
8	Minimálně na 48 rozhraních 15,4W PoE
9	Dostupná provedení - minimálně následující varianty
10	48 portů 10/100/1000 PoE, 4 porty GE (SFP)
11	Výkonnostní parametry
12	Propustnost přepínacího subsystému 104Gbps
13	Protokoly fyzické vrstvy
14	Podpora standardu IEEE 802.3ad
15	Minimálně 24 konfigurovatelných portchannel skupin
16	Podpora IEEE 802.3ad přes více přepínačů ve stohu
17	Podpora "jumbo rámců"
18	Protokoly 2. vrstvy
19	IEEE 802.1D
20	IEEE 802.1Q
21	Podpora Private VLAN nebo ekvivalentní
22	Minimálně 1000 aktivních VLAN
23	IEEE 802.1x
24	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresa, Web-autentizace)
25	Podpora integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)
26	IEEE 802.1s - multiple spanning trees
27	IEEE 802.1w - Rapid Tree Spanning Protocol
28	Detekce protilehlého zařízení (např. CDP nebo LLDP)
29	Protokol pro definici tříských VLAN (např. GVRP nebo ekvivalentní)
30	Detekce jednosměrnosti optické linky (např. OAM link fault management nebo ekvivalentní)
31	STP root guard nebo ekvivalentní
32	STP loop guard nebo ekvivalentní
33	Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)
34	Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech
35	Protokol IP
36	Podpora IGMP snooping
37	Podpora IPv6 MLD snooping
38	Podpora IPv6 port ACL
39	Podpora IPv6 QoS
40	Podpora IPv6 RA guard
41	Podpora IPv6 source guard
42	Podpora DHCPv6 snooping
43	Podpora IPv6 ND inspection
44	QoS
45	Podpora QoS classification - ACL, DSCP, CoS based
46	Podpora QoS marking - DSCP, CoS

93	SSHv2
94	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
95	Ochrana control plane pomocí rate limiterů
96	SNMPv2
97	SNMPv3
98	Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní události v systému zařízení (např. Embedded Event Manager nebo ekvivalentní)
99	Integrovaný web management
100	Konzolový port pro management
101	NTP klient s MD5 autentizací
102	Administrátorem definovatelné monitory (sady statistik) sbírané o každém přenášeném paketu
103	Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)
104	Statistiky exportovatelné pomocí NetFlow v9 (nebo IPFIX/IEFC 3917, RFC 3955)
105	Nástroje pro měření dynamických parametrů a odezev v síti v libovolný okamžik, syntetické generovaným provozem (například IP SLA nebo ekvivalentní)
106	RADIUS klient pro AAA (autentizace, autorizace, accounting)
107	TACACS+ klient
108	Syslog
109	Služby
110	DHCP server
111	Servisní a dopočítkové požadavky
112	Záruka a produktová podpora min. 5 let
113	Montáž a zprovoznění (včetně instalace počátečných systémů např. management a pod.) včetně zahoření
114	Veškeré licence SW potřebné ke specifikovanému řešení
115	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

7.3.2 NSPTV - LAN přepínač

Počet ks v jedné lokalitě: 2

Počet lokalit celkem(14x NSPTV IZS, 14x NSPTV ZZS, 14x NSPTV PČR, 1x PP PČR, 1x GŘ HZS): 46

Lan přepínač je dodáván ve 2 instancích pro každé operační středisko NSPTV pro zajištění požadované redundance.

7.3.2.1 Závazné parametry:

č.	Základní vlastnosti
1	Třída zařízení přepínač
2	Formát zařízení pro instalaci do Racku maximální velikost 1RU
3	Možnost rozšíření o redundantní zdroj
4	Možnost stohování
5	Minimální počet zařízení ve stohu 8
6	Minimální kapacita sběrnice stohu 80Gbps

Podpis/signature:……

47	Podpora QoS Policing
48	Podpora QoS - Strict Priority Queue pro ukládání paketů IP telefonního provozu
49	Podpora rate limiting
50	Bezpečnost
51	ACL na rozhraní IN/OUT (včetně virtuálních - VLAN)
52	Možnost definovat povolené MAC adresy na portu
53	Možnost definovat maximální počet MAC adres na portu
54	Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)
55	Podpora bezpečnostních funkcí umožňujících ochranu proti podvržení zdrojové IP adresy - IP source guard nebo ekvivalentní
56	Podpora bezpečnostních funkcí umožňujících ochranu proti připojení neautorizovaného DHCP serveru - DHCP snooping nebo ekvivalentní
57	Podpora bezpečnostních funkcí umožňujících inspekci provozu protokolu ARP - ARP inspection nebo ekvivalentní
58	Podpora konsoových zařízení
59	Podpora IEEE 802.1af
60	Podpora IEEE 802.1at
61	Podpora IEEE 802.3az
62	Podpora automatické detekce IP telefonu připojeného k portu LAN přepínače a automatické nastavení vhodných QoS parametrů daného portu
63	Podpora inteligentního PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení
64	Podpora automatické detekce IP telefonu připojeného k portu LAN přepínače a jeho automatické přiřazení do dedikované voice VLAN
65	Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu
66	Management
67	CLI rozhraní
68	SSHv2
69	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
70	SNMPv2
71	SNMPv3
72	DNS klient
73	NTP klient s MD5 autentizací
74	RADIUS klient pro AAA (autentizace, autorizace, accounting)
75	TACACS+ klient
76	Port mirroring (SPAN)
77	Vzdálený port mirroring (RSPAN)
78	Syslog
79	Podpora interních nástrojů pro debugging procházejícího provozu
80	Monitorování aplikačních toků
81	Podpora monitorování aplikačních toků s využitím Sampled NetFlow nebo sFlow
82	Podpora monitorování aplikačních toků na fyzických i VLAN rozhraních

83	Možnost nastavení vzorkovací rychlosti
84	Interfaceové moduly (převzmou vlnovou délku a převzný počet modulů zadavatel stanoví v objednávce)
85	Minimálně 1x 1GE Multimode SX optický modul (original od výrobce)
86	Minimálně 1x 1GE Singlemode LX/LH optický modul (original od výrobce)
87	Minimálně 1x 1GE Metalický modul s konzovkou RJ45(original od výrobce)
88	Servisní a doplňkové požadavky
89	Záruka a produktová podpora min. 5 let
90	Montáž a zprovoznění (včetně instalace podpůrných systémů např. management a pod.) včetně zaškolení
91	Veškeré licence SW potřebné ke specifikovanému řešení
92	Součástí dodávky je i zajištění dokumentace specifikovaného řešení

8 Seznam obrázků

Obrázek 1 - Připojení CDC k ITS (ITS NGN), fyzická vrstva 5
Obrázek 2 - Připojení KDC k ITS (ITS NGN), fyzická vrstva 7
Obrázek 3 Připojení lokalit NPSTV k ITS (ITS NGN), fyzická vrstva 10
Obrázek 4 – Schéma zapojení CDC 17
Obrázek 5 - Schéma zapojení KDC 18
Obrázek 6 - Zapojení NPSTV HZS 19
Obrázek 7 - Zapojení NPSTV PČR a ZZS 20
Obrázek 8 - Zapojení NPSTV PČR a ZZS 21
Obrázek 9 VPN projektu NIS IZS 22

9 Seznam tabulek

Tabulka 1 - Harmonogram požadovaného připojení lokalit NIS IZS k síti ITS a ITS NGN 4
Tabulka 2 - Požadavky na připojení CDC 6
Tabulka 3 Přehled nároků na připojení KDC 10
Tabulka 4 – Tabulka adresace NPSTV 31

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

D. Harmonogram dodávek

Dokument obsahuje:	Metodika obchodního zajištění, harmonogram dodávek
Verze:	5.1b
Schválil za Dodavatele:	RNDr. Vladimír Přibramský
Datum:	17/4/2014

Obsah

01. Metodika dodavatelského zajištění 3
02. Harmonogram dodávek NIS IZS 4

01. Metodika dodavatelského zajištění

ČP OZ vystupuje vůči trhu v pozice veřejného zadavatele. Pro dodávku jednotlivých externě dodávaných komponent pro systém NIS IZS (tj. kromě dodávek, které budou realizovány in-house vlastními zaměstnanci ČP OZ, především aplikační SW systému NIS IZS) bude využito několik variant postupu nákupu:

První varianta je veřejná zakázka nadlimitní (dále „VZN") v souladu s platným Zákonem o Veřejných Zakázkách pro nadlimitní veřejné zakázky.

Druhá varianta je veřejná zakázka podlimitní (dále jen „VZP").

Třetí varianta je veřejná zakázka malého rozsahu (dále jen „VZMR").

Čtvrtá varianta je jednací řízení bez uveřejnění (dále jen „JŘBU"), která bude využita u technologií, u nichž bude prokázána technická jedinečnost.

Pátá varianta je pořízení technologií, které jsou volně dostupné a šiřitelné (tzv. Open Source).

Pro jednotlivé funkční bloky řešení bude zvolena odpovídající varianta nákupu / pořízení technologií. Všechny varianty nákupu budou předem projednány a schváleny dohledovým orgánem pro financování z prostředků EU (Centrum pro regionální rozvoj - CRR MMR), které trvá vždy cca 14 kalendářních dnů.

V harmonogramu (viz další kapitola) jsou již zahrnuty časové podsepnosti pro VZN, tj. ty, které budou časově nejnáročnější.

02. Harmonogram dodávek NIS IZS

V harmonogramu NIS IZS (viz Přílohy 1. a 2. části D – Harmonogram) jsou obsaženy změny postupových termínů i finálního termínu (posuny na pozdější termín – podle Dodatku č. 1. ke smlouvě NIS IZS). Jde o tyto dodávky:

- Dokončení a akceptace Prováděcího konceptu s výhradami – 31.10.2013
- Dokončení a akceptace Prototypu (SW) s výhradami – do 31.10.2013
- Vybavení Datových center – do 30.6.2014
- Operačních středisek – do 30.6.2014
- Pilotní instalace – od 1.7.2014 do 31.10.2014
- Plošná instalace – od 3.11.2014 do 28.11.2014
- Testování SW (vč. zátěžových testů) – od 2.12.2014 do 27.2.2015
- Závěrečné převzetí SW a HW – od 1.3.2015 do 29.5.2015
- Dodávka pro Hlavní město Prahu - od 3.11.2014 do 28.11.2014

V Přílohách 1. a 2. jsou obsaženy různé podoby harmonogramu:

Příloha 1. – harmonogram NIS IZS (jednoduchý)

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

E. Specifikace provozu

Dokument obsahuje:	Specifikaci provozního zajištění včetně vyčíslení nákladů, katalogu služeb a návrhu provozní smlouvy a návrh reportingu.
Verze:	5.1
Schválil za Dodavatele:	Tomáš Faško
Datum aktualizace:	30/10/2013

Obsah

1. Specifikace provozu 4
Koncept zajištění provozu 4
Model 1 – Úrovně provozu 4
První vrstva – Centrum podpory uživatelů 4
Druhá vrstva - Technická podpora 4
Třetí vrstva – Vývoj a rozvoj systému 5
Technické zázemí provozu 5
Specifikace předmětu provozu 5
Vyčíslení provozních nákladů Dodavatele 9
Tabulka 1: Náklady na provoz a údržbu NIS IZS 10
Návrh plánu obnovy 12
Tabulka 2: Plán obnovy koncových zařízení 12
Procesní zajištění provozu 13
Model 4 - Proces managementu problémů 18
Model 6 - Proces vyhodnocení změn systému 22
Model 7 - Proces řízení verzí 23
Model 9 - Proces managementu konfigurace 27
Model 10 – Schéma eskalace 28
2. Reporting 30
Výstupy o operátorech a jejich stavech 30
Výstupy o pracovištích a jejich stavech 30
Výstupy o volání a jejich stavech 30
Výstupy o událostech a jejich stavech 31
Výstupy o výkonnosti systému 31
Výstupy o monitoringu zátěže 32
Technický reporting 32

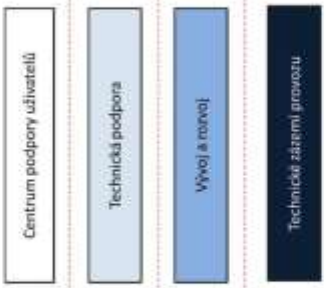
Příloha 1: Katalog služeb 34
Příloha 2: Smlouva o poskytování podpory 39
Rejstřík 62

1. Specifikace provozu

Koncept zajištění provozu

Provoz systému NIS IZS bude zajištěn třemi vrstvami podpory (třířovňový Servis desk).

Model 1 - Úrovně provozu



Mezi tyto vrstvy jsou rozděleny níže uvedené služby:

První vrstva – Centrum podpory uživatelů

První vrstva – Centrum podpory uživatelů je především úvodním kontaktním bodem Zadavatele; představuje první úroveň provozu Servis desku, tedy přijímá veškerá hlášení o incidentech a požadavky Zadavatele. Role úvodního kontaktu Centra bude platná hlavně pro operátory a standardní úkony. Mimo standardní úkony bude komunikace možná napřímo na všechny další úrovně, což bude klíčové při řešení havarijních stavů či rozsáhlých změn systému. Tyto kontaktní body budou specifikovány v rámci eskalačních procedur.
Na straně Dodavatele je tato vrstva zajištěna pracovníky, kteří komunikují přímo s uživateli a jsou schopni řešit některé incidenty, tj. uživatel v 98 % případů dostane potřebnou pomoc přímo od kontaktované osoby. Tím je zajištěna maximální rychlost podpory uživatelů.

Na této úrovni bude dále probíhat sběr požadavků na změnu a podnětů ke školení uživatelů.

Personálně je tato úroveň Servis desku zajištěna technickými pracovníky, kteří budou specializováni na komunikaci s uživateli, řešení jednoduchých incidentů a učení se řešení složitých, ale často se opakujících incidentů. To zajistí, že uživatelé dostanou v drtivé většině případů potřebnou podporu již při prvním kontaktu se Servis deskem.

Druhá vrstva - Technická podpora

Druhá vrstva - Technická podpora představuje druhou úroveň provozu Servis desku, tedy technicky odbornou část provozu. Na této úrovni jsou řešeny všechny kritické incidenty, prováděny pravidelné servisní a profylaktické práce, zpracovávány změnové požadavky.

provádena údržba vrstev HW a sítě jak systému NIS IZS, tak systému pro dohled provozu. Na úkonech vyžadujících součinnost bude tato vrstva aktivně komunikovat se Zadavatelem, a to jak v rámci eskalačních procedur, tak i během standardního řešení incidentů. Kontaktní matice bude součástí provozního řádu.

Dále jsou v rámci této vrstvy organizována školení.

Personálně je tato úroveň Servis desku složena především z následujících specializací – aplikační vrstva, HW, sítě, telefonie, nahrávání, databáze a GIS.

Pracovníci „experti na aplikační vrstvu" budou udržovat know-how o veškerém použitém SW. U SW se předpokládá udržování jeho aktuálnosti a řešení případných změnových požadavků. Pracovníci „experti na HW a síťovou vrstvu" pak budou udržovat v plné funkčnosti technické zázemí jak všech spravovaných systémů, tak systémů provozu jako takového.

V této vrstvě bude zároveň držena údržba aplikací a procesní vrstvy. Jelikož aplikační vrstva bude vytvořena převážně z opensource produktů, budou v rámci struktur Dodavatele k dispozici potřební specialisté pro jejich údržbu. Toto je jednou z klíčových aktivit zajištění provozu, protože to zaručí relativní nezávislost a nahraditelnost podpory od skupin podporujících použité opensource produkty.

Třetí vrstva – Vývoj a rozvoj systému

Třetí vrstva – Vývoj a rozvoj systému – zajišťuje základní činnosti spočívající ve výkonu věceprací spojených se změnovými požadavky a opravami zásadních chyb systému.

Personálně bude zajištěna především pracovníky, resp. specialisty sdílenými napříč projekty Dodavatele. Sdílení napříč strukturami Dodavatele zajistí maximální technickou aktuálnost a připravenost těchto specialistů a zařazení na projekty pak jejich pro-projektový přístup a odbornost. Zároveň budou udržovat maximální aktuálnost know-how napříč všemi závislými systémy.

Technické zázemí provozu

Technické zázemí provozu Servis desku pro výše popsané vrstvy není předmětem realizace projektu NIS IZS. Toto bude vybudováno v rámci jiného projektu s cílem zajistit podporu uživatelů i technickou podporu dalších systémů a služeb. V rámci technického zázemí je především aplikace provozu organizace Dodavatele a infrastruktura, na které tato aplikace běží. Aplikace pak bude obsahovat zejména technický monitoring provozovaného systému. Vzhledem k velikosti systému se bude jednat o standardní tržní řešení, které bude přizpůsobeno potřebám systému NIS IZS. Skrze tato aplikaci bude probíhat především automatická identifikace chyb a závad, tyto chyby a závady budou přímo propagovány jako incidenty do druhé úrovně Servis desku. Zároveň bude systém provozu jako hlavní analytický nástroj pro zjišťování příčin incidentů a jejich následné řešení.

Časová dostupnost služeb – které poběží v režimu 7 x 24, které 5 x 8 a které budou prováděny periodicky (například x týdně) je specifikována v Příloze 1 – Katalog služeb tohoto dokumentu.

Specifikace předmětu provozu

Dodavatel bude zabezpečovat provoz, dohled, podporu a údržbu celého systému po dobu 5 let od data předání a převzetí do ostrého provozu. Za tímto účelem bude mezi Dodavatelem

a Zadavatelem uzavřena zvláštní smlouva, která bude hrazená mimo strukturální fondy Evropské unie. Předmětem podpory a provozu je poskytování expertní kontroly, podpory a administrace systému v produkčním prostředí, odstraňování nefunkčních stavů a konfigurační úpravy.

Provozní služby budou poskytovány v následujícím rozsahu:

Pravidelné servisní a profylaktické práce

- Provozování systému monitoringu a zázemí provozu
- Monitoring systému
- Pravidelná periodická kontrola funkčnosti produkčního prostředí
- Diagnostika a optimalizace LDAP serveru
- Správa definovaných aplikačních rolí
  - Zajištění administrativního rozhraní pro správu uživatelů
  - Zajištění administrativního rozhraní pro správu pravidel
  - Zajištění administrativního rozhraní pro správu procesů
  - Úprava rolí
  - Úprava pravidel
  - Úprava procesů
- Pravidelné servisní odstávky částí provozovaného systému bez vlivu na produkční provoz z důvodu provedení profylaktických prací na svěřených technologiích
  - Čištění logů
  - Defragmentace diskových polí
  - Defragmentace databází
  - Optimalizace výkonu
- Kontrola a údržba diskového prostoru
- Zálohování systému
- Zálohování dat
- Obnova konfigurace systému ze záloh
- Replikace – export dat dle sjednaných pravidel
- Kontrola systémových a aplikačních logů
- Analýza systémových a aplikačních logů
- Kontrola spuštěných procesů IS
- Zajištění telefonních služeb dle sjednaných podmínek
  - Zajištění telefonie v rámci NIS IZS
  - Zajištění zasílání SMS v rámci interních procedur systému
- Vedení elektronického provozního deníku
- Vedení kompletní provozní dokumentace

- Poskytování pravidelných reportů o průběhu provozu
- Poskytování reportů o průběhu provozu na vyžádání
- Správa systémových prostředků pro zajištění standardního provozu
- Administrátorské práce IS dle dokumentace výrobce

Centrum uživatelů a řešení incidentů

- Provoz centra podpory uživatelů
  - Zajištění všech definovaných možností komunikace uživatelů s Centrem
  - Udržování technické aktuálnosti Centra
- Zpracování a řešení zjištěných incidentů
  - Příjem a prvotní analýza incidentů
  - Eskalace incidentů dle eskalačních pravidel
  - Pravidelný reporting nad řešenými incidenty
  - Reporty nad řešenými incidenty na vyžádání
- Analýza řešených problémových situací systémů a aplikací a eskalace objevených závad
- Poskytování konzultací
- Řešení akutních požadavků Zadavatele při havarijních stavech a velkých zátěžích systému

Zajištění technické aktuálnosti

- Administrace produkčního prostředí
- Pravidelná aktualizace provozní dokumentace dodavatelem provozované technologie
- Správa aktualizací a oprav provozovaného SW vydávaného výrobcem
  - Sledování aktualizací a oprav provozovaného SW vydávaných výrobcem
  - Testování aktualizací a oprav před instalací do produkčního prostředí
  - Doporučení nasazení opravných patchů a aktualizací Zadavateli
  - Instalace Zadavatelem schválených aktualizací a oprav do produkčního prostředí
- Zpracování zprávy o využívání HW, SW a systémových zdrojů s doporučením změn systémových zdrojů a optimalizací výkonu

Školení uživatelů Zadavatele

- Zajištění školicích prostor
- Udržování vzdělanosti klíčových uživatelů
- Školení nových uživatelů
- Školení nových funkcionalit při změnách systémů

Zajištění dostupnosti

- Dodržování smluvně zakotvených reakčních dob
- Zabezpečení stability klíčových parametrů systému
  - Předání rozhovoru na rozhraní
  - Zakončení události
  - Provedení automatické identifikace
  - Provedení automatické lokace GSM
  - Provedení automatické lokalizace pevné linky
  - Přehrání úvodní hlášky
  - Zajištění jazykové podpory pro EN/DE
  - Zajištění jazykové podpory pro vybrané jazyky
  - Zajištění systémové jazykové podpory
  - Zobrazení spectrik zvláštního účastníka
  - Čas vyhledání volného operátora
  - Rychlost vizualizace oblasti volání v GIS
  - Rychlost překreslování polohy v GIS
  - Čas předání hovoru v NSPTV
  - Rychlost předání hovoru PHQ
  - Čas hledání v místopisu (omezené)
  - Čas hledání v místopisu (neomezené – 3 znaky)
  - Rychlost odezvy aplikace pro příjem TV
  - Rychlost vizualizace události pro ostatní operátory NSPTV
  - Čas vyžádání součinnosti (tech. prodleva)
  - Rychlost předání události do OR na rozhraní
  - Čas do vyhledání nejbližšího objektu podle polohy v GIS
  - Rychlost provádění výpočtů v GIS

Rozvojové práce

- Přijetí požadavků na rozvojové práce
- Vstupní analýza požadavku na rozvojové práce
- Drobné rozvojové práce v celkovém rozsahu do 20 člověkodní ročně

- Detailní analýza požadavků na rozvojové práce
- Projekt rozvoje systému
- Akceptační řízení
- Převedení produkčního systému do stavu po změně

Infrastruktura

- Zajištění dostupnosti systému provozu
- Zajištění uživatelské bezpečnosti
  - Pravidelné penetrační testy

Podpora koncových stanic

- Zajištění příjmu požadavků a oznámení problémů koncových stanic
- Zajištění a provádění technické analýzy požadavků ke koncovým stanicím
- Provádění rozvojových prací
- Instalace koncových zařízení
- Podpora a servis tiskáren
- Opravy chyb na koncových zařízeních

Specifikace služeb je uvedena v Příloze č. 1 Katalog služeb provozu.

Vyčíslení provozních nákladů Dodavatele

Vyčíslení provozních nákladů Dodavatele shrnuje následující tabulka v členění personální a technické náklady (všechny finanční hodnoty jsou uvedeny v tis. Kč bez DPH).

Dodavatel bude provoz zajišťovat tak, aby nebyla ohrožena udržitelnost projektu NIS IZS spolufinancovaného z IOP.

Tabulka 1: Náklady na provoz a údržbu NIS IZS

Náklady na provoz a údržbu NIS IZS			
Personální			
Pozice	**Počet**	**Měsíční náklad [tis. Kč]**	**Roční náklad [tis. Kč]**
Vedoucí pracovník	1	100	1 200
Pracovník call centra	8	60	5 760
Technický pracovník	13	80	12 480
Technické			
Element			**Roční náklad [tis. Kč]**
Podpora HW – platby třetím stranám (viz bod 6. níže)			9 500
Podpora SW – platby třetím stranám (viz bod 7. níže)			3 000
Podpora provozu – aplikační vrstva (viz bod 11. níže)			3 000
Podpora provozu – vrstva HW (viz bod 11. níže)			2 000
Podpora tiskáren (viz bod 12. níže)			875
Další provozní náklady Dodavatele			1 500
Telefonní			
Pronájem linek ISDN (90 ISDN linek - viz bod 9. níže)			3 240
Celkem			**42 555**

Kalkulace vychází z následujících předpokladů:

1) Datová centra budou umístěna v lokalitách HZS Plzeň, HZS Olomouc a Olšanská 4 (Praha 3 - Žižkov).
2) Pronájem prostor a napájení racků je plně hrazeno HZS v rámci vlastních objektů, v rámci objektu Olšanská 4 (Praha 3 - Žižkov) je hrazeno Ministerstvem vnitra bez přefakturování k tíži HZS.
3) Veškerý HW bude vysoutěžen se zárukou na dobu 5 let, nezáruční opravy a obnova jsou zajištěny a hrazeny přímo Zadavatelem bez finanční účasti Dodavatele.
4) Předpokládá se vysoutěžení veškerého HW se zárukou na dobu 5 let. Požadavek, aby pětletá záruka nezvýšila pořizovací cenu, bude zajištěn takovým postupem veřejné zakázky, který byl již v jedné veřejné zakázce (otevřené nadlimitní) schválen kontrolní autoritou (ÚOHS). V dalších veřejných zakázkách bude tento postup zopakován.
5) Při provozu NIS IZS bude využita mimo jiné infrastruktura pro podporu provozu (dohled a jiné) a tato infrastruktura bude na technické úrovni v maximální účinné míře sdílena napříč projekty. Provozní náklady této sdílené infrastruktury budou rovněž sdíleny napříč projekty.

6) Platby třetím stranám v rámci podpory HW jsou náklady na rozšířenou podporu, která bude hrazena v rámci provozu. Předpokládá se tedy vysoutěžení veškerého HW se zárukou na dobu 5 let a dokoupení (v rámci provozu) rozšířené podpory na zařízení, kde základní záruka nebude vyhovující.

7) Platby třetím stranám v rámci podpory SW je odhad cen licencí za licencované produkty. Tento odhad počítá s předpokladem, že vývoj je veden vlastními silami Dodavatele nad převážně open source komponentami.

8) Kombinace vyšších personálních nákladů, vedlejších nákladů a nákladů na platby třetím stranám pokrývá veškerý servis a podporu. U servisního zásahu jsou dvě možnosti – buď zařídí vyřešení problému externí subjekt, jenž je za tuto rozšířenou podporu placen, nebo problém vyřeší sami zaměstnanci Dodavatele. V tom případě jsou veškeré náklady na jejich práci zahrnuty v jejich personálních nákladech a vedlejších nákladech.

9) Poplatky za odchozí volání do VTS budou hrazeny Dodavatelem a přefakturovány Zadavateli podle skutečnosti. Jejich konkrétní výše není v této kalkulaci zahrnuta ani odhadem (velký rozptyl). Fixní poplatky za konektivitu do VTS činí 3 000 Kč měsíčně za 1 ISDN linku, přičemž těchto je počítáno max. 90. Tento počet se může snížit na základě analýzy reálné maximální zátěže NSPTV.

10) Záložní připojení a s ním spojené náklady jsou hrazeny přímo Zadavatelem. Tato funkcionalita nebyla Zadavatelem požadována a je řešena mimo projekt NIS IZS.

11) Dohled nad systémem NIS IZS bude Dodavatel realizovat na vlastní platformě dohledu a Servis desku. Tato platforma není financována z projektu NIS IZS, avšak v rámci provozu bude na její běh Zadavatel přispívat. Odhad výše příspěvku je uveden v tabulce v položkách Podpora provozu – aplikační vrstva a Podpora provozu – vrstva HW.

12) Náklady na plnou podporu a servis tiskáren (včetně doplňování tonerů) odhadl Dodavatel benchmarkové jako cca dva tisíce korun měsíčně za jednu tiskárnu (bez doplňování papíru). V rámci tabulky jsou však personální náklady vedeny mimo, takže Dodavatel očekává náklad na plnou podporu tiskáren bez doplňování papíru na necelý jeden tisíc korun měsíčně na jednu tiskárnu. Náklady na papír budou rozúčtovány po jednotlivých subjektech dle jejich spotřeby. Tiskáren je v rámci projektu počítáno 74.

13) Položky *Podpora HW – platby třetím stranám* a *Podpora HW – platby třetím stranám* jsou odhadem cen na základě benchmarku. Celkové náklady za pětileté období činí 25% z celkové odhadované pořizovací ceny, tzn. 5% z pořizovací ceny ročně.

14) Personální náklady jsou počítány jako kompletní náklady na danou osobu, tedy nákladv pouze náklady mzdové, ale také náklady režijní, náklady na dovolenou, a dále náklady a udržování vzdělanosti daného zaměstnance. I přesto se však jedná spíše o hrubé odhady, protože Dodavatel očekává vysokou fluktuaci ve mezích mezi zaměstnanci na obdobné úrovni vzdělením k nárokům na množství specializací, které jsou potřebné pro zajištění provozu systému NIS IZS.

15) Vzhledem k faktu, že výběrová řízení nebyla doposud realizována, se v následující kalkulaci jedná o předběžné hrubé odhady, které jsou všechny

Návrh plánu obnovy

Plán obnovy je zde navržen jako pro období po vypršení záruk na koncová zařízení, tj. pro na dobu po skončení doby udržitelnosti (5 let). Do té doby budou náklady Zadavatele na obnovu zařízení koncových stanic minimální až nulové, protože případná závada / nefunkčnost bude řešena v rámci záruky nebo rozšířené podpory (v rámci paušálních provozních nákladů - podpora HW).

Plán obnovy je založen na očekávané životnosti a poruchovosti nakupovaných komponent. Zajištění obnovy navrhuje Dodavatel formou vytvoření skladu v období následujícím po 5 leté záruce. Sklad navrhuje Dodavatel doplňovat v rámci investičních nákladů Zadavatele, všechny položky v něm pak nepřetržitě majetkem Zadavatele. To Zadavatelů zajistí plnou kontrolu nad nakupovanými položkami a eliminuje veškeré majetkové a legislativní problémy. Pro účely skladu jsou náklady na obnovu vypočteny v průměru na rok, konkrétní naplánování do let je pak věcí především rozpočtových a veřejně-soutěžních možností Zadavatele.

Speciální kategorií je spotřební zboží, které nebude Dodavatel nijak zajišťovat mimo první dodávku v rámci projektu. Toto se týká jediné položky a to náhlavní soupravy, jež je považována za spotřební zboží. Tyto nejsou zahrnuty do plánu obnovy, protože zde není z pozice Dodavatele možná předlůice.

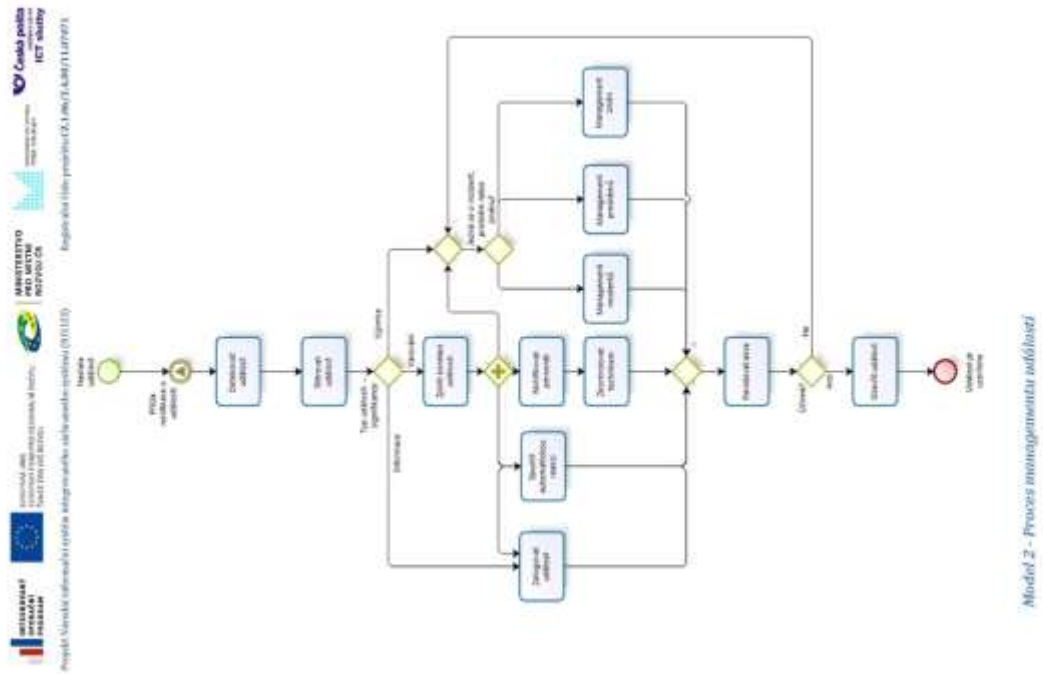
Tabulka odhadu plánu obnovy pro koncová zařízení je uvedena níže:

Tabulka 2: Plán obnovy koncových zařízení

	Plán obnovy					
Zařízení	Očekávaná cena za kus [Kč]	MTBF[1] (hodiny)	Statistická průměrná životnost (roky)	Průměrná roční obnova	Průměrné roční náklady na obnovu [Kč]
Displej	7 500	40 – 60 000	7-10	69	517 500
Myš	200	50 – 200 000	3-7	39	7 800
Klávesnice	350	30 – 60 000	3-4	56	19 600
Mini PC	17 500	175 000	5-7	33	577 500
IP telefon	4 500	100 000	7	28	126 000
Celkem					**1 248 400**

Tabulka obnovy předpokládá vytížení zařízení o 30 % nižší než pro standardní dobu životnosti na základě skutečnosti, že na operačních střediscích nejsou neustále vytížena všechna pracoviště. Náhlavní soupravy jsou chápány jako spotřební zboží Zadavatele a jsou tedy mimo tuto kalkulaci.

[1] MTBF =mean time between failure – střední doba mezi poruchami



Model 2 - Proces managementu událostí

V případě, že by Zadavateli nevyhovovalo vytvoření vlastního skladu pro zajištění obnovy zařízení koncových stanic po vypršení doby udržitelnosti, navrhuje Dodavatel jako alternativu, že sklad vytvoří on a nabídne ho Zadavateli jako službu.

Obnova ostatních prvků než zařízení koncových stanic, zejména serverů a sítě, není momentálně predikovatelná. Vzhledem k tomu, že bude vše Dodavatelem vysoutěženo se zárukou na 5 let, do uplynutí těchto pěti let bude obnova prakticky nulová a po jejich skončení až absolutní. Tuto obnovu však nelze vzhledem k časovému horizontu a neznámosti finálních technologií predikovat, bude tedy nezbytné provést analýzu obnovy teprve poté, kdy se doba udržitelnosti bude chýlit ke svému konci. Pro zjištění stavu bude v rámci Servisní smlouvy dohodnut postup k vytvoření analýzy stavu systému ke konci doby udržitelnosti. Tato analýza zjistí skutečný stav HW a vybavení koncových stanic a poskytne tak ucelený obraz, jaké investice budou po vypršení doby udržitelnosti potřeba.

Procesní zajištění provozu

Služby provozu budou zajištěny standardizovanými procesy. Základní procesy budou:

- Management událostí
- Management incidentů
- Management problémů
- Management změn
- Vyhodnocení změnových požadavků
- Řízení verzí
- Validace a testování
- Management konfigurace
- Základní schéma eskalace

Pro zajištění dostatečné kvality jednotlivých procesů a služeb budou následně vytvořeny eskalační procedury a popsány jednotlivé kroky interakce mezi Zadavatelem a Dodavatelem. Zcela podrobně bude tato možné předložit teprve po konkretizaci finálně použitých technologií. Součástí služby je rovněž implementace SW nástroje pro podporu funkcí Servis desk a procesů Incident, Konfigurace, Problém a Managementu změn, včetně potřebných eskalací. Konkretizace procesu eskalací proběhne až při specifikaci provozního řádu systému. V tomto dokumentu je tedy přiloženo pouze jednoduché eskalační schéma.

Management událostí

Management událostí bude následovat tento proces:

Proces začíná tím, že se v rámci provozovatelského systému stane něco neobvyklého a systém provozu vygeneruje notifikaci. Tato notifikace je pracovníkem ve službě prověřena skrze její detekování a filtraci. Tyto kroky zjistí problémové místo a jednoznačně určí událost – zda se například nejedná o opakující se událost či již známý problém, nebo se například jedná o neškodný následek po změně či pouze informační notifikaci. V tomto bodu dojde k rozhodnutí, jestli se jedná informační notifikaci, varování nebo výjimku. Podle této filtrace je spuštěn další sled akcí.

Informace a varování jsou zalogovány, u varování je však navíc zjištěna možná korelace (zda notifikace nesouvisí s již známými událostmi), dále je pak spuštěna automatická reakce, pokud je pro tento typ notifikace nastavena a je notifikován personál, z jehož řad to technik následně zkontroluje. Zároveň je u varování spuštěn stejný proces jako výjimky – notifikace je klasifikována, jestli se jedná o incident, problém nebo následek změny. V každém z těchto tří případů je pak událost postoupena do příslušného procesu.

Nakonec jsou akce zrevidovány, kdy je především zkontrolováno vyřešení události. Je-li událost vyřešena, je následně uzavřena a proces končí. Není-li událost vyřešena, je postoupena zpět do klasifikace, jestli se jedná o incident, problém nebo následek změny.

Proces managementu incidentů začíná zjištěním incidentu. Ten může přijít buď po jedné z komunikačních linek – Hotline, fax, email, webový formulář nebo z procesu managementu událostí. Následně je incident identifikován, zalogován a kategorizován.
Pokud se jedná o požadavek na rozvojové práce, tak tyto jsou v tomto bodě postoupeny do vlastního procesu.

Pokud se jedná o skutečný incident, je tento prioritizován – tedy určena míra jeho kritičnosti. V případě, že se jedná o kritický incident, je tento okamžitě posunut do svého procesu.
U standardního incidentu je následně provedena úvodní analýza, na jejímž základě může být incident eskalován. Eskalace probíhá dle potřeby buď na další úrovně podpory a/nebo na vedení provozu jako takového.

Následně je incident prošetřen, diagnostikován, vyřešen a systém je obnoven. Detailní podprocesy diagnostiky, řešení incidentů a obnovy budou stanoveny až při zavádění provozu jako takového – momentálně z důvodů neexistence provozního systému jako takového není tato přesná specifikace možná. Po obnově systému je pak incident uzavřen.

Proces managementu problémů začíná výskytem problému. Tato informace může přijít z mnoha míst, především:

- Přímo od Servis desku
- Z procesu managementu incidentů
- Z procesu managementu událostí
- Z proaktivního vyhledávání problémů
- Od Zadavatele

V každém případě je problém neznámým nežádoucím stavem systému, který způsobuje incidenty. V každém případě, po zjištění možného problému je tento detekován, zaloguován, kategorizován a prioritizován, čímž je zajištěna plná klasifikace problému pro pozdější účely a až poté je přistoupeno k řešení problému samotného.

Toto řešení začíná vyšetřením a diagnostikou problému, přičemž zde dochází k přímé interakci se systémem managementu konfigurace. Následně je zjištěna možnost či existence workaroundu – tedy dočasného překlenutí období s problémem. Workaround zabrání dalšímu vzniku incidentů, ale problém jako takový neřeší. V každém případě je vytvořen záznam o chybě a ten odeslán do databáze známých chyb.

Následně je vyhodnoceno, jestli je pro vyřešení problému nezbytná změna systému. Pokud ano, je problém eskalován do změnového managementu a pak, v každém případě, je postoupen k řešení. Pokud se řešení problému podaří, je problém uzavřen; pokud nikoliv tak je problém posunut zpět do fáze diagnózy hledání workaroundu. Po uzavření problému je problém revidován, pokud se jednalo o problém zásadní – například dočasná ztráta funkcionality, jejíž opravení vyžadovalo rozsáhlou změnu.

Proces managementu změn systému začíná potřebou na změnu. Ta může vzniknout buď skrze přání Zadavatele, nebo z ostatních procesů, zejména procesu managementu problémů.

V každém případě však je požadavek na změnu zaevidován, je provedena vstupní analýza, ve které jsou vyhodnoceny dopady požadavku na změnu plus jeho očekávaná pracnost a tedy náklady na provedení a návrh harmonogramu až do ukončení implementace. Následně je tato analýza prezentována Zadavateli, který se rozhodne, zdali se cestou změny vydá. Pokud se rozhodne, že nikoliv, tak je požadavek postoupen k přehodnocení straně, která ho původně vytvořila. Na základě vlastního přehodnocení je buď zcela zavřen, nebo je přepracován. Nový požadavek na změnu je pak podstoupen ke schválení dané straně. Při neschválení se proces vrací k jeho přehodnocení (stále stranou, jež s ním původně přišla).

Tento upravený požadavek je opět postoupen přes evidenci, analýzu a prezentaci do bodu schválení. V případě neschválení se celý proces opakuje, v případě schválení je požadavek posunut do fáze projektu změny. Tento projekt je standardně řízen projektovým manažerem, začíná od převzetí schválené úvodní analýzy a končí až implementací do ostrého provozu. Implementace je pak zpětně vyhodnocena a celý proces změny je tímto uzavřen.

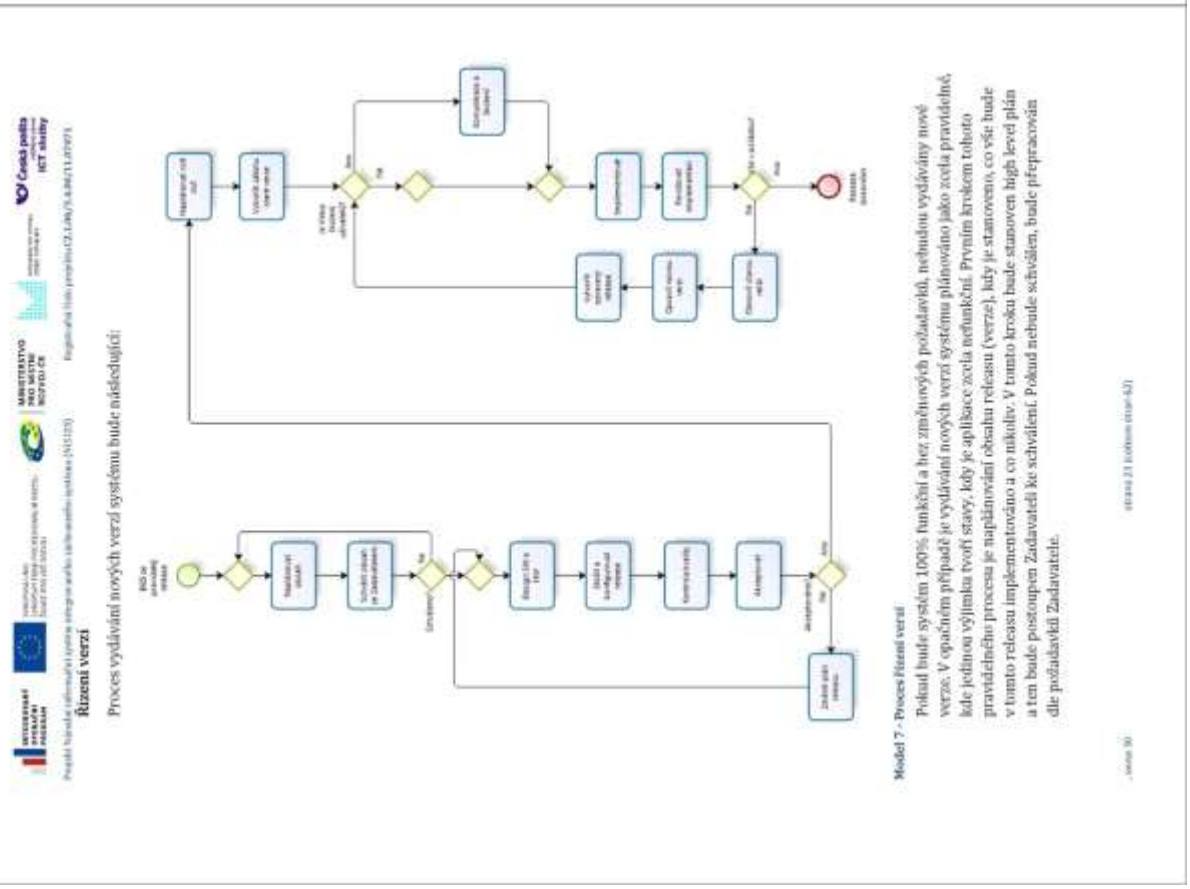
V případě pěti marných pokusů o schválení změnového požadavku bude problém eskalován na vyšší úroveň řízení projektu (Řídící výbor nebo jiný odpovídající).

Model 6 – Proces vyhodnocení změn systému

Ačkoliv je tento proces jednoduchý, je pro dlouhodobý provoz systému klíčový. S časovým odstupem od provedení samotné změny je třeba tuto změnu vyhodnotit. To proběhne tak, že bude shromážděna dokumentace týkající se změny – jak původní změnová dokumentace, tak dokumentace z realizačního projektu, tak provozní dokumentace z období po implementaci. Na základě srovnání a vyhodnocení této dokumentace je pak vyhodnocena změna jako taková. Vyhodnocení změny, což je hlavním dokumentárním výstupem tohoto procesu, je pak předáno Zákazníkovi k jeho potřebám.

Po schválení nějakého plánu releasu přejde proces do technicky detailní roviny, kde bude naplánován design SW a HW a především jejich změn vzhledem k danému releasu.
Po designu bude tento skožen a konfigurován do podoby, která by již měla být implementována. Nad tímto detailním konceptem proběhne akceptace za účasti Zadavatele, kde se finálně vyladí, že tuto novou verzi chce. Při neakceptování přejde proces zpět k designu SW a HW.

Po akceptaci dojde již k samotné implementaci, bude tedy naplánován roll out, vytvořena záložní stará verze a - pokud bude třeba - budou proškoleni uživatelé k používání nové funkcionality. Následně bude nová verze implementována a implementace vyhodnocena. V případě vzniku problému bude v nejkratším možném termínu obnovena stará verze, dále bude opravena nová verze a vytvořeno opravené vydání (tzv. release patch). To přejde zpět do procesu před možné školení uživatelů a tato smyčka se bude opakovat, dokud nebude implementace realizována bez problémů.

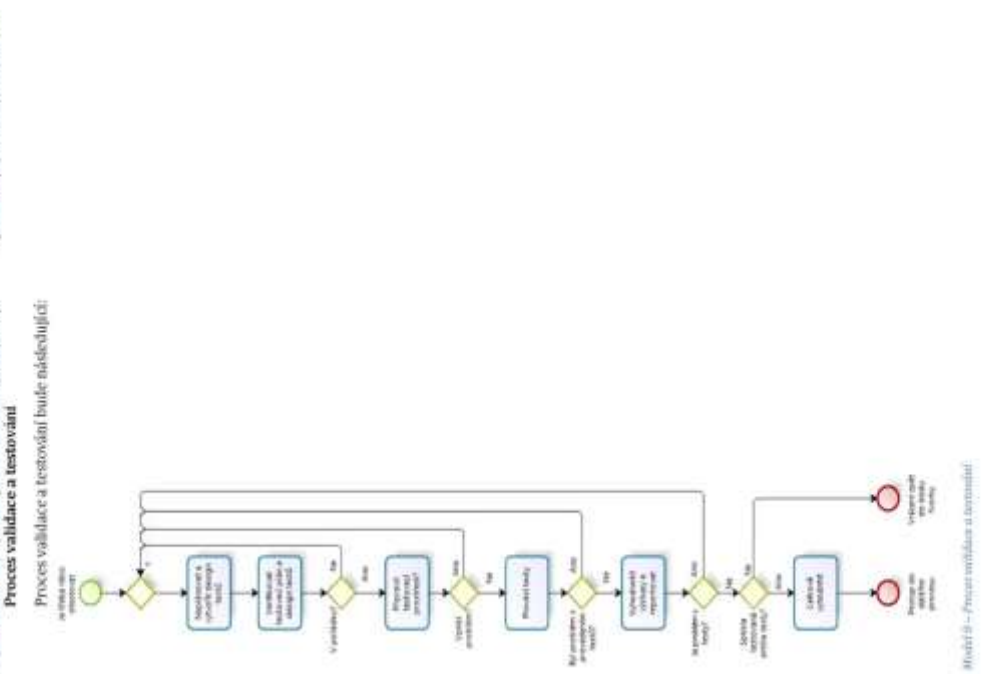


Model 7 - Proces Řízení verzí

Pokud bude systém 100% funkční a bez změnových požadavků, nebudou vydávány nové verze. V opačném případě je vydávání nových verzí systému plánováno jako zcela pravidelné, kde jedinou výjimku tvoří stavy, kdy je aplikace zcela nefunkční. Prvním krokem tohoto pravidelného procesu je naplánování obsahu releasu (verze), kdy je stanoveno, co vše bude v tomto releasu implementováno a co nikoliv. V tomto kroku bude stanoven high level plán a ten bude postoupen Zadavateli ke schválení. Pokud nebude schválen, bude přepracován dle požadavků Zadavatele.

Proces validace a testování

Proces validace a testování bude následující:

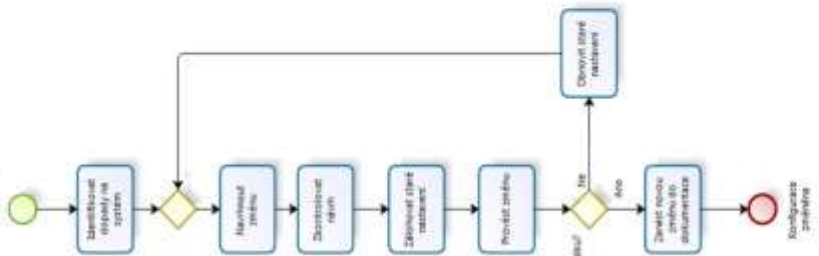


Zjednodušený proces validace a testování bude začínat designem testovacích scénářů a naplánováním samotných testů. Scénáře a plán pak budou jako celek verifikovány a v případě, že budou vyhovovat potřebám, budou postoupeny k přípravě testovacího prostředí. Pokud bude problém s konfigurací testovacího prostředí, vrátí se proces zpět na začátek.

Když nebude problém zjištěn, přejde se k samotnému testování. Pokud bude problém se samotnou realizací testů, vrátí se proces na začátek. V opačném případě budou výsledky testů postoupeny do vyhodnocení. V rámci vyhodnocení bude nejprve zkontrolováno, zda nebyl problém s koncepcí testů jakožto takovou (např. nebyla otestována některá klíčová část). Pokud zde nebude problém, bude zjištěno, jestli testovaná entita prošla nebo neprošla testy. Pokud neprošla, bude vrácena zpět do své vlastní tvorby. Pokud prošla a je vše v pořádku, jsou testy finálně celkově vyhodnoceny a výsledek je postoupen do návazných procesů.

Proces managementu konfigurace

Proces bude následující:

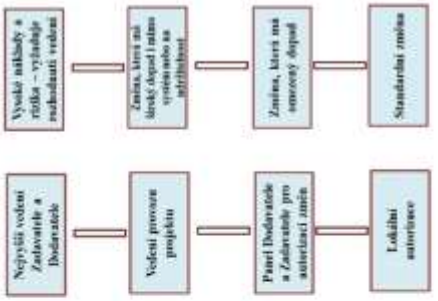


Model 9 – Proces managementu konfigurace

Tento proces bude neustále běžet v pozadí téměř všech ostatních procesů. Změny v konfiguraci nebudou prováděny náhodně, ale budou probíhat podle přesné procedury, v jejímž rámci bude zabráněno vzniknutí dezorganizaci nebo nedostatku v dokumentaci systému. Před každou změnou konfigurace budou nejprve identifikovány dopady na systém, teprve až na základě identifikace bude případně navržena změna. Tento návrh bude interně zkontrolován a před jeho implementací bude vytvořena záloha staré konfigurace. Až poté bude samotná změna provedena, přičemž pokud se zde vyskytne problém, bude systém okamžitě obnoven do stavu před změnou a celý proces změny konfigurace poběží znovu od začátku. Až poté, co bude implementována změna, a nebudou zjištěny problémy, bude změna náležitě zanesena do provozní technické dokumentace.

Schéma eskalace

Schéma eskalace je následující:



Model 10 – Schéma eskalace

Základní schéma eskalace počítá se čtyřmi úrovněmi rozhodování – lokální autorizace, panel Zadavatele a Dodavatele pro autorizaci změn, vedení provozu projektu a nejvyšší vedení Zadavatele a Dodavatele. Lokální autorizace je technické oddělení provozu. To bude mít v kompetenci standardní změny, které nemají širší dopady. Panel pro autorizaci změn bude obsahovat nejen technické pracovníky provozu NIS IZS, ale také z ostatních projektů (v případě potřeby) a zástupce Zadavatele. Tento panel bude rozhodovat o změnách, které budou mít omezený dopad i na ostatní systémy nebo významnější dopad na systém NIS IZS. Změny, které budou mít rozsáhlé dopady i mimo systém NIS IZS nebo na udržitelnost

2. Reporting

Reporting bude poskytován jak aplikační, tak technický. Reporty budou poskytovány napříč lokalitami a úrovněmi uživatelů. Pro uživatele budou poskytovány na těchto úrovních:

- Lokalita NSPTV dané složky IZS – úroveň NSPTV kraj/složka IZS (složková krajská úroveň)
- Lokalita NSPTV složek IZS pro daný kraj – úroveň NSPTV kraj (krajská úroveň)
- Všechna NSPTV složky IZS v České republice – úroveň NSPTV republika/složka IZS (složková centrální úroveň)
- Všechna NSPTV všech složek IZS v České republice – úroveň NSPTV republika/složky IZS (centrální úroveň)

Výstupy (reporty) systému budou poskytovány vždy za stanovené období a ve stanovených termínech (v případě pravidelných reportů), jejich dostupnost bude zajištěna z vnitřku aplikace i online. Reporty budou pravidelně archivovány. V rámci podpory automatizace reportingu a chybových stavů bude umožněna vizualizace výstupů za pomoci služeb GIS.

Reporty budou poskytovány především o:

- Operátorech NSPTV a jejich stavech
- Pracovištích a jejich stavech
- Volání a jejich stavech v rámci celého procesu od přijetí hovoru v systému do bodu ukončení hovoru
- Událostech a jejich stavech
- Výkonnosti systému
- Monitoringu zátěže
- Technickém monitoringu

Výstupy o operátorech a jejich stavech
Základní reportované veličiny výstupů NSPTV v této oblasti bude doba setrvání operátorů v jednotlivých stavech (doba aktivity, odhlášení od systému, opuštění systému apod.).

Výstupy o pracovištích a jejich stavech
Základními reportovanou veličinou výstupů NSPTV v této oblasti budou setrvání pracovišť v jednotlivých stavech.

Výstupy o volání a jejich stavech
Základními sledovanými veličinami výstupů NSPTV v této oblasti jsou:

projektu NIS IZS jako takovou, budou v kompetenci samotného vedení provozu na straně Dodavatele a věcného gestora projektu na straně Zadavatele. Extrémní změnové případy, které potenou vysoká rizika či finanční nároky, budou eskalovány až na samotné nejvyšší vedení Zadavatele a Dodavatele. Detailní eskalační procedury budou definovány samostatným dokumentem před uvedením systému do ostrého provozu.

- Počty přijatých tísňových volání:
  - Na operátora NSPTV
  - Na lokalitu (kraj, celá ČR, sousední stát, celkem)
    - Na složku
    - Na jednotlivé tísňové linky
    - Z pevné sítě, z mobilní sítě
    - Bez SIM karet
    - Připojených hovorů na složku IZS z pracoviště NSPTV v horizontálním směru a vertikálním směru
    - Dle vyžádané jazykové podpory
    - Zdroj volání (dle mobilních operátorů)
  - Počet odchozích hovorů mimo složky IZS
    - Dle tel. čísla volajícího
    - Dle tel. čísla volaného
  - Evidence stavů volání:
    - Počet volajících čekající ve frontě
    - Počet zodpovězených volání (volání, u kterých volající úspěšně dosáhl systému NSPTV)
    - Délky hovorů v návaznosti na operátory NSPTV, lokality NSPTV a typu události

Výstupy o událostech a jejich stavech

V této oblasti budou reportovány především následující veličiny:

- Počty událostí:
  - Přijatých
  - Předaných složkám IZS
  - Dle lokality
  - Dle typu
- Evidence stavů událostí:
  - Kdo a kdy se podílel na zpracování události
  - Délka zpracování události na operátora NSPTV, na lokalitu NSPTV, dle typu události

Výstupy o výkonnosti systému

Základními sledovanými veličinami výstupů NSPTV v této oblasti jsou data z technického monitoringu.

Výstupy o monitoringu zátěže

Základními sledovanými veličinami výstupů NSPTV v této oblasti jsou data z monitoringu zátěže.

Technický reporting

Systém bude umožňovat práci s chybovými hlášeními přímo na pracovištích, resp. aplikaci NSPTV ve všech lokalitách:

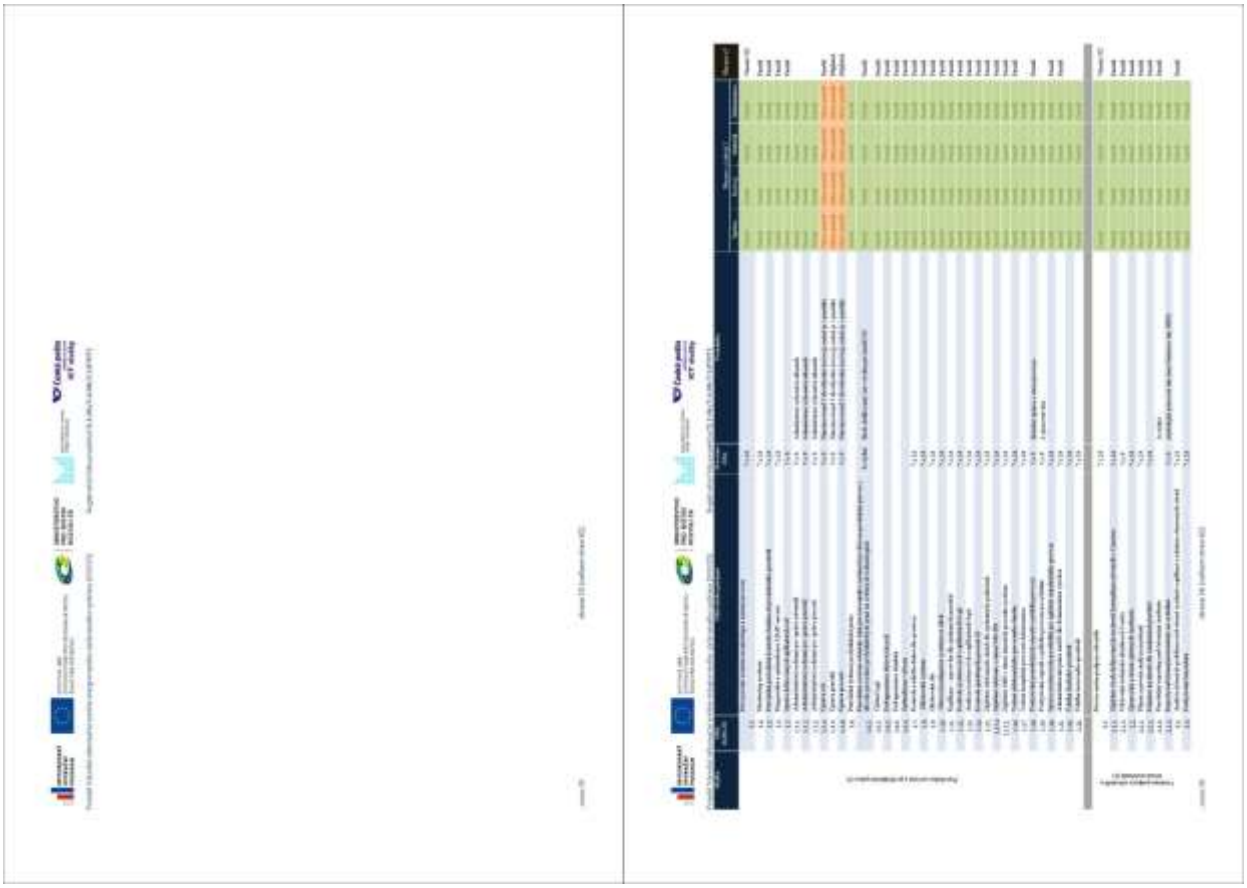
- Jednoznačný identifikátor chybového hlášení pro úroveň:
  - Jedno NSPTV v kraji a pro složku IZS
  - NSPTV v kraj pro všechny složky IZS
  - Všechna NSPTV pro vybranou složka IZS (HZS, PČR, ZZS kraji)
  - Všechna NSPTV pro všechny složky IZS
- Založit chybové hlášení s povinnými údaji:
  - Kraj
  - Složka IZS
  - Operátor složky IZS (jmenovitě, dle evidovaných rolí v systému)
  - Termín založení chybového hlášení
  - Termín výskytu chyby
  - Klasifikace chyby – určuje operátor
  - Příloha (např. snímek obrazovky)
  - Textový popis chyby
  - Textový popis řešení chyby
  - Subjekt, osoba zodpovědná za řešení chyby
- Evidovat chybová hlášení včetně historického kontextu
- Nabízet do evidovaných chybových hlášení dle filtru, filtr budou kombinovatelné a v základní verzi obsahovat:
  - Složku IZS
  - Území – kraj, republika
  - Úroveň kraj, republika
  - Období od-do
  - Období od-do (termín založení)
  - Platné, neplatné chybové hlášení
  - Operátor (jmenovitě), který hlášení založil
  - Stav řešení
  - Možnost editace již založeného hlášení garantem NSPTV (složka IZS/kraj)

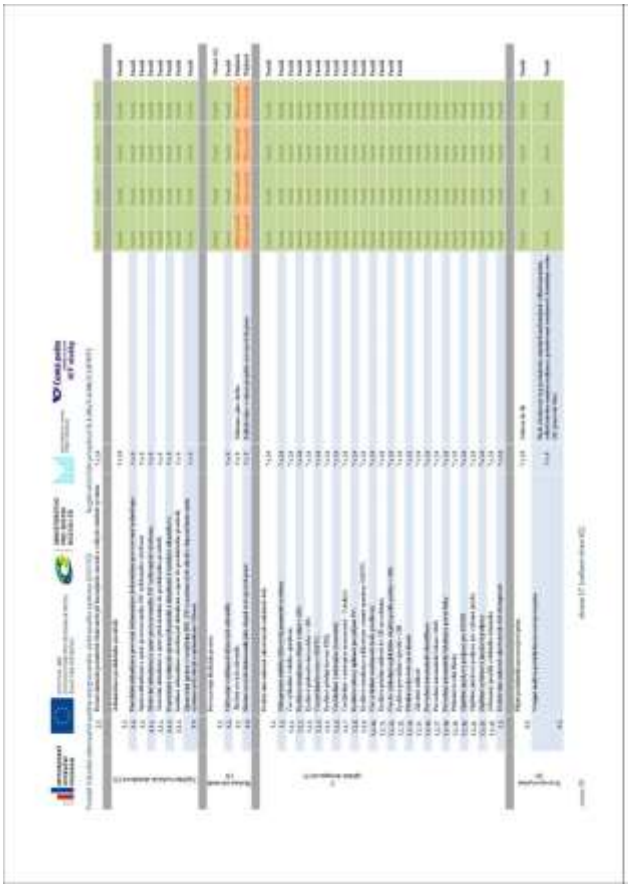
- Zajišťovat statistiku chybových hlášení
  - Operátor NSPTV (jmenovitě)
  - Složka IZS
  - Území – kraj, republika
  - Termín od –do (založení - uzavření)
  - Úroveň nahlášené chyby (klasifikace)
- Umožnit sloučení dvou chybových hlášení bez ztráty kontinuity předchozího řešení chybového hlášení
- Tisk chybových hlášení
- Export chybového hlášení s přenosem vně systému
- Možnost přístupu k chybovým hlášením i z úrovně OŘ složky IZS (pracoviště OŘ).

Přílohy

Příloha 1: Katalog služeb

Viz Příloha č. 1, část E – Provoz (samostatný dokument).





Příloha 2: Smlouva o poskytování podpory

Česká pošta s.p., Odštěpný závod ICT služby

Olšanská 1951/4

13000 Praha 3, Žižkov

jednající .....

IČ : 47114983

DIČ: CZ47114983

bankovní spojení: Československá obchodní banka, a.s.

č. účtu: 117404973/0300

vedenou u rejstříkového soudu v Praze, oddíl A, vložka 7565

(dále jen „Poskytovatel")

a

Česká republika - MINISTERSTVO VNITRA

Nad Štolou 936/3, 170 34, Praha 7

Zastoupená

MINISTERSTVEM VNITRA-generálním ředitelstvím Hasičského záchranného sboru České republiky,

Kloknerova 2295/26, 148 01, Praha 414

jednající .....

IČ: 00007064

DIČ: CZ 00007064

(dále jen "Objednatel")

(Objednatel a Poskytovatel dále jednotlivě jen „Smluvní strana" a společně jen „Smluvní strany")

uzavřeli tuto Smlouvu o poskytování podpory v souladu s ustanovením § 269 odst. 2 zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů

(dále jen "Smlouva")

Smluvní strany vědomy si svých závazků v této Smlouvě obsažených a v úmyslem být touto Smlouvou vázány, dohodly se na následujícím znění Smlouvy:

DEFINICE POJMŮ

Pro účely této Smlouvy se níže uvedenými pojmy rozumí:

- „Systém NIS IZS" nebo „Informační systém" je systém dodávaný v rámci projektu CZ.1.06/3.4.00/11.07071 – NIS IZS.
- „Smlouva" tato Smlouva o poskytování podpory uzavřená mezi Objednatelem a Poskytovatelem, podepsaná osobami oprávněnými zavazovat Smluvní strany, včetně jejích případných dodatků.
- „Údržbou a podporou" systému NIS IZS služby, které jsou vymezeny v Příloze č. 2 Smlouvy.
- „Požadavkem Objednatele" jakákoli objednávka nebo žádost o změnu, úpravu, rozvoj, nebo opravu systému oblášená Objednatelů v souladu s nastavenými komunikačními pravidly.
- „Kritickou chybou" taková vada systému, jež způsobí úplné zastavení systému, nebo zasáhne systém tak, že celek či jeho část již není použitelný tak, že nemohou být prováděny kritické procesy Objednatele.
- „Kritickým procesem" takové činnosti, na kterých je závislá základní funkčnost systému NIS IZS a není možné je vykonat alternativním způsobem v požadovaném čase (např. odeslání žádosti o součinnost).
- „Havarijní situací" nebo „Havárií" takový okamžik, kdy systém vykazuje kritickou chybu.
- „Člověkodnem" výkon práce jednoho člověka po dobu 7,5 hodiny.

1. **PREAMBULE**

1.1. Poskytovatel prohlašuje, že je právnickou osobou řádně založenou a existující podle českého právního řádu a že splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2. Objednatel prohlašuje, že splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

2. **PŘEDMĚT SMLOUVY**

2.1. Poskytovatel se touto Smlouvou zavazuje poskytovat Objednateli služby spočívající v provozu, dohledu, úplné podpoře a údržbě systému NIS IZS Objednatele podle Přílohy č. 2 této Smlouvy (dále jen "Podpora") a Objednatel se na základě Smlouvy zavazuje Poskytovateli uhradit cenu za řádné a včas poskytnutou úplnou Podporu ve výši a způsobem sjednaným v této Smlouvě. Dodavatel se zavazuje při poskytování podpory postupovat tak, aby byly udrženy výstupy projektu NIS IZS spolufinancovaného z Integrovaného operačního programu, a to po dobu minimálně 5 let od ukončení realizační fáze projektu NIS IZS. Jednotlivé objednávky a Požadavky Objednatele, jejichž periodicita není ošetřena smluvně, budou přijímány prostřednictvím Centra podpory uživatelů (dále jen „CePU") v souladu s Přílohou č. 3 této Smlouvy

2.2. Poskytovatel se zavazuje všechny Požadavky Objednatele evidovat. Výpis Požadavků Objednatele a zprávu o tom v jakém stavu se nachází jejich řešení, bude Poskytovatel měsíčně předávat Objednateli.

2.3. Objednatel se touto Smlouvou zavazuje vyvinout součinnost stanovenou v článku 11.

2.4. Rozsah podpory může být dohodou smluvních stran a v souladu s právními předpisy dodatečně rozšířen. Poskytovatel takovou změnu neodmítne, je-li to v jeho provozních možnostech a úspěšně proběhne vyjednávání mezi Objednatelem a Poskytovatelem o změně ceny. Rozšířit rozsah podpory lze i písemným přijetím písemné objednávky Oprávněnými osobami.

3. MÍSTO A DOBA PLNĚNÍ

3.1. Nestanoví-li Smlouva jinak, jsou místem plnění sídlo a souvislé lokality Objednatele. Poskytovatel je oprávněn některé služby, jejichž charakter umožňuje plnění prostřednictvím vzdáleného přístupu, poskytovat prostřednictvím vzdáleného přístupu, které zajistí Objednatel.

3.2. Poskytovatel je povinen poskytovat Podporu dle Smlouvy ode dne nabytí účinnosti Smlouvy do doby ukončení její platnosti, minimálně však po dobu 5ti let.

4. CENA A PLATEBNÍ PODMÍNKY

4.1. Uvedené ceny jsou maximálními a nejvýše přípustnými. Veškeré ceny uváděné v této Smlouvě jsou bez započtení sazby DPH, která bude vypočtena na základě platných právních předpisů.

4.2. Cena za poskytování Podpory se stanoví jako cena smluvní a je stanovena následovně:

4.2.1. Cena za poskytování služeb za každý rok shrnuje následující cenová kalkulace:

Předmět	Roční platba (tis. Kč)
Podpora a koncových stanic	XXX
Zajištění infrastruktury	XXX
Zajištění dostupnosti	XXX
Zajištění školení	XXX
Zajištění technické aktuálnosti	XXX
Centrum podpory uživatelů a řešení incidentů	XXX
Pravidelné servisní a profylaktické práce	XXX

4.2.2. Celková cena za dobu účinnosti Smlouvy činí xxx xxx tis. Kč bez započtení ceny zvláště placených prací prováděných na základě požadavku Objednatele dle Přílohy č. 2.

4.2.3. Cena za práce provádělné na základě Požadavků Objednatele definované v kapitole 3 Přílohy č. 2 této Smlouvy typu „Rozvojové práce" bude stanovena vždy na základě vstupní analýzy požadavku.

4.3. Objednatel se zavazuje cenu za poskytování služeb hradit zpětně za předchozí kalendářní měsíc. Pravidelná měsíční platba bude hrazena paušálně (služby uvedené v bodu 4.2.1.) na základě pravidelných reportů o provozu odsouhlasených oběma Smluvními stranami.

4.4. Platby se hradí na základě faktur – daňových dokladů vystavených Poskytovatelem vždy do 15. dne následujícího kalendářního měsíce. Přílohou každé faktury bude pravidelný report o provozu.

4.5. Cena je splatná v korunách českých (Kč), a to na základě faktur vystavených Poskytovatelem v souladu s pravidly uvedenými v ustanovení 4.1 až 4.3 Smlouvy.

4.6. Lhůta splatnosti všech faktur činí třicet (30) kalendářních dní ode dne jejich doručení povinné Smluvní straně. Faktura se považuje za doručenou též, bylo-li její převzetí odepřeno, nebo pokud se jí nepodařilo doručit pro nepřítomnost adresáta, ač byla zasílána na adresu sídla Objednatele uvedenou v této Smlouvě nebo dodatečně Objednatelem oznámenou jako změna sídla, a to třetí den po jejím prokazatelném odeslání.

4.7. Každá faktura vystavená na základě Smlouvy musí mít náležitosti daňovému dokladu vyžadované právními předpisy, zejména ustanovením § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Pokud nebude faktura obsahovat stanovené náležitosti nebo nebude obsahovat povinnost nebo dohodnutou náležitost nebo bude-li chybně vyúčtována cena nebo DPH, je Objednatel oprávněn vrátit ji Poskytovateli ve lhůtě pěti (5) kalendářních dnů od jejího doručení Objednateli s uvedením chybějících náležitostí nebo nesprávných údajů. V případě, že Objednatel fakturu vrátí, přestože faktura byla vystavena řádně a předepsané náležitosti obsahuje, lhůta se nestaví a pokud Objednatel fakturu nezaplatí v původním termínu splatnosti, je v prodlení.

4.8. Peněžité částky se platí bankovním převodem na účet druhé Smluvní strany uvedený v záhlaví této Smlouvy. Dojde-li ke změně čísla tohoto účtu, tato skutečnost bude druhé Smluvní straně oznámena. Povinnost příslušné Smluvní strany bude splněna dnem odepsání příslušné částky z účtu Smluvní strany.

4.9. Případná náhrada škody bude zaplacena v české měně, přičemž pro přepočet na českou měnu je rozhodný kurz České národní banky ke dni vzniku škody.

5. PRÁVO UŽITÍ

5.1. V případě, že je výsledkem poskytování služeb Podpory dílo, které podléhá ochraně podle zákona č. 121/2000 Sb., o právech autorských, právech souvisejících s právem autorským a o změně dalších zákonů (autorský zákon), v platném znění, a nebyly pro takové dílo písemně sjednány jiné podmínky licence, získá Objednatel k takto vytvořenému dílu jako celku i k jeho jednotlivým částem oprávnění k výkonu práva jej užít (licenci), a to jako licenci nevýhradní, nepřenosnou, territoriálně omezenou územím České republiky a na dobu využívání díla. Poskytovatel je povinen každý takový případ písemně doložit a Objednateli na takový případ upozornit. To platí i ohledně veškerých technických řešení, koncepcí, know-how, postupů či metod zpracování dat, analytických nástrojů, software, pracovní dokumentace, diagramů, schémat a konceptů, pokud jsou vyvinuty Poskytovatelem při poskytování Podpory dle této Smlouvy a nemají charakter autorského díla.

5.2. Smluvní strany se dohodly, že cena za licenci k dílu dle odst. 5.1 této Smlouvy je již zahrnuta v ceně za poskytování Podpory na základě této Smlouvy.

6. KVALITA PLNĚNÍ

6.1. Poskytovatel nese odpovědnost za to, že Podpora bude poskytována tak, aby vyhovovala potřebám Objednatele, se kterými byl Poskytovatel seznámen. Podpora bude poskytována s náležitou odbornou péčí a prostřednictvím osob, které mají potřebnou kvalifikaci i zkušenosti k plnění svých úkolů.

6.2. Poskytovatel se zavazuje, že reakční doba v případě havarijních situací bude dodržena v souladu s pravidly definovanými v Příloze č. 4 této smlouvy.

7. **OPRÁVNĚNÉ OSOBY**

7.1. Každá ze Smluvních stran jmenuje Oprávněnou osobu. Oprávněné osoby budou zastupovat Smluvní stranu ve smluvních, obchodních a realizačních záležitostech souvisejících s plněním této Smlouvy.

7.2. Jména oprávněných osob jsou uvedena v Příloze č. 1 této Smlouvy. Smluvní strany jsou oprávněny jednostranně změnit oprávněné osoby, jsou však povinny na takovou změnu druhou Smluvní stranu písemně upozornit, jinak nemá vůči druhé Smluvní straně právní účinky. V případě změny oprávněných osob není nutné uzavírat ke Smlouvě dodatek.

8. **ODPOVĚDNOST ZA ŠKODU**

8.1 Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných právních předpisů a této Smlouvy.

8.2 Žádná Smluvní strana neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany. Žádná ze Smluvních stran není odpovědná za nesplnění svého závazku v důsledku prodlení druhé Smluvní strany nebo v důsledku nastalých okolností vylučujících odpovědnost (§ 374 Obchodního zákoníku).

8.3 Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují vyvíjet maximální úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

8.4 Každá ze Smluvních stran je oprávněna požadovat náhradu škody i v případě, že se jedná o porušení povinností, na kterou se vztahuje smluvní pokuta, a to v části přesahující smluvní pokutu.

8.5 V případě poškození systému z důvodu působení vyšší moci nebo z důvodu nedostatečného zabezpečení prostor Objednatele, ve kterých je umístěna technologie, nenese na tomto Poskytovatel žádnou vinu, a tedy na něj nebudou uplatněny žádná penále či sankce. Vyřešení situace a obnovení funkčnosti systému bude probíhat ve spolupráci Poskytovatele s Objednatelem.

9. **SANKCE**

9.1. Smluvní strana je v prodlení s plněním nepeněžitého závazku, jestliže nesplní řádně a včas svůj závazek, který pro Smluvní stranu vyplývá ze Smlouvy anebo platných právních předpisů.

9.2. Dojde-li k prodlení Poskytovatele s plněním z důvodů neležících na jeho straně nebo na straně jeho subdodavatelů, prodlužují se adekvátně tomuto prodlení lhůty k poskytnutí plnění nebo jeho ucelených částí.

9.3. Objednatel je oprávněn požadovat po Poskytovateli smluvní pokutu v případě porušení povinnosti dodržet lhůtu řešení požadavku dle Přílohy č. 6 této Smlouvy.

9.4. Pokud je vada předmětu plnění závěrečná neznalost konečného uživatele, je řešení zahájeno v době dle tabulky v Příloze č. 4 této smlouvy, avšak v případě neodvratení termínu zahájení řešení nebo průběhu řešení nebudou uplatňovány příslušné sankce.

9.5. Zaplacením jakékoliv sjednané smluvní pokuty není dotčeno právo poškozeného na náhradu škody a nezbavuje povinnou smluvní stranu povinnosti splnit své závazky.

9.6. Pro případ prodlení se zaplacením peněžité částky je Smluvní strana oprávněna požadovat smluvní pokutu za každý i započatý den prodlení ve výši 0,05% z dlužné částky, s níž je Smluvní strana v prodlení. Tím není dotčeno právo Smluvní strany na uplatnění náhrady škody.

9.7. Smluvní strana, která poruší povinnosti vyplývající z této Smlouvy ohledně ochrany důvěrných informací je povinna zaplatit druhé Smluvní straně smluvní pokutu ve výši 100.000,- Kč (slovy: sto tisíc korun českých) bez DPH za každé závažné porušení takové povinnosti, a to do patnácti (15) dnů ode dne doručení faktury vystavené na její uhrazení. Tím není dotčen nárok na náhradu vzniklé škody.

10. **OCHRANA INFORMACÍ**

10.1. Žádná ze Smluvních stran nesmí zpřístupnit třetí osobě důvěrné informace, které při plnění této Smlouvy získala od druhé Smluvní strany. To neplatí, mají-li být za účelem plnění této Smlouvy potřebné informace zpřístupněny zaměstnancům, orgánům nebo jejich členům a subdodavatelům Poskytovatele podílejících se na plnění dle této Smlouvy za stejných podmínek, jaké jsou stanoveny smluvním stranám v tomto článku 10, a to v jen rozsahu nezbytně nutném pro řádné plnění této Smlouvy.

10.2. Ochrana informací se nevztahuje na případy, kdy

10.2.1. Smluvní strana prokáže, že je tato informace veřejně dostupná, aniž by tato dostupnost způsobila sama Smluvní strana;

10.2.2. Smluvní strana prokáže, že měla tuto informaci k dispozici ještě před datem zpřístupnění druhou Smluvní stranou, a že ji nenabyla v rozporu se zákonem;

10.2.3. může Smluvní strana získat bezúplatně tuto informaci od třetí osoby, která není omezena v jejím zpřístupnění;

10.2.4. obdrží Smluvní strana od zpřístupňující strany písemný souhlas zpřístupňovat danou informaci nebo

10.2.5. je-li zpřístupnění informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu.

10.3. Za důvěrné informace jsou dle této Smlouvy strany považovány veškeré informace vzájemně poskytnuté v ústní nebo v písemné formě, zejména informace, které se Smluvní strany dozvěděly v souvislosti s touto Smlouvou, jakož i know-how, jimž se rozumí veškeré poznatky obchodní, výrobní, technické či ekonomické povahy související s činností smluvní strany, které mají skutečnou nebo alespoň potenciální hodnotu a které nejsou v příslušných obchodních kruzích běžně dostupné a mají být utajeny. Za důvěrné informace jsou dále dle této Smlouvy považovány software, diagnostika, dokumentace včetně manuálů a veškeré další informace, které jsou písemně označeny jako důvěrné informace Poskytovatele, jejich licencí nebo Objednatele.

10.4. Smluvní strany se zavazují, že nebudou důvěrné informace poskytnuté druhou Smluvní stranou v ústnické podobě kopírovat jako celek, ani zčásti; tato povinnost se nevztahuje na případy, kdy je to nezbytné k opravě, generování nebo modifikování důvěrných informací pro jejich oprávněné užití ve smyslu této Smlouvy. Smluvní strany opatří každou kopii včetně jejího pamětového nosiče veškerým označením, které je uvedeno v dokumentu obsahujícím důvěrné informace poskytnutým druhou Smluvní stranou.

10.5. Obě Smluvní strany se zavazují nakládat s důvěrnými informacemi, které jim byly poskytnuty druhou Smluvní stranou nebo je jinak získaly v souvislosti s plněním této Smlouvy, jako s obchodním tajemstvím, zejména uchovávat je v tajnosti a učinit veškerá smluvní a technická opatření zabraňující jejich zneužití či prozrazení.

10.6. Po ukončení nebo zrušení jakékoli licence poskytnuté na základě této Smlouvy Objednatel zničí a písemně zničení Poskytovateli potvrdí, nebo vrátí Poskytovateli všechny originály a kopie Software a dokumentace, k nimž byla zrušena nebo ukončena licence, a všechny s nimi související důvěrné informace v držení Objednatele včetně důvěrných informací začleněných do jiného software nebo písemnosti. Na žádost Objednatele Poskytovatel neprodleně vrátí Objednateli nebo zničí důvěrné informace Objednatele, které již nejsou zapotřebí pro účely této Smlouvy.

10.7. Smluvní strany se zavazují, že pošlé své zaměstnance, statutární orgány, jejich členy a subdodavatele, kterým jsou zpřístupněny důvěrné informace dle odst. 10.1 této Smlouvy, o povinnosti utajovat důvěrné informace ve smyslu článku 10 Smlouvy.

10.8. Budou-li informace poskytnuté Objednatelem, které jsou nezbytné pro plnění dle této Smlouvy, obsahovat data podléhající režimu zvláštní ochrany podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, je Objednatel povinen zabezpečit splnění všech oblašovacích povinností, které ctirovaný zákon vyžaduje, a obstarat předepsané souhlasy subjektů osobních údajů předaných ke zpracování. Této povinnosti se Objednatel nemůže zprostit.

10.9. Povinnost utajovat důvěrné informace uvedené v tomto článku zavazuje Smluvní strany po dobu účinnosti této Smlouvy a po dobu dvou 2) let po ukončení jejich smluvního vztahu.

10.10. Žádné ustanovení této Smlouvy přitom nebrání nebo nezmenšuje Poskytovatele ve zveřejnění nebo obchodním využití jakékoliv technické znalosti, dovednosti nebo zkušenosti obecné povahy, kterou získal při plnění této Smlouvy.

11. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

11.1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.

11.2. Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.

11.3. Základní součinností Objednatele je zajištění přenosové vrstvy (síť ITS). V případě, že tato vrstva nebude funkční, nemese Poskytovatel odpovědnost za garantované doby dostupnosti ani funkčnost služeb a v tomto případě na něj nebudou aplikovány sankce.

11.4. Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních

11.5. Objednatel se zavazuje umožnit Poskytovateli přístup na místo plnění a k informačním systémům Objednatele, tak aby byl Poskytovatel schopen řešit vzniklé havarijní situace a Požadavky Objednatele.

11.6. Objednatel je povinen nejpozději do dvou (2) pracovních dnů od převedení systému NIS IZS do ostrého provozu zajistit a protokolárně předat Poskytovateli přístupová práva k Informačnímu systému v rozsahu nezbytném pro účely této Smlouvy. V případě, že Objednatel nezajistí Poskytovateli přístupová práva v požadovaném čase a požadovaném rozsahu, nebo v průběhu plnění Poskytovatele tyto práva jakkoliv omezí nebo zruší, nemese Poskytovatel odpovědnost za případné vzniklé škody.

11.7. Veškerá komunikace mezi Smluvními stranami bude probíhat prostřednictvím Oprávněných osob, statutárních orgánů Smluvních stran, popř. jimi pověřených pracovníků.

11.8. Všechna oznámení mezi Smluvními stranami, která se vztahují k této Smlouvě nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné podobě a druhé Smluvní straně doručena buď osobně nebo doporučeným dopisem či jinou formou registrovaného poštovního styku na adresu uvedenou v záhlaví této Smlouvy, není-li stanoveno nebo mezi Smluvními stranami dohodnuto jinak (např. v případě Požadavku Objednatele v souladu s Přílohou č. 3 této Smlouvy).

11.9. Oznámení správně adresovaná se považují za doručená 1. dnem, o němž tak stanoví zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (dále jen „ZDS"), je-li oznámení zasíláno prostřednictvím datové zprávy do datové schránky ve smyslu ZDS.

11.10. Ukládá-li Smlouva doručit některý dokument v písemné podobě, může být doručen buď v papírové formě nebo v elektronické (digitální) formě jako dokument textového procesoru MS Word verze 2000 nebo vyšší na dohodnutém médiu.

11.11. Smluvní strany se zavazují, že v případě změny své adresy budou o této změně druhou Smluvní stranu informovat nejpozději do tří (3) kalendářních dnů.

12. PLATNOST A ÚČINNOST SMLOUVY

12.1. Tato Smlouva nabývá platnosti dnem podpisu Smluvními stranami a účinnosti dnem převedení systému NIS IZS do ostrého provozu.

12.2. Smlouva zaniká mimo další možnosti stanovené právními předpisy rovněž:

12.2.1. dohodou Smluvních stran, jejíž součástí je i vypořádání vzájemných závazků a pohledávek;

12.2.2. písemným odstoupením od Smlouvy za podmínek stanovených v odst. 12.4 této Smlouvy v případě podstatného porušení Smlouvy jednou ze Smluvních stran, které je účinné dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

12.3. Podstatným porušením Smlouvy se rozumí zejména prodlení Smluvní strany s plněním předmětu plnění této Smlouvy po dobu delší než 21 dní.

12.4. Smluvní strana je oprávněna odstoupit od Smlouvy pouze v případě, že druhá Smluvní strana přes písemné upozornění na porušení Smlouvy toto porušení v poskytnuté lhůtě, která nesmí být kratší než 21 kalendářních dnů, neodstranila.

12.5. Odstoupením od Smlouvy nejsou dotčena ustanovení týkající se smluvních pokut, ochrany informací a řešení sporů.

12.6. Smlouva se uzavírá na dobu pěti let od nabytí účinnosti nebo do předčasného ukončení některé ze Smluvních stran dle odstavců 12.2.-12.4.

13. ŘEŠENÍ SPORŮ

13.1. Smluvní strany se zavazují řešit případné spory vzniklé na základě této Smlouvy přednostně dohodou.

13.2. Pokud se případný spor z této Smlouvy nepodaří vyřešit smírně, dohodly se Smluvní strany, že místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.

14. ZÁVĚREČNÁ USTANOVENÍ

14.1. Tato Smlouva, jakož i práva a povinnosti vzniklé na základě této Smlouvy nebo v souvislosti s ní, se řídí zákonem č. 513/1991 Sb., obchodní zákoník ve znění pozdějších předpisů.

14.2. Tato Smlouva představuje úplnou dohodu Smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků k této Smlouvě, podepsaných oprávněnými zástupci obou Smluvních stran.

14.3. Smluvní strany se dohodly, že z důvodů stability a bezpečnosti systému bude po dobu udržitelnosti systém provozován ve verzi, v jaké byl předán v rámci projektu NIS IZS. Výjimkou jsou bezpečnostní záplaty vydané na relevantní software po předání projektu. Jakékoliv jiné změny verzí software a firmware budou implementovány na požadavek Objednatele formou Rozvojových prací. Výjimku tvoří změny systému způsobeny změnou relevantní legislativy, takovéto úpravy budou součástí paušální platby za službu udržování legislativní aktuálnosti.

14.4. Po vypršení doby udržitelnosti projektu (5 let od ukončení realizační fáze) nabídne Objednatel Poskytovateli buď odkoupení veškerých zařízení systému za zbytkovou cenu a následný provoz podle nových podmínek, nebo prodloužení Smlouvy za stejných nebo výhodnějších podmínek. Odkoupení a výše následné platby za službu bude předmětem vyjednávání Poskytovatele s Objednatelem před vypršením doby udržitelnosti.

14.5. Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1 Oprávněné osoby
Příloha č. 2 Specifikace předmětu plnění
Příloha č. 3 Dostupnost CePU

Příloha č. 4 Garantované reakční doby
Příloha č. 5 Katalog služeb
Příloha č. 6 Sankční ujednání

14.6. Tato Smlouva je uzavřena v pěti (5) vyhotoveních, z nichž Objednatel obdrží tři (3) vyhotovení a Poskytovatel dvě (2) vyhotovení.

Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují své podpisy:

Poskytovatel	Objednatel
V _____ dne _._._____	V _____ dne _._._____
.....	.....
Česká pošta s.p., Odštěpný závod ICT služby	MV – GŘ HZS ČR

Podpis/signature:.....

Příloha č. 1 - Oprávněné osoby

Objednatel:

- ve věcech smluvních:
- ve věcech obchodních:
- ve věcech technických a realizačních:

Poskytovatel:

- ve věcech smluvních:
- ve věcech obchodních:
- ve věcech technických a realizačních:

Osoby oprávněné jednat ve věcech smluvních jsou oprávněny v rámci této Smlouvy vést s druhou Smluvní stranou jednání obchodního a smluvního charakteru, jsou oprávněny měnit či rušit tuto Smlouvu či uzavírat dodatky k této Smlouvě.

Osoby oprávněné jednat ve věcech obchodních jsou oprávněny v rámci této Smlouvy vést s druhou Smluvní stranou jednání obchodního charakteru, nejsou však oprávněny měnit či rušit tuto Smlouvu či uzavírat dodatky k této Smlouvě.

Osoby oprávněné jednat ve věcech technických a realizačních jsou oprávněny v rámci této Smlouvy vést s druhou Smluvní stranou jednání technického charakteru, nejsou však oprávněny měnit či rušit tuto Smlouvu či uzavírat dodatky k této Smlouvě. Dále jsou oprávněny provádět činnosti a úkony, o nichž to stanoví tato Smlouva.

Příloha č. 2 - Specifikace předmětu plnění

Poskytovatel bude Objednateli poskytovat podporu a rozvoj NIS IZS. Předmětem podpory a provozu je poskytování expertní kontroly, podpory a administrace Národního informačního systému integrovaného záchranného systému v produkčním prostředí, odstraňování nefunkčních stavů a konfigurační úpravy. Provozní služby budou poskytovány v následujícím rozsahu:

Pravidelné servisní a profylaktické práce

- Provozování systému monitoringu a zázemí provozu
- Monitoring systému
- Pravidelná periodická kontrola funkčnosti produkčního prostředí
- Diagnostika a optimalizace LDAP serveru
- Správa definovaných aplikačních rolí
  - Zajištění administrativního rozhraní pro správu uživatelů
  - Zajištění administrativního rozhraní pro správu pravidel
  - Zajištění administrativního rozhraní pro správu procesů
  - Úprava rolí
  - Úprava pravidel
  - Úprava procesů
- Pravidelné servisní odstávky části provozovaného systému bez vlivu na produkční provoz z důvodu provedení profylaktických prací na svěřených technologiích
  - Čištění logů
  - Defragmentace diskových polí
  - Defragmentace databází
  - Optimalizace výkonu
- Kontrola a údržba diskového prostoru
- Zálohování systému
- Zálohování dat
- Obnova konfigurace systému ze záloh
- Replikace – export dat dle sjednaných pravidel
- Kontrola systémových a aplikačních logů
- Analýza systémových a aplikačních logů
- Kontrola spuštěných procesů IS
- Zajištění telefonních služeb dle sjednaných podmínek
  - Zajištění telefonie v rámci NIS IZS
  - Zajištění zasílání SMS v rámci interních procedur systému
- Vedení elektronického provozního deníku
- Vedení kompletní provozní dokumentace

- Poskytování pravidelných reportů o průběhu provozu
- Poskytování reportů o průběhu provozu na vyžádání
- Správa systémových prostředků pro zajištění standardního provozu
- Administrátorské práce 15 dle dokumentace výrobce

Centrum uživatelů a řešení incidentů

- Provoz centra podpory uživatelů
  - Zajištění všech definovaných možností komunikace uživatelů s Centrem
  - Udržování technické aktuálnosti Centra
- Zpracování a řešení zjištěných incidentů
  - Příjem a prvotní analýza incidentů
  - Eskalace incidentů dle eskalačních pravidel
  - Pravidelný reporting nad řešenými incidenty
  - Reporty nad řešenými incidenty na vyžádání
- Analýza řešených problémových situací systémů a aplikací a eskalace objevených závad
- Poskytování konzultací

Zajištění technické aktuálnosti

- Administrace produkčního prostředí
- Pravidelná aktualizace provozní dokumentace dodavatelem provozované technologie
- Správa aktualizací a oprav provozovaného SW vydávaného výrobcem
  - Sledování aktualizací a oprav provozovaného SW vydávaných výrobcem
  - Testování aktualizací a oprav před instalací do produkčního prostředí
  - Doporučení nasazení opravných patchů a aktualizací Objednateli
  - Instalace Objednatelem schválených aktualizací a oprav do produkčního prostředí
- Zpracování zprávy o využívání HW, SW a systémových zdrojů s doporučením změn systémových zdrojů a optimalizací výkonu

Školení uživatelů Objednatele

- Zajištění školících prostor
- Udržování vzdělanosti klíčových uživatelů
- Školení nových uživatelů
- Školení nových funkcionalit při změnách systémů

Zajištění dostupnosti

- Dodržování smluvně zakotvených reakčních dob
- Zabezpečení stability klíčových parametrů systému
  - Předání rozhovoru na rozhraní
  - Založení události
  - Provedení automatické identifikace
  - Provedení automatické lokace GSM
  - Provedení automatické lokalizace pevné linky
  - Přehrání úvodní hlášky
  - Zajištění jazykové podpory pro EN/DE
  - Zajištění jazykové podpory pro vybrané jazyky
  - Zajištění systémové jazykové podpory
  - Zobrazení specifik zvláštního účastníka
  - Čas vyhledání volného operátora
  - Rychlost vizualizace oblasti volání v GIS
  - Rychlost překreslování polohy v GIS
  - Čas předání hovoru v NSPTV
  - Rychlost předání hovoru PHQ
  - Čas hledání v místopisu (omezené)
  - Čas hledání v místopisu (neomezené – 3 znaky)
  - Rychlost odezvy aplikace pro příjem TV
  - Rychlost vizualizace události pro ostatní operátory NSPTV
  - Čas vyžádání součinnosti (tech. prodleva)
  - Rychlost předání události do OR na rozhraní
  - Čas do vyhledání nejbližšího objektu podle polohy v GIS
  - Rychlost provádění výpočtů v GIS

Rozvojové práce

- Přijetí požadavků na rozvojové práce
- Vstupní analýza požadavku na rozvojové práce
- Drobné servisní a rozvojové práce v rozsahu do 20 člověkodní ročně

- Detailní analýza požadavku na rozvojové práce
- Projekt rozvoje systému
- Akceptační řízení
- Převedení produkčního systému do stavu po změně

Infrastruktura

- Zajištění dostupnosti systému provozu
- Zajištění uživatelské bezpečnosti
  - Pravidelné penetrační testy

Projekt Národní informační systém integrovaného záchranného systému (NIS IZS) Registrační číslo projektu CZ.1.06/3.4.04/11.07971

Podpora koncových stanic

- Zajištění příjmu požadavků a oznámení problémů koncových stanic
- Zajištění a provádění technické analýzy požadavků ke koncovým stanicím
- Provádění vývojových prací
- Instalace koncových zařízení
- Podpora a servis tiskáren
- Opravy chyb na koncových zařízeních

Podrobná specifikace služeb je uvedena v Příloze č. 5 – Katalog služeb provozu této Smlouvy.

1. Centrum podpory uživatelů

Služba - název	Popis	Komentář
Centrum podpory uživatelů	Jednotný komunikační bod objednatele, CePU sbírá veškeré Požadavky Objednatele s garantovanou dostupností (dle Přílohy č. 3) a garantovanými termíny odezev, dále zajišťuje přidělení řešitele, komunikaci a evidenci přes interní aplikaci a vedení databáze Požadavků Objednatele	Komunikačním kanálem je především interní webové rozhraní, dále e-mail a telefon Sledování stavu realizovaných prací, podklady pro vyúčtování a kontrolu na straně Objednatele Standardní služba, paušální platba

Funkce CePU a jeho dostupnost je popsána v Příloze č. 3 – Dostupnost CePU této Smlouvy. Všechny Požadavky Objednatele musí být evidovány CePU standardními postupy (předepsanými komunikačními kanály), aby mohla být zaručena požadovaná reakční doba a včasné zahájení řešení. V případě kdy pro evidenci požadavků nebude využíváno služeb Centra podpory – CePU, Poskytovatel negarantuje reakční doby stanovené v Příloze č. 4 – Garantované reakční doby této Smlouvy.

2. Pravidelné servisní a profylaktické práce

Služba - název	Popis	Komentář
Pravidelné servisní a profylaktické práce	Soubor periodicky prováděných úkonů, jejichž volba je závislá na potřebách a Požadavcích Objednatele	Standardní služba, paušální platba

Úlohy prováděné 1x týdně na produkčním systému v dohodnutou dobu a úlohy prováděné v první pondělí v měsíci jsou specifikovány v Příloze č. 5 – Katalog služeb této Smlouvy.

Závady zjištěné během pravidelných periodických kontrol budou bez zbytečných odkladů nahlášeny Objednateli a následně bude provedeno odstranění těchto závad za podmínek specifikovaných v Příloze č. 4 – Garantované reakční doby této Smlouvy.

Podpis/signature:……

3. Vývojové práce

Služba - název	Popis
"Konzultační služby v pracovní době" (8:00 hod. - 16:00 hod. v pracovní dny) Týká se priorit 1 - 4 dle Přílohy č. 4 Smlouvy	Provozní podpora, rozvoj a modifikace dle požadavků Objednatele. Do této oblasti spadají převážně: • podpora implementace zlepšení a doplňků NIS IZS; • úpravy nastavení dle požadavků Objednatele; • realizace doplňujících řešení navazujících na implementaci NIS IZS; • úprava stávajících funkcí NIS IZS; • informační servis.
"Konzultační služby mimo pracovní dobu" Týká se priorit 1 - 2 dle Přílohy č. 4 Smlouvy	Konzultační služby, programátorské zásahy a zásahy na systému Objednatele vedoucí k odstranění akutních vad a nefunkčnosti systému, zásahy vedoucí k obnově provozu. Zásahy mimo pracovní dobu nikdy nejsou prováděny bez vědomí odpovědné osoby Objednatele.

4. Ostatní

Ostatní služby svojí dostupností odpovídají standardnímu režimu CePU, tedy budou poskytovány v dostupnosti 5 x 8 – každý pracovní den od 8:00 do 16:00.

Detailní specifikace předmětu plnění

V této části Smlouvy bude detailní soupis všech komponent a prvků, které bude systém obsahovat. Bude zde seznam všech lokalit a rozmístění vypsaných prvků na tyto lokality. Toto bude do smlouvy doplněno po ukončení všech veřejných zakázek spojených s projektem, protože až poté bude tento soupis možné vytvořit.

Příloha č. 3 – Dostupnost CePU

Centrum podpory uživatelů (dále jen „CePU") je kontaktním místem pro služby související se zaváděním a využíváním vybraných informačních systémů a softwarových produktů za podmínek a v rozsahu dle uzavřené Smlouvy. CePU organizuje podporu, eviduje a dozoruje databázze požadavků Objednatele. CePU je vedeno Poskytovatelem

CePU poskytuje pro Objednatele spadané služby v režimu 7/24/365. Aktivně dozoruje HotLine telefon a organizuje dodávky (řešení havárií atd. dle požadavků Objednatele).

Komunikace ohledně zákaznických požadavků se oznámí CePU, a to jedním z předepsaných komunikačních kanálů – telefonická forma skrze HotLine, e-mail na xxx@cpost.cz, přes elektronický formulář, také na stránce http://www.XYZ.cz.

Prostředek	HotLine	Fax	E-mail	Web
Kontakt	+	+	+	+
Dostupnost	Nepřetržitě	Nepřetržitě	Nepřetržitě	Nepřetržitě
Časové omezení reakce	Nepřetržitě	Nepřetržitě	Nepřetržitě	Nepřetržitě

Všechny požadavky Objednatele musí být evidovány CePU standardními postupy (předepsanými komunikačními kanály), aby mohla být zaručena požadovaná reakční doba a včasné zahájení řešení v souladu s Přílohou č. 4 – Garantované reakční doby této Smlouvy.

Pravidelné servisní a profylaktické práce nejsou objednávány prostřednictvím HelpDesku. Poskytovatel je provádí automaticky ve stanovenou dobu a Objednatele informuje o výsledku prostřednictvím emailu.

Dostupnost dohledového systému jako takového je poskytována jako služba v rámci garance dostupnosti centra podpory uživatelů. Disaster recovery dohledového systému a tedy i centra podpory uživatelů je řešeno interními procesy Poskytovatele a zde je brano jako implicitní služba.

Ohlášení požadavků bude primárně probíhat přes elektronický formulář aplikace Servis desk na stránce http://www.XYZ.cz, kde bude prokazatelná evidence přijatých požadavků nebo hlášení a reakční doby. V případě jeho nedostupnosti telefonicky, písemně, faxem nebo elektronickou poštou s tím, že požadovaná lhůta vyřešení počítá hodinou okamžikem potvrzení ze strany Poskytovatele (e-mail, přidělení řešitele v aplikaci Servis desk) o doručení požadavků a potřebných podkladů. Poskytovatel uvede požadavky na osoby, kalendářní termíny a na formy požadované služby. Poskytovatel se zavazuje potvrdit požadavek (a to i ústně) v nejbližším možném termínu a vyspecifikuje v potvrzení osoby, termíny a formy řešení, případně navrhne jiné než požadované řešení. Ve složitějších případech se předpokládá vícekroková komunikace vedoucí k nalezení a potvrzení oboustranně vyhovujícího řešení.

Podpis/signature:……

Příloha č. 4 – Garantované reakční doby

Poskytovatel uvažuje následující členění chyb (vad) a Požadavků Objednatele a jim odpovídající reakční doby a garance:

Priorita	Odezva	Nástup na řešení	Kategorie vad
1	Do 4 hodin	Do 4 hodin	Závada kategorie A
2	Do 24 hodin	Do druhého pracovního dne	Závada kategorie B
3	Do 24 hodin	Do 2 pracovních dnů	Závada kategorie C
4	Do dvou pracovních dnů	Do 10 pracovních dnů	Požadavky na Rozvojové práce, poskytnutí konzultací

Příloha č. 5 – Katalog služeb

Viz Příloha č. 1, Části E – Provoz (samostatný dokument)

Sankční kalkulace				
Předmět	Kategorie chyby	Prodlení trvající ne déle než dvojnásobek garantované reakční doby služby	Prodlení trvající déle než dvojnásobek garantované reakční doby služby	Prodlení trvající déle než trojnásobek garantované reakční doby služby
Pravidelné servisní a profylaktické práce	A	Úroveň 2	Úroveň 3	Úroveň 3
	B	Úroveň 1	Úroveň 2	Úroveň 3
	C	Úroveň 1	Úroveň 2	Úroveň 3
Centrum podpory uživatelů a řešení incidentů	A	Úroveň 3	Úroveň 3	Úroveň 3
	B	Úroveň 1	Úroveň 2	Úroveň 3
	C	Úroveň 1	Úroveň 2	Úroveň 3
Zajištění technické aktuálnosti	A	Úroveň 1	Úroveň 2	Úroveň 3
	B	Úroveň 1	Úroveň 2	Úroveň 3
	C	Úroveň 1	Úroveň 2	Úroveň 3
Školení uživatelů	A	Úroveň 1	Úroveň 2	Úroveň 3
	B	Úroveň 1	Úroveň 2	Úroveň 3
	C	Úroveň 1	Úroveň 2	Úroveň 3
Zajištění dostupnosti	A	Úroveň 3	Úroveň 3	Úroveň 3
	B	Úroveň 1	Úroveň 2	Úroveň 3
	C	Úroveň 1	Úroveň 2	Úroveň 3
Rozvojové práce	A	Úroveň 1	Úroveň 2	Úroveň 3
	B	Úroveň 1	Úroveň 2	Úroveň 3
	C	Úroveň 1	Úroveň 2	Úroveň 3
Infrastruktura	A	Úroveň 1	Úroveň 2	Úroveň 3
	B	Úroveň 1	Úroveň 2	Úroveň 3
	C	Úroveň 1	Úroveň 2	Úroveň 3
Podpora koncových stanic	A	Úroveň 2	Úroveň 3	Úroveň 3
	B	Úroveň 1	Úroveň 2	Úroveň 3
	C	Úroveň 1	Úroveň 2	Úroveň 3

strana 60 (celkem strana 62)

Příloha č. 6 – Sankční ujednání

Sankce budou klasifikovány dle kategorizace závad. Ta je následující:

Kategorizace závad

- Kategorie A
  - Kritická závada - aplikace je zcela nefunkční, uživatelé nemohou s aplikací vůbec pracovat.
  - Porucha prvků a komponent, které jsou v záruce, s reshumanci nižší než 200 %.
- Kategorie B
  - Hlavní závada - aplikace vykazuje chyby, uživatelé mohou s aplikací pracovat s malým omezením, nebo zcela bez omezení nebo existuje workaround.
  - Porucha prvků a komponent, které jsou v záruce, s reshumanci 200 % nebo vyšší.
- Kategorie C
  - Vedlejší závada - koncová zařízení, vyjma náhlavní soupravy, vykazují chyby a uživatelé je mohou používat maximálně s velkými omezeními.
  - Požadavek na změnu, úpravu, výměnu, konzultaci týkající se koncových zařízení v lokalitách klienta vyjma náhlavní soupravy a tiskárny.

K jednotlivým službám je vždy garantována určitá úroveň SLA. Úrovně SLA vzhledem k sankcím jsou následující:

- Úroveň 1 – porušení této úrovně není důvodem pro uplatnění smluvní pokuty Objednatelem
- Úroveň 2 – porušení této úrovně následuje napomenutí Poskytovatele Objednatelem bez uplatnění smluvní pokuty
- Úroveň 3 – Objednatel uplatňuje smluvní pokutu ve výši XXX,– Kč (pět tisíc korun českých) za každý den prodlení v odstranění závady po překročení této hranice

Nakonec budou sankce definovány nad garantovanou provozní dobou jednotlivých částí systému:

Garantovaná provozní doba	Dostupnost
Provozní systém NIS IZS	X
Centrum podpory uživatelů	X
Produkční prostředí NIS IZS	X
Školící systémy NIS IZS	X
Garantovaná dostupnost aplikace	X

Celková matice aplikovatelných sankcí je následující:

strana 59 (celkem strana 62)

Rejstřík

Model 1 - Úrovně provozu 4
Model 10 - Schéma eskalace 28
Model 2 - Proces managementu událostí 14
Model 3 - Proces managementu incidentů 16
Model 4 - Proces managementu problémů 18
Model 5 - Proces managementu změn systému 20
Model 6 - Proces vyhodnocení změn systému 22
Model 7 - Proces řízení verzí 23
Model 8 - Proces validace a testování 25
Model 9 - Proces managementu konfigurace 27
Tabulka 1: Náklady na provoz a údržbu NIS IZS 10
Tabulka 2: Plán obnovy koncových zařízení 12

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

F. Bezpečnostní projekt

Dokument obsahuje:	Vymezení rozsahu projektu z hlediska bezpečnosti, specifikaci rizik, zajištění fyzické a komunikační, kybernetické a personální bezpečnosti a její testování a přehled bezpečnostní dokumentace.
Verze:	5.1b
Schválil za Dodavatele:	RNDr. Vladimír Příbramský
Datum aktualizace:	17/4/2014

Projekt Národní informační systém integrovaného záchranného systému (NIS IZS) Registrační číslo projektu CZ.1.06/3.4.00/11.07471

Obsah

01. Metodika ... 4
Předpoklady ... 4
Koncepce informační bezpečnosti NIS IZS ... 4
02. Vymezení rozsahu NIS IZS ... 6
Subjekty NIS IZS ... 6
Data NIS IZS ... 6
Provozní data NIS IZS ... 6
Geografická data z veřejných zdrojů ... 6
Geografická data z ostatních zdrojů ... 6
Data od vybraných poskytovatelů ... 6
Data pro správu NIS IZS ... 7
Záznamy o provozu NIS IZS ... 7
Software NIS IZS ... 7
Hardware NIS IZS ... 7
Lokality NIS IZS ... 7
03. Řízení rizik NIS IZS ... 8
Identifikace a klasifikace rizik ... 8
Hodnocení rizik ... 9
Zvládání rizik ... 9
04. Fyzická bezpečnost ... 12
Fyzická bezpečnost DC NIS ... 12
Fyzická bezpečnost KDC NIS ... 14
Fyzická bezpečnost zařízení NIS IZS ... 14
05. Technická a komunikační bezpečnost ... 15
Bezpečnost sítí v CDC a KDC NIS IZS ... 15
Bezpečnost propojení mezi komponentami NIS IZS ... 15
Bezpečnost připojení cizích zařízení k NIS IZS ... 18
Bezpečnost připojení vlastních zařízení k NIS IZS ... 19
Bezpečnost záložního propojení ... 20
Připojení do Internetu ... 23
Řízení privilegovaného přístupu k systému ... 24
Řízení změn v systému ... 24

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ - F - BEZPEČNOST, verze Strana 2 (celkem strar 20)

Podpis/signature:.....

Správa systému 25
Řízení kontinuity a obnova po havárii 25
06. Kybernetická bezpečnost NIS IZS 27
Bezpečnostní monitoring NIS IZS 27
Ochrana proti virům a škodlivému kódu 29
Analýza technických zranitelností 29
Zálohování a archivace 29
07. Personální a organizační bezpečnost 31
Personální bezpečnost 31
Organizace bezpečnosti 32
Řízení bezpečnostních incidentů 32
08. Testování bezpečnosti NIS IZS 33
Testování bezpečnosti aplikací 33
Testování bezpečnosti infrastruktury 34
Kontroly souladu 37
09. Bezpečnostní dokumentace pro provoz 38
Příloha 39
Rejstřík 39

01. Metodika

Předpoklady

V textu je použito označení Dodavatel pro dodavatele projektu NIS IZS jak pro označení dodavatele v roli dodavatele NIS IZS, tak v roli budoucího provozovatele NIS IZS. Dodavatel popsanými činnostmi nepřijímá žádné závazky pro dobu, kdy nebude provozovatelem NIS IZS.

Řešení informační bezpečnosti NIS IZS popsané v tomto dokumentu vychází z následujících předpokladů:

- Předmětem ochrany nejsou **data klasifikovaná podle** zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
- Pro komunikaci je použita bezpečná síť ITS.
- Bezpečnostní opatření tvoří provázaný celek. Při změně nebo vynechání jednoho opatření musí být prozkoumán a vyhodnocen vliv změny na celkovou bezpečnost NIS IZS.

Koncepce informační bezpečnosti NIS IZS

NIS IZS je navržen a budován jako vysoce bezpečný informační a komunikační systém. Důraz je kladen na všechny základní složky bezpečnosti informací.

- **Dostupnost**: informace jsou dostupné v požadovaném čase a na požadovaném místě. V případě NIS IZS se jedná o kritický požadavek.
- **Integrita**: pouze oprávněné subjekty mohou informace vytvářet a měnit.
- **Důvěrnost**: pouze oprávněné subjekty mohou informace číst.
- **Nepopiratelnost**: subjekt, který provedl nějakou operaci s informacemi, se nemůže vzdát odpovědnosti za provedení akce.

Dodavatel chápe informační bezpečnost NIS IZS jako proces. V etapě přípravy a realizace budou navržena a implementována určitá bezpečnostní opatření.

Během provozu bude Dodavatel identifikovat případné nové hrozby ohrožující systém a případné nové zranitelnosti systému a navrhne a realizuje **preventivní opatření** proti novým hrozbám a bude odstraňovat nové zranitelnosti.

Dodavatel bude činnost systému kontinuálně a v reálném čase monitorovat, mj. s cílem **detekovat** případná **narušení bezpečnosti**. Pokud se taková narušení vyskytnou, přijme **nápravná opatření a navrhne zvýšení bezpečnosti systému**. Monitoring bude provádět dohledové centrum Dodavatele.

Při řízení informační bezpečnosti NIS IZS bude Dodavatel dodržovat následující **principy**:

Podpis/signature:.....

02. Vymezení rozsahu NIS IZS

Do rozsahu NIS IZS patří:

- Subjekty NIS IZS
- Data NIS IZS
- Služby NIS IZS
- Software NIS IZS
- Hardware NIS IZS
- Lokality NIS IZS
- Síť NIS IZS

Subjekty NIS IZS

Subjekty NIS IZS tvoří dvě skupiny – uživatelé a správci. Uživatelé jsou osoby používající NIS IZS. Jejich role jsou definovány v části „I - Školení". Správci jsou osoby na straně Dodavatele NIS IZS, které provádějí administraci, monitoring, dohled a podporu 1. a 2. úrovně celého systému NIS IZS.

Data NIS IZS

Data NIS IZS jsou rozdělena do následujících skupin:

Provozní data NIS IZS

a) Záznamy o hovorech na tísňových linkách.
b) Údaje poslané z příjmu tísňového volání v KDC na krajská operační střediska.
c) Údaje poslané z krajských operačních středisek na příjem tísňového volání v KDC.

Geografická data z veřejných zdrojů

a) Geodata ČÚZK.
b) Mapová díla ISKN.
c) RÚIAN.
d) Digitální mapa veřejné správy (až bude vytvořena a poskytnuta).

Geografická data z ostatních zdrojů

a) ZABAGED.
b) Geonames.

Data od vybraných poskytovatelů

a) Údaje poskytované telefonními operátory. Specifikovány v části J Prováděcího koncepta.
b) JSDI.
c) Údaje o meteorologické situaci. Poskytuje ČMHÚ, jde o neveřejné údaje.

- Bezpečnost je založena na zvládání rizik, tj. na identifikaci rizik a realizaci odpovídajících opatření proti nim.
- Bezpečnost je a bude Dodavatelem řešena ve fázi přípravy NIS IZS pro provoz a v provozu v době, kdy Dodavatel bude provozovatelem NIS IZS.
- Jsou definovány a personálně obsazeny bezpečnostní role pro provoz a správu NIS IZS a vymezeny povinnosti osob, které budou jednotlivé role vykonávat.
- Je kontinuálně a v reálném čase monitorována bezpečnost provozu NIS IZS. Jsou definovány postupy pro vyšetřování bezpečnostních událostí a incidentů a zajištěny mechanismy pro přijetí nápravných opatření.
- Je zajištěna kontinuita činností NIS IZS při narušení systému, zejména pak výskytu následujících situací: při výpadcích jednotlivých zařízení potřebných pro provoz NIS IZS a při výpadcích jednotlivých centrálních DC a krajských DC NIS.
- Ze strany Zadavatele i Dodavatele jsou respektovány specifické bezpečnostní požadavky kladené na NIS IZS.
- Existuje a v průběhu provozu systému Dodavatel udržuje plán rozvoje NIS IZS pokrývající realizaci bezpečnostních opatření, která vyplývají z vyhodnocení incidentů, ze změn v charakteristice a hodnotách rizik a z návrhů na zvýšení bezpečnosti systému a jeho prostředí.

d) Údaje o dopravní situaci. Poskytuje CDI prostřednictvím Policie ČR, jde o neveřejné údaje.

Data pro správu NIS IZS

a) Konfigurační data síťových zařízení v DC.

b) Konfigurační data síťových zařízení na krajích. Včetně konfiguračních dat směrovačů CE pro připojení KDC a krajských operačních středisek k ITS.

c) Konfigurační data aplikace: definice procesů, definice pravidel.

d) Definice pravidel pro směrování zpráv.

e) Data posílaná dohledovými systémy.

f) Obsah komunikace správců s jednotlivými zařízeními.

Záznamy o provozu NIS IZS

a) Logy.

b) Auditní záznamy.

Software NIS IZS

Software je podrobně specifikován v části B Prováděcího konceptu.

Hardware NIS IZS

Hardware je podrobně specifikován v části A Prováděcího konceptu.

Lokality NIS IZS

Lokality jsou podrobně specifikovány v příloze 1 části A Prováděcího konceptu.

03. Řízení rizik NIS IZS

Identifikace a klasifikace rizik

Následující rizika rozdělená do kategorií jsou uvažována jako základní seznam pro fázi provozu NIS IZS. Systém bude kontinuálně monitorovaný a budou sledována všechna potenciální rizika, která mohou být identifikována i mimo níže uvedený seznam.

Fyzická rizika

a) Ohrožení zařízení NIS IZS přírodními vlivy (záplavy, vítr, sníh, zemětřesení, blesk).

b) Ohrožení zařízení NIS IZS ohněm.

c) Ohrožení zařízení NIS IZS průmyslovými haváriemi.

d) Ohrožení zařízení NIS IZS nevyhovujícími podmínkami pro provoz (teplota, vlhkost, prašnost, stabilita dodávané elektřiny).

e) Krádež zařízení nebo jejich zničení či poškození.

f) Teroristický útok.

Personální rizika

g) Chyba obsluhy: chybné konfigurace hardware nebo software, chybné příkazy administrátorů. Chyby v DNS, směrování, IP adresách.

h) Sociální inženýrství proti osobám podílejícím se na provozu nebo správě NIS IZS s cílem zneužít jejich oprávnění.

i) Provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů nebo správců.

Kybernetická rizika

j) Výskyt škodlivého software, např. viry, spyware, trojské koně apod v NIS IZS.

k) Kybernetický útok vedený proti NIS IZS z nějaké vnější sítě (ITS, CMS, KSP) - footprinting, lámání hesel, spouštění kódu.

l) Útok na dostupnost NIS IZS z nějaké vnější sítě (ITS, CMS, KSP).

m) Kybernetický útok vedený proti NIS IZS z vnitřní sítě (NIS) - footprinting, lámání hesel, spouštění kódu.

n) Útok na dostupnost NIS IZS z vnitřní sítě (NIS).

o) Falšování identity uživatele nebo zařízení.

Technická rizika

p) Chyba aplikačního software.

q) Nedostupnost dat potřebných pro fungování aplikací.

r) Použití neověřených dat potřebných pro fungování aplikací.

s) Neoprávněná modifikace nebo smazání dat NIS.

t) Infiltrace komunikace, narušení integrity přenášených dat NIS.

u) Zneužití dat NIS, neoprávněný přístup k datům NIS, neoprávněné kopírování dat NIS.

v) Zachycení komunikace, narušení důvěrnosti přenášených dat NIS.

w) Chyba systémového software.

x) Selhání nebo neúmyslné poškození hardware.

y) Nedostupnost komunikací (počítačové sítě, telefonní síť).

z) Přerušení dodávky elektrické energie.

aa) Využívání software v rozporu s licenčními podmínkami.

Hodnocení rizik

Dodavatel provedl hodnocení rizik, ve kterém vyhodnotil jednotlivá rizika a navrhl opatření na jejich pokrytí, odstranění nebo snížení jejich míry. Opatření tvoří základ tohoto dokumentu a jsou popsána v jeho jednotlivých kapitolách jako požadavky na zajištění bezpečnosti. Hodnocení informačních rizik a návrh protiopatření je klíčovou částí řízení bezpečnosti informačních systémů obecně a tedy i NIS IZS.

Cílem hodnocení rizik je stanovení závažnosti jednotlivých rizik a zajištění, že aktuálně navržená bezpečnostní opatření jsou dostatečná a efektivní.

Rizika budou vyhodnocována kontinuálně v rámci celého životního cyklu NIS IZS. Během hodnocení rizik může být zjištěno, že některá rizika vykazují při aktuálně navržených opatřeních příliš vysokou míru. Pokud taková situace nastane, Dodavatel navrhne způsob zvládnutí rizika.

Zvládání rizik

Existuje několik metod pro zvládnutí rizika existujícího i po realizaci navržených opatření. Tato rizika se nazývají zbytková rizika.

1) Pokrytí rizika, tedy snížení jeho míry výběrem takových opatření (dosud nerealizovaných a nenavržených), aby mohlo být zbytkové riziko vyhodnoceno jako akceptovatelné trvale nebo dočasně.

2) Vědomé přijetí (akceptace) rizika se může použít v případě, že se nejedná o vysoké riziko a není vážně ohrožena bezpečnost informačních aktiv a jsou splněny požadavky zadavatele na bezpečnost informací.

3) Přenos rizika lze použít v případě, že je obtížné snížit riziko na přijatelnou úroveň vlastními zdroji. Možnými metodami je pojištění nebo outsourcing.

4) Vyhnutí se riziku znamená jakoukoli akci, při které jsou podmínky provozu informačního nebo komunikačního systému změněny tak, aby výskyt rizika nehrozil.

Větší část rizik bude pokryta opatřeními, která zajistí požadovanou úroveň bezpečnosti NIS IZS. Akceptace rizik, případně jeho přenos budou využity pouze za předpokladu, že nehrozí znamenat porušení požadavků Zadavatele na bezpečnost NIS IZS a zákonných požadavků na bezpečnost NIS IZS.

Pro pokrytí rizik budou realizována bezpečnostní opatření, která jsou ekonomicky přiměřená a technicky dostupná a která budou mít následující formy:

a) Technická opatření.

b) Personální opatření.

c) Organizační opatření.

d) Bezpečnostní standardy v bezpečnostní politice NIS IZS.

e) Pracovní postupy používané při správě a užívání NIS IZS.

Cílem opatření je zajistit přiměřenou bezpečnost NIS IZS v následujících oblastech:

- Fyzická bezpečnost. Tato opatření zajišťují bezpečné umístění technických prostředků NIS IZS a omezení fyzického přístupu k zařízením NIS IZS. Mezi opatření fyzické bezpečnosti patří i zajištění bezpečných podmínek pro provoz technických zařízení NIS IZS včetně klimatizace, dostatečných prostor, pravidel pro údržbu a kontrolu přístupu k zařízení systému.
- Technická a komunikační bezpečnost. Tato opatření zahrnují implementaci bezpečnostních technologií, které zajistí kontinuální prosazení požadované úrovně bezpečnosti v celém systému po technické stránce. Technická bezpečnostní opatření vycházejí z bezpečnostních standardů a vynucují jejich dodržování uživateli a správci NIS IZS.
- Kybernetická bezpečnost. Tato opatření zajišťují bezpečnost dat v digitální formě při jejich zpracování, ukládání a přenosech včetně ochrany proti malware, hackerským útokům a jinému zneužití.
- Personální bezpečnost. Tato opatření zajišťují bezpečnost činností osob při provozu NIS IZS. Zahrnuje definice postupů pro různé činnosti, obsazování bezpečnostních rolí důvěryhodnými osobami (viz kapitolu „Personální bezpečnost"), povinnosti zachovávat mlčenlivost a bezpečnostní vzdělávání.
- Organizační bezpečnost. Tato opatření zajišťují jasnou definici kompetencí, práv a odpovědností jednotlivých rolí v systému na straně Zadavatele i Dodavatele.

Součástí návrhu řešení NIS IZS je řada bezpečnostních opatření. Během výběru opatření je důležité zvážit náklady na zavedení a provozování opatření ve vztahu k hodnotě chráněných aktiv. Dodavatel navrhne a implementuje taková protiopatření, která splní požadavky na zvládnutí rizik a budou respektovat existující finanční, časová a technická omezení.

V rámci dalších prací budou bezpečnostní požadavky uvedené v dalších kapitolách tohoto dokumentu transformovány do Registru bezpečnostních požadavků a opatření, který bude základním etalonem pro nastavení požadované úrovně bezpečnosti NIS IZS. Registr bude umožňovat sledování naplnění jednotlivých požadavků v průběhu vývoje.

implementace i provozu NIS IZS. Registr bezpečnostních požadavků a opatření vytvoří a bude udržovat Dodavatel.

Detailní a kompletní návrh bezpečnostních opatření v registru, včetně plánu jejich implementace bude vytvořen v dalších fázích projektu. Opatření budou vycházet z ISO/IEC 27002, NIST 800-53 a dalších nejlepších praktik. V dalších kapitolách jsou uvedena základní opatření, která musí být realizována, nicméně jejich přesná technická specifikace je závislá mj. na konkrétních technologiích, které při tvorbě tohoto konceptu nejsou známé zcela nebo z části. Dodavatel bezpečnostní opatření detailně specifikuje v rámci dalších fází projektu (viz kap. 9. této části PKv40).

04. Fyzická bezpečnost

Pojem „fyzická bezpečnost" je používán ve smyslu zajištění bezpečných podmínek pro provoz technických zařízení. Zahrnuje jak opatření pro omezení fyzického přístupu k zařízením, tak pro zajištění provozních podmínek (teplota, vlhkost atd.) pro zařízení. Toto je ve shodě s terminologií používanou v návrhu zákona o kybernetické bezpečnosti a s terminologií používanou NBÚ (např. v zákoně č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů).

Opatření na omezení fyzického přístupu k zařízením tvoří základ bezpečnostních opatření. Pokud totiž útočník získá fyzický přístup k některým zařízením, stanou se bezpečnostní opatření proti určitým typům útoků neúčinná.

Běžná zařízení výpočetní techniky potřebují ke své činnosti přiměřené provozní podmínky, zejména určitou teplotu a vlhkost a omezenou prašnost. Pro spolehlivé fungování zařízení je důležité takové prostředí zajistit. Dále tato zařízení potřebují zásobování elektřinou a to v požadované úrovni a kvalitě. Kolísání proudu a napětí ovlivňuje negativně nejen životnost zařízení výpočetní techniky ale i jejich funkce. Správné funkce a prodloužení životnosti zařízení lze také zajistit pravidelnou údržbou podle pokynů výrobce. Proto Dodavatel věnuje v rámci fyzické bezpečnosti pozornost i zajištění potřebných provozních podmínek pro zařízení výpočetní techniky a jejich údržbě.

Fyzická bezpečnost DC NIS

1) DC budou v budovách se řízeným přístupem a evidencí vstupujících osob. Kontrolu a evidenci budou provádět buď pracovníci recepce/vrátnice nebo bude prováděna automaticky pomocí technických zařízení.
2) Pro řízení přístupu do DC a prostor se zařízením NIS IZS jsou vytvořeny postupy a je udržován aktuální seznam pracovníků s oprávněným přístupem k zařízení NIS IZS.
3) Přístup do lokality a budovy DC bude monitorován.
4) V DC bude zajištěna požární ochrana.
5)
6) DC budou chráněna proti živelným katastrofám.
7) DC nebudou umístěna v blízkosti nebezpečných průmyslových provozů (typu výroby výbušnin a velkých chemických podniků).
8) V budovách s DC nebudou provozy nebo zařízení způsobující vibrace instalovaných zařízení.
9) DC budou umístěna tak, aby nebyla ve zvýšené míře ohrožena pořádáním hromadných akcí (zejména demonstrací a sportovních akcí spojených s vandalismem) v jejich blízkosti.

Podpis/signature:.....

10) Prostory se zařízeními NIS IZS budou monitorovány a záznamy budou uloženy a archivovány v souladu s požadavky Zadavatele a Dodavatele.

11) Prostory se zařízeními NIS IZS nebudou dostupné z veřejně přístupných prostor.

12) Systémy pro podporu zabezpečovacích a přístupových systémů budou umístěny mimo prostory, kde se nachází zařízení NIZ IZS. Přístup k zabezpečovacím a přístupovým systémům bude přísně řízen.

13) Prostory se zařízeními NIS IZS budou vybaveny proti elektromagnetismu a statické elektřině (antistatická podlaha).

14) Zařízení NIS IZS budou v rámci DC umístěna v prostorách oddělených od okolí. Stačí uzamykatelné skříně (racky).

15) Bude zajištěna fyzická ostraha DC. Ostrahu DC bude mít povolen přístup do prostor se zařízeními NIS IZS pouze v případě mimořádných událostí a každý vstup ostrahy bude zaprotokolován. Mimořádnými událostmi se zde myslí následující události: požár, zaplavení, vysoká teplota, neoprávněný vstup.

16) Fyzický přístup k zařízením NIS IZS bude monitorován (např. prostřednictvím automatických záznamů otevření racků/skříní nebo organizačním opatřením – klíče k racku budou vydávány pouze oprávněným pracovníkům Dodavatele proti podpisu, případně budou práce na zařízení NIS IZS prováděny pod dohledem ostrahy DC).

17) Dodavatelem budou vytvořeny postupy pro nouzové opravy zařízení a jejich výměnu, či opravu na místě.

18) Prostory v DC pro zařízení NIS IZS budou splňovat požadavky zařízení na provozní podmínky (teplota, vlhkost) instalovaných zařízení podle údajů výrobce. Bude zajištěno instalací klimatizačních jednotek včetně zvlhčovačů vzduchu.

19) Bude zajištěn bezpečný přístup k jednotlivým zařízením a budou zajištěny dostatečné servisní prostory kolem nich (min. 0.5m mezi racky).

20) DC budou vybavena elektrickými slovými rozvody dostatečné kapacity a kvality dle specifikace, která bude upřesněna po výběru konkrétních technologií. Budou splněny minimálně následující požadavky:

a. Elektrické kabely budou buď uloženy ve dvojitě podlaze, nebo budou zakryté lištami.

b. Bude zajištěna kvalita proudu a ochrana před kolísáním napětí. Napájení bude procházet přes záložní zdroj elektřiny, který potřebnou ochranu zajistí.

21) Bude zajištěno bezpečné zásobování všech zařízení NIS IZS v DC elektřinou. DC bude vybaveno UPS a centrálními záložními zdroji podle standardů A studie interoperability.

22) Bude omezen fyzický přístup k datovým rozvodům. Buď budou uloženy do lišt, nebo vedeny pod podlahou nebo pod stropem.

Fyzická bezpečnost KDC NIS

Požadavky na bezpečnost jsou uvedeny ve standardech A Analýzy interoperability základních složek integrovaného záchranného systému.

Fyzická bezpečnost zařízení NIS IZS

Vztahuje se na všechna zařízení NIS IZS nezávisle na jejich umístění.

1) Všechna zařízení NIS IZS budou provozována a udržována v souladu s doporučením výrobce. Veškeré opravy a servisní zásahy budou provádět pouze oprávněné osoby s potřebnou kvalifikací. Veškeré opravy a servisní zásahy budou prováděny pouze se souhlasem Dodavatele a za dozoru jeho zástupce nebo osoby pověřené Dodavatelem.

2) Budou vytvořeny postupy pro nouzové opravy zařízení a jejich výměnu, či opravu na místě. Opravy budou realizovány důvěryhodnými pracovníky s oprávněným přístupem.

3) Bude zajištěno bezpečné vymazání/přepsání obsahu paměťových médií používaných pro NIS IZS v případě jejich likvidace nebo zaslání do opravy.

4) Transport zařízení NIS IZS do opravy mimo lokalitu DC bude prováděn bezpečným způsobem, který zajistí Dodavatel. Dodavatelem budou vytvořeny postupy pro transport.

5) Je stále udržován aktuální seznam technického vybavení a jsou prováděny pravidelné kontroly souladu.

05. Technická a komunikační bezpečnost

Opatření zahrnují implementaci bezpečnostních technologií a jejich nastavení, které zajistí kontinuální prosazení požadované úrovně bezpečnosti v celém systému po technické stránce. Technická bezpečnostní opatření vycházejí z bezpečnostních standardů a vymezují jejich dodržování uživateli a správci NIS IZS.

Bezpečnost sítí v CDC a KDC NIS IZS

Pro zajištění bezpečnosti počítačových sítí v jednotlivých CDC a KDC NIS realizuje Dodavatel minimálně následující opatření:

1) Síťová zařízení NIS IZS budou umístěna pouze v chráněných a monitorovaných prostorech s řízeným přístupem.
2) Pro provoz a správu NIS IZS nejsou využívané bezdrátové sítě Wi-Fi.
3) Bude kontrolováno připojení zařízení k aktivním síťovým prvkům NIS IZS. Nepoužívané porty budou deaktivovány.
4) Bude prováděna autentizace zařízení připojených k aktivním síťovým prvkům NIS IZS, aby bylo zabráněno připojení neautorizovaných zařízení.
5) Zařízení v DC NIS IZS budou oddělena buď fyzicky nebo na L2 od zařízení, která nejsou určena pro provoz NIS IZS.

   Fyzické oddělení znamená, že zařízení NIS IZS nejsou fyzicky připojena k jiným síťovým zařízením.

   Oddělení na L2 znamená, že zařízení NIS IZS jsou provozována v různých VLAN. Za tohoto předpokladu je možné sdílet síťovou infrastrukturu s jinými systémy.
6) Zařízení v DC NIS IZS budou oddělena na L3 od všech ostatních zařízení umístěných v LAN.

   Oddělení na L3 znamená, že zařízení různých subsystémů ZR jsou v různých IP sítích (IP subnets) a provoz mezi nimi musí být směrován (routing).
7) Logický přístup na administrační rozhraní síťových prvků je řízen a je omezen pouze na oprávněné a jednoznačně identifikovatelné správce systému.
8) U síťových zařízení jsou pro privilegované a neprivilegované činnosti používány samostatné účty.
9) Vzdálený přístup k síťovým zařízením je omezen pouze na jednoznačně identifikovatelné správce systému.
10) Konfigurační nastavení síťových zařízení jsou pravidelně zálohována.

Bezpečnost propojení mezi komponentami NIS IZS

V této kapitole je řešena bezpečnost následujících propojení:

- komunikace operačních středisek NIS s CDC a KDC NIS,
- komunikace mezi CDC a KDC NIS.

Firewally v CDC a KDC NIS

Na operačních střediscích budou umístěny koncová zařízení pro práci s NIS IZS: telefony a pracovní stanice. Tato zařízení budou plně pod kontrolou Dodavatele a nebudou připojena do žádných dalších sítí.

V CDC a KDC budou umístěny servery a další zařízení potřebná pro provoz NIS (diková pole, zálohovací a archivační zařízení, atd.). Tato zařízení budou plně pod kontrolou Dodavatele a nebudou připojena do žádných dalších sítí s výjimkou telefonní ústředny, která bude připojena do VTS, ale od ní bude oddělena SIP firewallem.

Na střediscích operačního řízení budou umístěna zařízení jednotlivých složek IZS. Tato zařízení nebudou pod kontrolou Dodavatele.

K propojení bude použita zabezpečená síť ITS (viz část C „Síťová infrastruktura").

S výjimkou středisek operačního řízení IZS budou ostatní komponenty pod kontrolou Dodavatele. Proto postačí bezpečnostně oddělit střediska operačního řízení IZS od CDC a KDC NIS. Toto oddělení bude provedeno **ve všech CDC a KDC NIS instalací firewallů**. Tyto firewally budou sloužit k filtraci datového i hlasového provozu mezi CDC a KDC NIS a okolím.

Opatření v operačních střediscích NIS

Na jednotlivých operačních střediscích NIS firewally nebudou, ale i tam budou nastavena následující bezpečnostní opatření na CE směrovačích.

1) Omezit komunikaci na předem definované a dokumentované IP adresy a protokoly.
2) Zajistit, aby komunikace z operačních středisek byla směrována pouze směrem do CDC NIS nebo KDC NIS.
3) Rozdělit VPN projektu NIS IZS do dvou částí: NIS „backplain" a NIS „public".
4) Umístit CDC a KDC projektu v části NIS „backplain" (tato VPN zajišťuje komunikaci mezi jednotlivými systémy, klienti nemají mít do VPN NIS "backplain" přístup)
5) Zajistit komunikaci v rámci VPN NIS „backplain" řízeným proustupem výlučně pro požadované služby.
6) Nepovolit vypisování směrovacích údajů pro připojení do VPN NIS „backplain".
7) Zajistit vzájemné oddělení a prostupy LAN připojených sítí KSP jednotlivých složek a krajů, což umožní odebírání potřebných služeb bez nutnosti budovat oddělenou LAN pro projekt NIS IZS.
8) Oddělit VPN NIS „backplain" a VPN NIS „public" (stejně tak jako pro hlasové VPN „Voice backplain" a „Voice public") a prostupy mezi nimi řídit pomocí ACL nebo firewallu.
9) Zakázat propagaci směrovacích informací ostatních subjektů IZS z VPN NIS „public" do jednotlivých LAN složek IZS.

10) Ve VPN síti NIS „Voice public" budou zapojeny telefonní aparáty projektu NIS IZS, výjimkou je HZS kde je tato VPN společná pro projekty NIS a KSP.

11) Použít pro řízení prostupů v rámci hlasových VPN sítí „Voice public" a „Voice backplain" prvky SBC (Session Border Controller), Viz část C - Síť PKv6.1.

12) Omezit posílání ICMP na nezbytné případy.

13) Blokovat pakety s nastavenými IP options.

14) Blokovat pakety pokoušející se falšovat totožnost odesílatele (anti-spoofing).

15) Při výměně směrovacích informací používat autentizaci. Přijímat směrovací informace pouze ze známých bezpečných a jednoznačně identifikovatelných zdrojů. Zakázat source routing.

16) Omezit / zakázat broadcast a multicast, speciálně broadcast do nelokálních sítí.

17) Zakázat proxy ARP.

18) V odůvodněných případech použít pevné ARP záznamy.

19) Minimalizovat používání DNS.

20) Vypracovat postup pro rychlé a jednoduché zablokování jednotlivých VPN na síťových zařízeních.

21) Provádět pravidelné aplikace bezpečnostních aktualizací software síťová zařízení.

22) Požadovat jednoznačnou autentizaci pro přístup pracovníků k síťovým zařízením. Standardně používat AAA servery, ale pro nouzové případy povolit minimální počet privilegovaných účtů s lokální autentizací.

23) Nastavit autorizaci příkazů zadávaných na příkazové řádce tak, aby bylo možné na AAA serveru sledovat příkazy zadávané administrátorem na síťovém zařízení.

24) Nepovolit logický přístup jakýchkoli osob mimo správců síťových zařízení a to ani pro read only přístup.

25) Používat zamykání účtů po neúspěšných pokusech o přístup k síťovým zařízením.

26) Používat ochranu proti resetování hesel.

27) Změnit všechna předdefinovaná hesla. Zrušit předdefinované účty, pokud je to možné.

28) Nastavit automatické odhlášení uživatele po určité době nečinnosti (max 5 min).

29) Pro přístup ke směrovači používat šifrované protokoly.

30) Všechny nepoužívané protokoly na síťovém zařízení vypnout.

31) Pro povolené protokoly omezit přístup k síťovým zařízením pomocí ACL pouze z vymezených rozsahů adres.

32) Pro SNMP nepoužívat implicitní community strings.

33) Použít SNMPv3.

34) Pro různé SNMP community omezit přístup k pouze nezbytným částem MIB.

35) Definovat bezpečné NTP servery pro synchronizaci času síťových zařízení.

36) Rezervovat část systémových prostředků (paměti a procesoru) pro administrátorský přístup.

37) Zapnout ochrany proti modifikaci software a konfiguraci uložených v síťových zařízeních, pokud je na použitých zařízeních taková ochrana dostupná. Jedná se o digitální podpisy software, kontrolní součty a podobná opatření.

38) Zapnout ochrany proti útokům na úrovni dat, pokud je na použitých typech zařízení taková ochrana dostupná. Např. ochrana proti útokům typu buffer overflow.

39) K síťovým zařízením připojit IDS sondy založené na freeware (Snort). Sondy budou připojeny tak, že budou dostávat kopii veškerého provozu procházejícího síťovým zařízením a budou v něm sledovat známé útoky.

- Toto zapojení IDS sond je z hlediska zařízení v NIS IZS a zařízení ve VPN složek transparentní. Sonda může být kdykoli odebrána nebo připojena bez změny konfigurace ostatních zařízení.
- IDS sondy budou provozovány jako virtuální servery pod operačním systémem Linux. Nejsou tedy potřeba žádné licence.
- IDS sondy budou umístěny v KDC.
- Pokud IDS sonda nebude stříhat provádět inspekci veškerého provozu, neprojde příslušná část provozu inspekcí, ale síťový provoz tím nebude nijak narušen.
- IDS bude napojen na centrální (bezpečnostní) dohledový systém, který bude výskyt malware a anomálií v síťovém provozu hlásit.
- Výsledky monitoringu budou pravidelně vyhodnocovány a bezpečnostní manažer NIS IZS rozhodne podle výsledků po dohodě se Zadavatelem o realizaci dalších bezpečnostních opatření. Bezpečnostní manažer NIS IZS je osoba na straně Dodavatele pověřená dohledem nad bezpečností NIS IZS.

Bezpečnost připojení cizích zařízení k NIS IZS

Systém NIS IZS bude provozován na zařízeních Dodavatele, zařízeních Dodavatelem spravovaných a hybridních pracovních stanicích. Připojení jiných zařízení není povoleno, pouze s výjimkou pro přístup k záznamům o provozu síťových zařízení za následujících podmínek:

- Na žádost příslušné složky IZS v určité lokalitě bude definován port na přepínači, ke kterému bude možné připojit zařízení spravované příslušnou složkou.
- Na tento port bude směrovač, respektive firewall posílat část informací o síťovém provozu.
- Pro předávání informací budou použity standardní protokoly syslog a SNMP traps. Zprávy syslog budou omezeny podle typu (facility) a závažnosti (severity). Posílat se budou pouze takové zprávy, které mají význam z hlediska řešení problémů na úrovni kraje. Obdobně budou omezeny SNMP traps.

- V bezpečnostní politice NIS IZS bude definován postup a podmínky, kdy má Dodavatel právo v případě problémů či bezpečnostních incidentů odpojit zařízení, která nejsou pod jeho správou, výjma hybridních pracovních stanic.

Bezpečnost připojení vlastních zařízení k NIS IZS

Na operačních střediscích budou k NIS IZS připojeny pouze pracovní stanice a telefony NIS, a případné zařízení, na které bude posílána informace o síťovém provozu.

V DC a KDC NIS budou k NIS IZS připojena pouze schválená zařízení, která budou pod kontrolou Dodavatele NIS. Systém bude schopen ověřit pomocí systému NAC, zda má připojené síťové zařízení právo připojit se k síti NIS IZS.

Pracovní stanice na operačních střediscích, výjma hybridních pracovních stanic, budou pod kontrolou Dodavatele NIS a bude v nich pouze software nahrávaný z centrálního zdroje.

Telefony na operačních střediscích NIS budou pod kontrolou Dodavatele NIS (Dodavatel předpokládá součinnost ze strany složky PČR formou zajištění přístupu na CE směrovače).

Připojení neschváleného zařízení k NIS IZS bude kvalifikováno jako závažný bezpečnostní incident a proto budou realizována bezpečnostní opatření proti připojování neschválených zařízení k NIS IZS. Může se jednat buď o pokus připojit neschválené zařízení k nějakému nevyužitému portu aktivního síťového prvku, nebo o pokus o nahrazení schváleného zařízení neschváleným zařízením, nebo o pokus vydávat neschválené zařízení za schválené. Dodavatel zajistí kombinaci následujících opatření.

- Kompletní kontrola nad telefonem. Technickými prostředky bude zabráněno modifikaci software a nahrávání vlastního software. Malware by musel být nahrán již při zavádění software do pracovní stanice / telefonu z centrálního zdroje.
- Pracoviště OŘ bude vybaveno takovými periferními zařízeními (myš, klávesnice, atd), které nepodporují aktivní rozhraní pro připojení datových médií (např. USB disky).
- VDI servery pro pracovní stanice OŘ (ZZS, PČR) budou umístěny PČR a ZZS v rámci VPN sítě NIS „public", do této VPN sítě budou připojeny přes CE směrovače LAN složek IZS, kde jsou připojeny terminály/CPE.
- Autentizace zařízení připojených k jednotlivým portům aktivních síťových prvků. Dodavatel bude kombinovat následující metody autentizace.
  - Nechat aktivní prvek naučit se první MAC adresu pro každou VLAN („data" / „voice") a nepovolit na portu jiné MAC adresy.
  - Implementovat autentizaci pracovní stanice přímo do aplikace. V době, kdy aplikace na pracovní stanici není vytížená, bude centrální NIS IPL posílat aplikační „ping". Aplikace na pracovní stanici musí reagovat očekávaným způsobem. Pokud nereaguje, znamená to, že buď je pracovní stanice nedostupná, nebo je připojeno jiné zařízení. Informace o tom, že příslušný port na aktivním prvku je aktivní a současně zařízení připojené k portu nereaguje správně na aplikační „ping", se ukládá v bezpečnostním monitoringu (korelace dvou událostí).
  - Implementovat autentizaci telefonu přímo do aplikace. V době, kdy telefon není vytížený, bude centrální NIS IPL posílat aplikační „ping". Telefon musí reagovat očekávaným způsobem. Pokud nereaguje, znamená to, že buď je telefon nedostupný, nebo je připojeno jiné zařízení. Informace o tom, že příslušný port na aktivním prvku je aktivní a současně zařízení připojené k portu nereaguje správně na aplikační „ping", se ukládá v bezpečnostním monitoringu (korelace dvou událostí).
- Deaktivace všech nepoužívaných portů aktivních síťových zařízení.

Bezpečnost záložního propojení

Pro případ výpadku ITS doporučuje Dodavatel, aby existovala možnost komunikace mezi operačními středisky a DC NIS přes CMS2. **Zřízení těchto linek není součástí projektu NIS IZS**. V této kapitole jsou uvedeny bezpečnostní požadavky na toto propojení.

Záložní propojení bude realizováno využitím standardních přípojek KIVS. Existuje několik různých situací lišících se místem a rozsahem výpadku ITS:

- výpadek propojení z kraje k centrálním DC NIS,
- výpadek ITS v rámci kraje,
- výpadek napojení centrálních DC NIS,
- výpadek celé ITS.

Provoz je těmito VPN přeřazen do fungující centrální části ITS, která předá provoz centrální IPL ve VPN „NSPTV_data".

V obrázku výše je to situace **kraje C**.

- Kraj C nepotřebuje ke své činnosti KDC kraje D (to je nedostupné).
- Mezi složkami IZS lze v rámci kraje komunikovat přes centrální IPL umístěnou v DC NIS.
- Se složkami IZS mimo kraj C lze komunikovat přes CMS2. Tj. operační středisko HZS kraje C komunikuje s operačním střediskem kraje B přes CMS2 bez toho, aby provoz procházel přes centrální IPL. Toho je dosaženo standardní službou CMS2. „Vytvoření jedné VPN CMS2 z více VPN operátorů KIVS a ITS". Tj. CMS2 spojí všechny VPN „HZS" všech operátorů do jedné VPN „HZS_data" CMS2 a ITS.

Výpadek napojení centrálních DC NIS

V případě výpadku napojení jednotlivých centrálních DC NIS na ITS budou operační střediska IZS komunikovat se zbývajícími DC NIS, která zůstanou přes ITS připojena. V případě výpadku napojení všech DC NIS budou operační střediska komunikovat s KDC NIS ve svém kraji.

Výpadek celé ITS

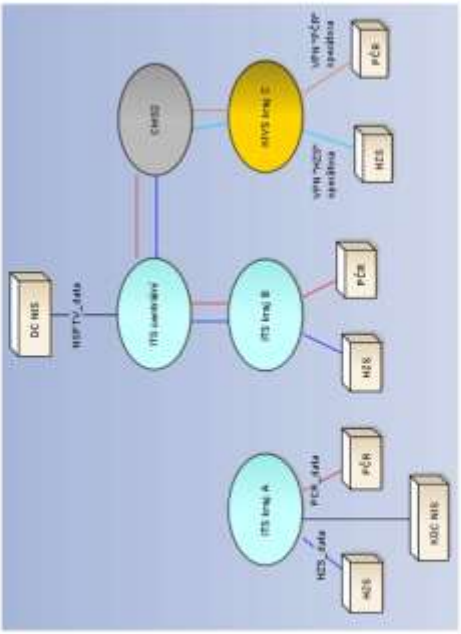
Výpadek celé ITS je kombinací výše uvedených typů výpadků. Veškerá komunikace bude probíhat přes KIVS a CMS2.

Pravidla

- Každé operační středisko NIS IZS by mělo mít dle doporučení Dodavatele záložní spojení na DC NIS přes CMS2.
- Operační střediska jednotlivých složek IZS v případě výpadku spojení přes ITS na DC NIS přecházejí na vzájemnou komunikaci v rámci kraje přes IPL v KDC. Žádné záložní spojení z operačních středisek nebude aktivováno.
- Operační střediska se přepínají na záložní připojení k DC NIS v případě výpadku spojení přes ITS na DC NIS i na KDC NIS.
- Každé DC NIS má záložní připojení do CMS2.
- DC NIS se přepíná na záložní připojení v případě výpadku svého připojení k ITS.
- Dokud funguje připojení aspoň jednoho DC NIS k ITS, komunikují všechna operační střediska s těmi DC NIS, kterým připojení k ITS funguje.
- KDC NIS žádná záložní připojení nemají.
- Komunikace na záložních připojeních musí být chráněna proti neautorizovanému odposlechnutí a monitorování (např. prostřednictvím VPN, HW/SW šifrátory apod.). Zařízení pro připojení k CMS2 přes KIVS musí být pro tento účel vybavena.

Základní schéma je uvedeno na následujícím obrázku. Kraj A je příklad kraje s fungující ITS v rámci kraje a bez připojení do centra. Kraj B je příklad kraje, kde funguje jak ITS v rámci kraje, tak propojení do centra. Kraj C je příklad kraje bez ITS na kraji.

Další komentáře k obrázku jsou dále v textu.



Výpadek propojení z kraje k centrálním DC NIS

V případě výpadku propojení ITS z kraje k centrálním DC NIS bude komunikace operačních středisek IZS s centrálními NIS přerušena a operační střediska budou spolu v rámci kraje komunikovat přes příslušné KDC NIS. Spojení mimo kraj není. V obrázku výše je to situace **kraje A**.

- Kraj A potřebuje ke své činnosti KDC kraje A.
- Mezi složkami IZS lze v rámci kraje komunikovat přes krajskou IPL umístěnou v KDC NIS kraje A.
- Se složkami IZS mimo kraj A nelze komunikovat.

Výpadek ITS v rámci kraje

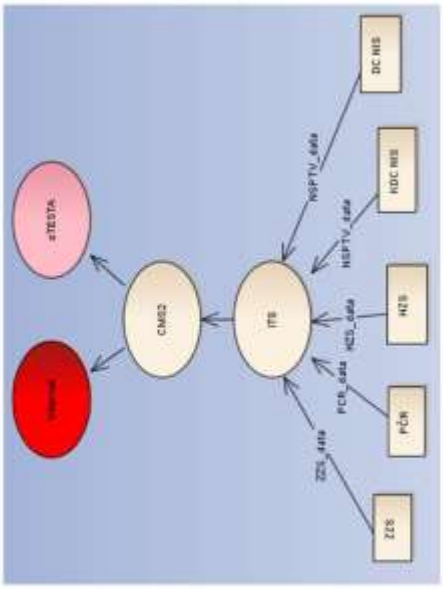
V případě výpadku ITS v rámci kraje naváží operační střediska z příslušného kraje náhradní spojení s centrálními DC NIS přes linky KIVS a CMS2. Linky KIVS z jednotlivých složek IZS z jednotlivých krajů jsou do CMS2 přivedeny jako VPN příslušného operátora KIVS. V CMS2 jsou z těchto VPN operátorů KIVS vytvořeny službami CMS2 příslušné standardní VPN ITS „HZS_data", „PCR_data" a „ZZS_data".

Připojení do Internetu

Operační střediska NIS IZS mohou mít přístup do Internetu. **Zřízení přístupu do Internetu není součástí projektu NIS IZS.** Doporučeným způsobem pro přístup do Internetu (a sTESTA) je využít služeb CMS2. Jednotlivé složky IZS mohou každá za sebe požádat provozovatele CMS2 o zřízení přístupu do Internetu, případně do sTESTA. Půjde o žádost na zřízení standardních služeb CMS2. Zejména o službu „Bezpečné připojení do Internetu". Tato služba bude nabízet zabezpečené připojení do Internetu.

Poskytovatelem připojení bude provizorovatel ITS v roli nekomerčního poskytovatele připojení k CMS2. Jednotlivé složky IZS použijí pro přístup do Internetu jim přidělené datové VPN NIS (technicky jde o VPN sítě ITS), tedy např. HZS použije VPN „HZS_data", KDC a DC použijí sběrnou VPN „NSPTV_data".

Na následujícím obrázku je schematicky znázorněno připojení HZS, PČR, ZZS, KDC NIS a DC NIS do Internetu a sTESTA přes CMS2. Orientace šipek udává směr navazování spojení, tj. od komponent NIS směrem do Internetu, respektive sTESTA.



Řízení privilegovaného přístupu k systému

Přístup administrátorů a správců systému NIS IZS bude řízen. Budou vytvořeny postupy pro získání, využívání a odebrání privilegovaného přístupu k systému. Budou naplněny minimálně následující bezpečnostní požadavky:

1) Privilegovaný přístup k NIS ISZ budou mít jen odpovědní administrátoři.
2) Pravomoci jednotlivých administrátorů budou odděleny podle SoD (Segregation of Duties, oddělení odpovědnosti).
3) Budou prováděny kontroly, že práva přidělená pracovníků nejsou v rozporu s bezpečnostní politikou a odpovídají jejich pracovní náplni.
4) Budou rušena přístupová práva pracovníkům měnícím pozici nebo opouštějícím organizaci.
5) Je vedena kompletní evidence administrátorů a přidělených privilegií.
6) Kopie hesel účtů systémových správců budou bezpečně uloženy.
7) Použití privilegovaných účtů administrátorů bude minimální a účty nebudou používány k běžné práci v systému.

Řízení změn v systému

Pro bezpečné řízení změn budou aplikována následující opatření:

1) Všechny změny v systému budou řízeny předem připraveným procesem.
2) Všechny změny budou před realizací schváleny oprávněným pracovníkem, dokumentovány a předem otestovány v testovacím prostředí, že změny nemají vliv na bezpečnost.
3) Jsou identifikovány všechny komponenty a oblasti, které změna ovlivní.
4) Jsou předem určeny osoby/role, které jsou odpovědné za změny.
5) Změny s vlivem na bezpečnostní požadavky jsou schvalovány vlastníkem aktiva systému, kterého se změna dotýká.
6) Změny budou v rámci možností realizovány v časech s nejnižší úrovní provozu.
7) Dodavatel nebude žádné aktualizace standardního software aplikovat na serverech a zařízeních automaticky, ale půjde vždy o manuální a kontrolovaný zásah.
8) Při aplikaci opravných balíčků bude Dodavatel dodržovat zásady (s výjimkou situací, kdy nutnost aplikace balíčků bude kritická, např. kvůli vysokému ohrožení NIS IZS existující zranitelnosti):
   a. Centrální systémy NIS IZS budou umístěny ve třech různých DC. Dodavatel aplikuje balíčky nejprve v DC3 a teprve po vyzkoušení v DC3 postupně s časovým odstupem na stejná zařízení v DC1 a DC2. Odstup bude zvolen podle typu zařízení, typu opravy a míře ohrožení existující zranitelnosti.

3) Plány a postupy budou identifikovat zapojení jednotlivých osob a jejich odpovědnosti. Budou dokumentovány role a odpovědnosti osob a týmů mající pravomoci během a po incidentu.
4) Postupy a plány budou přezkoumávány a aktualizovány při významných změnách v procesech nebo technologií NIS IZS a vždy, když se odhalí nedostatky.
5) Všechny nouzové postupy a procesy budou dokumentovány, aby mohly být později vyhodnoceny.
6) Všichni pracovníci Žadavatele i Dodavatele budou seznámeni s postupy a procesy pro případ stavu nouze a budou pravidelně školeni v oblastech BCM a DRP.
7) Opatření BCM a DRP budou přezkoumávána pomocí procesů testování, auditu i sebehodnocení, aby bylo zajištěno, že jsou přiměřená, vhodná a účinná. Nezávislé interní a externí audity BCM a DRP systému NIS IZS jsou prováděny odborně způsobilými osobami.

b. Pro zařízení, která jsou v jedné lokalitě zdvojena, Dodavatel aplikuje balíčky postupně vždy nejprve na jedno a potom na druhé zařízení, pokud bude tento postup technicky možný. Odstup bude zvolen podle typu zařízení, typu opravy a míře ohrožení existující zranitelnosti.
c. Dodavatel aplikuje najednou omezenou množinu oprav, aby byla usnadněna analýza případných problémů.

9) Pro řešení problémových stavů bude Dodavatel používat některý z následujících postupů, nebo jejich kombinace.
a. Návrat k předcházející verzi software (tj. odstranění balíčku).
b. Aktivace jiného zařízení jako náhrady.
c. Omezení funkcionality zařízení, pokud se omezení nevztahuje na kritické funkce zařízení.

10) Všechny nouzové změny budou zaznamenány v registru změn a budou následně detailně zdůvodněny.
11) V pravidelných intervalech je prováděna kontrola registru změn pro zajištění, aby všechny žádosti o změnu byly řádně dokumentovány.

Správa systému

Pro bezpečnou správu systému (HW i SW) budou aplikována následující opatření:

1) Správu NIS IZS bude provádět pouze autorizovaný personál Dodavatele.
2) Bude vedena evidence všech prací při správě NIS IZS. Všechny práce v rámci správy systému budou zdokumentovány.
3) Během provádění správy NIS IZS je uživatelům omezeného používání systému.
4) Plánované údržby nebudou zasahovat do ostrého provozu NIS IZS.
5) Fyzický i logický přístup pracovníků provádějících správu NIS IZS bude řízen, dokumentován a kontrolován. Budou vypracovány postupy pro řízení přístupu.
6) Nepoužívané zařízení NIS IZS bude fyzicky chráněno (bezpečně uskladněno).

Řízení kontinuity a obnova po havárii

Detailní požadavky a návrh řešení pro oblast BCM a DRP jsou uvedeny v kapitole G.
Výpočet spolehlivosti tohoto prováděcího konceptu. Z pohledu bezpečnosti musí být Dodavatelem naplněny minimálně následující požadavky:

1) Pro NIS IZS budou vytvořeny plány kontinuity systému a postupy obnovení činnosti. Budou vypracovány plány krizového řízení.
2) Strategie řízení kontinuity činností bude vytvořena na základě analýzy dopadů a hodnocení rizik. Jsou identifikována rizika, která mohou způsobit narušení chodu organizace

06. Kybernetická bezpečnost NIS IZS

Bezpečnostní monitoring NIS IZS

Bezpečnostní monitoring zajistí Dodavatel. Bezpečnostní monitoring splní následující požadavky.

1) Hlášení o výskytu bezpečnostních událostí v reálném čase.
2) Možnost vyhodnocování údajů o provozu NIS IZS od všech komponent. To znamená, že produkt bude umět přijímat a zpracovávat data v těch formátech, ve kterých je produkují jednotlivé systémy a zařízení NIS IZS. Bude podporovat sběr dat pomocí standardních protokolů, které se pro tento účel používají (zejména syslog, SNMP, netflow, a WMI).
3) Vyhodnocování bezpečnostních událostí za zvolené období.
4) Vytváření standardních a příležitostných reportů.

Bude vytvořen registr bezpečnostních metrik a pravidel, na jehož základě budou vyhodnocovány události a budou nastaveny postupy pro řešení alertů a incidentů. Množina událostí, o kterých bude systém informovat pomocí alertů v reálném čase, bude minimálně zahrnovat následující bezpečnostní události:

1) Pokus o útok proti NIS IZS. Jde o události zaznamenané aktivními síťovými prvky, firewally, servery a aplikací v tom rozsahu, v jakém jsou tyto komponenty schopné útoky detekovat. Zahrnuje pokusy o [D]DOS útok, výskyt malware, výskyt nebezpečných anomálií v síťových protokolech použitých pro komunikaci mezi prvky NIS IZS.
2) Pokus o nahrazení nějaké pracovní stanice nebo telefonu na operačních střediscích NIS IZS nepovoleným zařízením. Bude detekovat centrální NIS IPL. NIS IPL bude kontaktovat pracovní stanice a telefony a bude od nich vyžadovat zprávy. Pokud zařízení, které je dostupné pod IP adresou telefonu, respektive pracovní stanice, nepošle správnou odpověď, jde o bezpečnostní událost.
3) Pokus o neoprávněné připojení zařízení do sítě NIS IZS. Půjde o detekci připojení zařízení k aktivním síťovým prvkům, které jsou součástí infrastruktury NIS IZS. Nepoužívané porty aktivních prvků budou deaktivovány. Aktivní síťové prvky budou nakonfigurovány tak, aby hlásily změnu stavu jakéhokoli portu „down" -> „up" i opačně. Bezpečnostní dohledový systém bude vyhodnocovat, zda jde o zapnutí zařízení na povoleném portu, nebo o připojení zařízení k portu, který by neměl být aktivní.
4) Změny přiřazení hardwarových adres síťových karet a jejich logických adres zařízení, která jsou součástí NIS IZS. Bude detekována změna přiřazení IP adres a MAC adres. Změna jejich přiřazení signalizuje, že buď LAN rozhraní nějakého zařízení byla DHCP serverem přiřazena nová adresa, nebo v zařízení byla vyměněna LAN karta, nebo že se někdo pokouší zaútočit svojí totožností. Předpokládá se, že IP adresy budou zařízením NIS IZS přidělovány staticky.

V případě virtuálního prostředí dochází v některých případech k přirozené změně MAC adres virtuálních serverů, např. v případě migrace virtuálního serveru mezi fyzickými servery. Tyto situace budou ze sledování vyloučeny, aby nedocházelo k false positives.

5) Pokus o změnu času některého zařízení NIS IZS. Jakýkoli pokus o změnu času zařízení NIS IZS může signalizovat pokus o narušení bezpečnosti NIS IZS. Správné nastavení času je podstatné při analýze bezpečnostních událostí, při některých metodách autentizace (certifikáty a bezpečnostní kalkulátory) a z hlediska důvěryhodnosti systémových a audimních záznamů.
6) Neúspěšný pokus o přístup k aktivnímu síťovému prvku NIS IZS. Jde o pokus o přihlášení, při kterém byť překročen maximální počet povolených neúspěšných pokusů.
7) Pokus o manipulaci s lokálním uživatelským účtem, nebo lokální uživatelskou skupinou na serveru NIS IZS. Týká se vytvoření, zrušení a změny účtu nebo skupiny. Jde o událost, ať byla operace úspěšná nebo ne a ať se jednalo o oprávněnou nebo neoprávněnou operaci. Předpokládá se, že lokální účty budou sloužit téměř výhradně pro servisní účely. Budou vytvořeny při instalaci NIS IZS a jejich změna bude výjimečná.
8) Neočekávaná aktivita pracovních stanic spojená s monitorováním prostředí, pokusy o distribuci malware nebo s únikem dat. Základní informace pro tuto analýzu je export netflow dat ze směrovačů.

Aby bylo možné požadované události sledovat, budou mít jednotlivé komponenty NIS IZS zapnuté logování a zapnutý auditing. Komponentami NIS IZS jsou zejména aktivní síťové prvky, aplikační servery a infrastruktura pro správu NIS IZS. Tím bude zajištěno, že vzájemná primární data o událostech podstatných z hlediska bezpečnosti přímo u zdroje. Tato data budou systémem bezpečnostního dohledu centralizována a centrálně vyhodnocována, oznamována (alerty) a prezentována.

Systém bezpečnostního dohledu (SIEM) bude upozorňovat na výskyt bezpečnostních událostí v reálném čase. Bude umožněno okamžité vyhodnocení událostí. Součástí bude uchování a archivace bezpečnostních záznamů pro potřeby dodatečných analýz a vyšetřování. Dodavatel bude tato data pravidelně vyhodnocovat a na základě vyhodnocení bude případně přijímat dodatečná bezpečnostní opatření a kontrolovat účinnost existujících opatření.

Systém bezpečnostního dohledu (SIEM) a systém pro zaznamenávání systémových událostí (log management) bude naplňovat minimálně následující požadavky:

1) Rozsah zaznamenávaných dat (logů) bude nastavitelný a budou zaznamenány všechny informace o událostí dle registru metrik a pravidel.
2) Logy a záznamy budou bezpečně uloženy a archivovány. Vybrané záznamy budou archivovány minimálně po dobu 5 let.
3) Nearchivované logy a záznamy budou bezpečně mičeny v rámci předem ustaveného procesu.

4) Řízení přístupu k logům a záznamům bude přísně řízen, viz kap. Řízení privilegovaného přístupu k systému.
5) Všechny zaznamenávané události budou auditovatelné v souladu s registrem bezpečnostních metrik a pravidel. SIEM bude poskytovat nástroje pro práci s logy a záznamy. Prací je myšlené vyhledávání, filtrování, zobrazení detailu o auditním záznamu apod. Budou existovat prostředky pro analýzu logů a záznamů, které umožňují exportování do databázových a textových formátů.
6) Systémy SIEM a log management budou napojeny na všechna zařízení a aplikace NIS IZS.
7) V registru metrik a pravidel budou definovány události, které budou eskalovány dále k řešení v rámci procesu řízení incidentů. Budou vyšetřovány všechny podezřelé incidenty a zjištěné pokusy o narušení bezpečnosti.

Ochrana proti virům a škodlivému kódu

Bude implementován systém na ochranu proti virům a škodlivému kódu. Bude specifikován rozsah implementace, tzn. zařízení, na kterých bude systém instalován. Systém bude udržován aktuální.

Analýza technických zranitelností

Bude implementován proces pro řízení technických zranitelností, který zajistí, že každá identifikovaná zranitelnost bude řádně řešena. Bude implementován systém pro analýzu technických zranitelností, který bude naplňovat minimálně následující požadavky:

1) Systém pro analýzu technických zranitelností bude napojen na všechna zařízení NIS IZS, aby se zjistilo, že všechna zranitelná místa a slabiny budou identifikovány a řešeny.
2) Bude kontrolována konfigurace síťových zranitelností, zda neobsahuje zranitelná místa.
3) Konfigurace síťových zařízení bude ověřována za použití specializovaných nástrojů.
4) Databáze známých zranitelností bude pravidelně aktualizována v minimálních intervalech.
5) Pro řízení a správu technických zranitelností budou určeny role a odpovědnosti.

Zálohování a archivace

Zálohování je popsáno v kap. 1.4. části A - HW PKv51 a archivace v kap. 1.3. části A - HW PKv51. Budou naplněny základní bezpečnostní požadavky na zálohování:

1) Veškeré servery, data a datová pole budou zrcadlena na záložní úložiště v jiném DC.
2) Budou vytvořeny zálohy všech klíčových dat.
3) Zálohy dat budou chráněny stejně jako ostrá data
4) Bude udržována více než jedna generace záloh.
5) Budou pravidelně testovány postupy zálohování a obnovování záloh.
6) Zálohy budou zahrnovat i programové vybavení všech aplikací.
7) Určená data budou zálohována a archivována vhodnou technologií.
8) Dodavatelem budou vytvořeny postupy pro zálohování, archivaci a zničení dat.

07. Personální a organizační bezpečnost

Bude zajištěna jasná definice kompetencí, práv a odpovědností jednotlivých rolí v systému na straně Zadavatele i Dodavatele. Obsazení všech rolí bude dokumentováno a udržováno aktuální.

Důležitým prvkem pro zajištění bezpečného provozu NIS IZS je dostatek kvalifikovaného a důvěryhodného personálu. Existují osoby, které budou mít fyzický přístup k zařízením NIS IZS, a osoby, které budou mít privilegovaný (ve smyslu vysokých oprávnění) logický přístup k zařízením NIS IZS.

Dodavatel si je vědom rizik spojených s fyzickým přístupem a logickým privilegovaným přístupem osob k zařízením NIS IZS a věnuje proto pozornost výběru osob na příslušné pozice. Nábor pracovníků se řídí interními pravidly Dodavatele. Na všech pozicích je požadován čistý trestní rejstřík a na výše uvedené pozice je požadována odpovídající kvalifikace, provádí se kontrola životopisu a zjišťují reference. S pracovníky je uzavřána dohoda o mlčenlivosti.

Pracovníci, kteří se budou podílet na zajištění provozu NIS IZS, mají odpovídající vzdělání a praxi. Dodavatel organizuje interní školení zaměstnanců v informační bezpečnosti a podle potřeby vysílá pracovníky na školení a kursy.

Dodavatel zajistí obsazení rolí správců NIS (role viz část „I - Školení") kvalifikovanými a důvěryhodnými osobami. Jde o osoby, které provádějí administraci, monitoring, dohlédování a podporu 1. a 2. úrovně celého systému NIS IZS.

Personální bezpečnost

V rámci personální bezpečnosti budou naplněny minimálně následující požadavky:

1) Pro správu systému bude vytvořen definovaný tým po celou dobu využití systému.
2) Bude připraveno úvodní školení pro pracovníky pracující s informacemi a daty NIS IZS.
3) Budou stanoveny postihy, které hrozí zaměstnancům při zanedbání bezpečnostních požadavků.
4) Všechny osoby se vztahem k NIS IZS musí podepsat závazek o zachování mlčenlivosti, pokud pro ně požadavek mlčelivosti nevyplývá přímo ze zákona nebo z pracovně právního vztahu.
5) Bude stanovena strategie bezpečnostního vzdělávání a školení pro práci s NIS IZS (pro pracovníky Dodavatele i Zadavatele).
6) Bude provedeno školení všech pracovníků pro práci s NIS IZS, které bude přizpůsobeno roli, odpovědnostem a schopnostem dotyčné osoby.
7) Je vytvořena a udržována evidence zaměstnanců, kteří se zúčastnili školení pro práci s NIS IZS.

Organizace bezpečnosti

Bezpečnost NIS IZS bude organizačně řízena ze strany Dodavatel tak, aby byla vždy a za všech okolností zajištěna požadovaná úroveň bezpečnosti systému. Budou naplněny minimálně následující požadavky:

1) Za bezpečnostní činnosti v rámci NIS IZS budou stanoveny konkrétní role a odpovědnosti
2) Budou určeni pracovníci odpovědní za přezkoumání/audit stavu bezpečnosti NIS IZS.

Řízení bezpečnostních incidentů

Budou ustaveny postupy pro řízení bezpečnostních incidentů, které budou naplňovat minimálně následující požadavky:

1) Budou vytvořeny a zavedeny postupy pro řízení bezpečnostních incidentů, včetně schéma pro hlášení incidentů a podezření.
2) Budou vypracovány pracovní postupy pro řešení incidentů.
3) Incidenty budou hlášeny schváleným způsobem.
4) Bezpečnostní incidenty budou zaznamenány v souladu se zavedenými postupy pro hlášení incidentů.
5) Všechny slabiny bezpečnosti budou bez prodlení ohlašovány.
6) Pracovníci NIS IZS nebudou sami odstraňovat vzniklé problémy, pokud k tomu nebudou odpovědnou osobou přímo vyzváni.
7) Budou zavedeny mechanismy a nástroje pro analýzu incidentu.
8) Budou shromažďovány důkazy na podporu kroků proti osobám či organizacím.
9) Budou vyšetřovány všechny podezřelé incidenty a zjištěné pokuty o narušení bezpečnosti.
10) Vyšetřování bude prováděno odpovědnými pracovníky Dodavatele v rozsahu jeho kompetence. Zadavatel poskytne při vyšetřování bezpečnostních incidentů požadovanou součinnost.
11) Po skončení vyšetřování bude vypracována zpráva pro vedení Zadavatele i Dodavatele, která bude popisovat příčiny, škody a provedené nápravné činnosti.

08. Testování bezpečnosti NIS IZS

Před zahájením provozu a následně pravidelně v průběhu používání NIS IZS budou prováděny sady bezpečnostních testů, které jsou v základu specifikovány v následujících kapitolách. Pro provádění testů budou stanoveny a naplněny následující požadavky:

1) Budou vytvořeny plány bezpečnostního testování před a po uvedení NIS IZS do provozu.
2) Pro testování bezpečnosti NIS IZS jsou vytvořena akceptační kritéria.
3) Budou stanoveny výkonnostní a kapacitní požadavky na bezpečnost systému.
4) Testy budou zahrnovat testování bezpečnostních funkcí.
5) Budou stanoveny testy, data potřebná pro testy a odhadnuty výsledky testů.
6) Závěry testů budou rozděleny podle závažnosti.
7) Testování bude prováděno podle sady standardních bezpečnostních testů.
8) Testy budou sestaveny mj. na základě znalosti slabin systému.
9) Bezpečnostní testy budou kontrolovat prosazení bezpečnostních požadavků podle akceptačních kritérií.
10) Bude prováděna kontinuální kontrola, zda jsou v systému aktivovány bezpečnostní funkce stanovené systémovou bezpečnostní politikou NIS IZS.
11) Bezpečnostní testy budou prováděny i po celou dobu vývoje systému.

Testování bezpečnosti aplikací

Preventivním prostředkem pro zajištění bezpečnosti aplikací vyvíjených vlastními silami Dodavatele bude statické testování kódu. Vyvíjené programy i programy přebírané z externích zdrojů ve zdrojovém tvaru budou testovány analyzátory zdrojových programů s cílem odhalit případné zranitelnosti v programech a odstranit je před nasazením aplikací do provozu. Týká se aplikací:

- Aplikace NSPTV.
- Aplikace TEL (telefonie).
- Aplikace REC (nahrávání).
- Centrální integrační platforma.
- Krajské integrační platformy.
- Centrální GIS.
- Krajské GIS.

Statické testování aplikací bude doplněno dynamickým testováním, které bude primárně orientováno na odolnost vůči chybám ve vstupních datech. Speciálně bude provedeno testování aplikací v následujících situacích.

- Chybějící geografická data. Aplikace je nebude mít z nějakého důvodu dostupná.
- Chyba v geografických datech. Špatný formát dat, neúplná data, pozměněná data.
- Chyba v datech posílaných z příjmu tísňového volání v DC na krajská operační střediska. Špatný formát dat, neúplná data.
- Chyba v datech posílaných z krajských operačních středisek na integrační platformu.
- Logicky nekonzistentní data posílaná přes integrační platformu.
- Chybějící lokalizační údaje o přijatém tísňovém volání.
- Chyba v lokalizačních údajích o přijatém tísňovém volání. Pozměněná data, např. nesmyslné souřadnice.
- Nedostupné úložiště pro ukládání záznamů o přijatých tísňových voláních.
- Nedostupné údaje o dopravní situaci.
- Chyba v datech o dopravní situaci.
- Nedostupné údaje o meteorologické situaci.
- Chyba v datech o meteorologické situaci.

Dodavatel provede statické i dynamické testování před nasazením aplikací do provozu. Dynamické testování provede na produkčním prostředí (ale před nasazením aplikací do provozu).

Po nasazení do provozu provede Dodavatel statickou analýzu příslušné části zdrojového kódu po větších změnách v některé aplikaci a při stejné příležitosti provede relevantní dynamické testy.

Po nasazení do provozu bude Dodavatel provádět dynamické testy pouze v testovacím nebo vývojovém prostředí.

Testování bezpečnosti infrastruktury

Před nasazením NIS IZS do provozu Dodavatel provede bezpečnostní testy infrastruktury NIS IZS na produkčním prostředí.

- Testy filtrace provozu v operačních střediscích.
  - Test: z VPN HZS_data zkusit navázat spojení s centrálním NIS IPL protokolem telnet.
    Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.
  - Test: z VPN HZS_data zkusit navázat spojení na nějakou adresu ve VPN PCR_protokolem HTTP.
    Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.
  - Test: z VPN_HZS posílat ICMP time stamp na adresu v téže VPN v jiném kraji.

- Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.
  - Test: z VPN_HZS poslat pakety s nastavenými IP options na adresu v téže VPN v jiném kraji.
    - Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.
  - Test: z VPN_HZS poslat pakety se zdrojovým IP adresami z VPN_PCR do VPN_PCR.
    - Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.
  - Test: z VPN_HZS poslat pakety s nastaveným source routing na adresu v téže VPN v jiném kraji.
    - Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.
  - Test: z VPN_HZS poslat broadcast pakety, ve kterých je cílovou IP síť (subnet) stejná VPN.
    - Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.
  - Test: na operačním středisku HZS zablokovat přístup z 1 do VPN PCR_data a vyzkoušet komunikaci s PCR přes integrační platformu, standardně jde o povolený provoz. Po testu přístup opět odblokovat.
    - Očekávaný výsledek: spojení je zablokováno a v bezpečnostním monitoringu se objeví záznam o odmítnutí spojení.
- Testy ochrany CE směrovačů v operačních střediscích.
  - Test: zadat při přihlašování k CE směrovači nesprávné heslo o jednu vícekrát, než je povolený počet neúspěšných pokusů, potom zadat správné heslo, cílem je vyzkoušet zamykání účtu po neúspěšných pokusech o přístup k CE směrovači.
    - Očekávaný výsledek: CE směrovač připojení odmítne i při zadání správného hesla a v logu routeru se objeví záznam o odmítnutí.
  - Test: zadat při přihlašování k CE směrovači nějaké standardní předdefinované jméno.
    - Očekávaný výsledek: CE směrovač připojení odmítne a v bezpečnostním monitoringu se objeví záznam o odmítnutí.
  - Test: zadat při přihlašování k CE směrovači nějaké jméno, které není mezi jmény s povoleným přístupem.
    - Očekávaný výsledek: CE směrovač připojení odmítne a v bezpečnostním monitoringu se objeví záznam o odmítnutí.
  - Test: zablokovat přístup CE směrovače k AAA serveru a zadat při přihlašování k CE směrovači lokální účet a správné heslo a potom nelokální účet a správné heslo.
    - Očekávaný výsledek: CE směrovač připojení pro lokální účet akceptuje a pro nelokální odmítne a odmítnutí zaznamená v bezpečnostním monitoringu.
  - Test: přihlásit se k CE směrovači s použitím platného jména a hesla a počkat na automatické odhlášení.
    - Očekávaný výsledek: uživatel je automaticky odhlášen.
  - Test: pokusit se k CE směrovači přihlásit s použitím protokolu telnet.
    - Očekávaný výsledek: CE směrovač nereaguje, neobjeví se výzva k zadání jména a hesla.
  - Test: pokusit se k CE směrovači přihlásit z počítače, jehož IP adresa není mezi povolenými.
    - Očekávaný výsledek: CE směrovač nereaguje, neobjeví se výzva k zadání jména a hesla.
  - Test: provést skenování portů proti CE směrovači, zjistit dostupné síťové služby.
    - Očekávaný výsledek: Podaří se zjistit pouze čísla portů.
- Test: pokusit se o SNMP přístup k CE směrovači z počítače, jehož IP adresa není mezi povolenými.
  - Očekávaný výsledek: CE směrovač nereaguje, není možné získat žádné informace.
- Test: pokusit se o SNMP přístup k CE směrovači s použitím standardních implicitních community strings.
  - Očekávaný výsledek: CE směrovač nereaguje, není možné získat žádné informace.
- Test: provést základní útoky proti operačnímu systému CE směrovačů s využitím útoků předdefinovaných v použitém nástroji, lze použít freeware nástroje (Nexpose Community edition, Nessus, OpenVAS).
  - Očekávaný výsledek: není nalezena žádná závažná zranitelnost.
- Test: provést DOS útok proti CE směrovači a v době útoku se k němu přihlásit přes správcovské rozhraní.
  - Očekávaný výsledek: k CE směrovač je možné se přihlásit i během útoku.
- Testy připojení neschváleného zařízení.
  - Test: připojit notebook k neaktivnímu portu síťového prvku a zkusit kontaktovat centrální nebo krajský NIS.
    - Očekávaný výsledek: spojení s NIS se nenavže.

- Test: připojit notebook k aktivnímu portu síťového prvku (odpojit nějakou pracovní stanici) a zkusit http na centrální nebo krajský NIS, cílem je pokusit se obejít autentizaci zařízení připojených k aktivním síťovým prvkům.
  - Očekávaný výsledek: spojení s NIS se nenaváže a v bezpečnostním monitoringu se objeví záznam o pokusu.
- Test: připojit notebook k aktivnímu portu síťového prvku (odpojit nějakou pracovní stanici) a počkat, cílem je otestovat kontrolu připojených zařízení.
  - Očekávaný výsledek: v bezpečnostním monitoringu se objeví záznam o připojení neznámého zařízení.
- Test: připojit k nevyuženému síťovému portu aktivního síťového prvku rozbočovač (hub) a k němu autentizovanou pracovní stanici a notebook a zkusit z notebooku kontaktovat centrální nebo krajský NIS.
  - Očekávaný výsledek: spojení s NIS se nenaváže a v bezpečnostním monitoringu se objeví záznam o pokusu.
- Simulace výpadku ITS a aktivace náhradních komunikačních linek.

Po nasazení NIS do provozu Dodavatel zopakuje relevantní bezpečnostní testy v testovacím nebo vývojovém prostředí NIS IZS vždy před provedením změn konfigurace komponent v produkčním prostředí.

Kontroly souladu

Systém musí procházet pravidelnými audity a kontrolami, jejímž sponzorem může být Zadavatel i Dodavatel. Audity budou napřkład následující požadavky:

a) Splnění bezpečnostních požadavků a standardů je ověřováno Dodavatelem a nezávislou třetí stranou. Aby byl zajištěn soulad mezi fyzickými, procedurálními a technickými protiopatřeními, jsou prováděny nezávislou osobou pravidelné bezpečnostní analýzy.

b) Bezpečnostní audity jsou prováděny podle předem schváleného plánu, který je revidován minimálně jednou ročně.

c) Výsledky bezpečnostního auditu jsou předkládány vedení Zadavatele i Dodavatele.

d) Jsou prováděny pravidelné i namátkové kontroly souladu faktického nastavení s bezpečnostními předpisy.

e) Jsou explicitně určeny a zdokumentovány veškeré požadavky odpovídající zákonům, nařízením a smlouvám a tyto jsou pravidelně kontrolovány.

f) Je pravidelně prováděn audit nainstalovaného programového vybavení na zařízeních NIS IZS a jsou realizována nápravná opatření v případě auditních nálezů. Jsou implementována řešení zajišťující nepřekročení limitu stanoveného licencí.

g) Jsou udržovány registry/seznamy všech aktiv/zařízení NIS IZS a je pravidelně prováděn soulad reálného stavu systému s registry.

09. Bezpečnostní dokumentace pro provoz

Pro NIS IZS bude vytvořena bezpečnostní dokumentace, která bude zahrnovat všechny bezpečnostní požadavky na vývoj, implementaci a provoz systému, včetně přesných určení rolí a odpovědností. Základní struktura bezpečnostní dokumentace NIS IZS bude následující:

1) Systémová bezpečnostní politika NIS IZS
2) Bezpečnostní směrnice/Administrátorský manuál NIS IZS
3) Bezpečnostní směrnice/Uživatelský manuál NIS IZS
4) Směrnice pro řízení bezpečnostních incidentů NIS IZS
5) Plány kontinuity a obnovy NIS IZS
6) Bezpečnostní postupy pro administrátory a uživatele (podřízení Administrátorskému a Uživatelskému manuálu)

Příloha

Rejstřík

Model 1: Rozsah NIS IZS .....Chyba! Záložka není definována.
Model 2: Připojení zařízení v KDC.....Chyba! Záložka není definována.

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

G. Spolehlivost, disaster recovery a krizové scénáře

Dokument obsahuje:	Metodiku a výpočet bezpečnosti na úrovni HW a výpočet bezpečnosti na úrovni celého systému.
Verze:	5.1b
Schválil za Dodavatele:	RNDr. Vladimír Přibramský
Aktualizace:	17/4/2014

Projekt Národní informační systém integrovaného záchranného systému (NIS IZS) Registrační číslo projektu CZ.1.06/3.4.00/11.07471

Obsah

01. Spolehlivost navrženého řešení 3
1.1 Oblast telefonie 3
1.2 Oblast SW 3
Krizové scénáře 3
1.2.1 Výpadek IPL na CDC 3
1.2.2 Výpadek databáze na CDC 4
1.2.3 Výpadek IPL na KDC 4
1.2.4 Výpadek mapových služeb na KDC 5
1.2.5 Výpadek konektivity na KDC (ostrovní provoz) 5
1.3 Oblast HW 5
Krizové scénáře 6
1.3.1 Výpadek jednoho centrálního DC 6
1.3.2 Výpadek dvou centrálních DC 6
1.3.3 Výpadek tří centrálních DC 7
1.3.4 Výpadek krajského DC 7
1.3.5 Výpadek VDI serveru 7
1.3.6 Výpadek elektrické energie 7
1.3.7 Selhání HW 7
1.3.8 Lidská chyba (manipulace s HW, nasazování nových verzí SW) 9
1.4 Oblast síťové infrastruktury 9
1.4.1 Výpadek jednoho síťového prvku v redundanci 9
1.4.2 Výpadek obou prvků v redundanci 10
1.4.3 Výpadek CDC 10
1.4.4 Výpadek KDC 10
1.4.5 Výpadek NSPTV 10
1.4.6 Odpojení kraje od ITS 10
1.4.7 Rozdělení kraje 10
1.4.8 Rozpůlení ITS 11
1.4.9 Ztrátovost na lince 11
1.4.10 Pád ITS 11

Podpis/signature:.....

01. Spolehlivost navrženého řešení

Dodavatel návrhem řešení NIS IZS zajišťuje požadovanou vysokou dostupnost a 200% zálohu všech služeb provozovaných v režimu 24x7x365 a definovanou dostupnost dle smlouvy.
Následující kapitoly popisují zajištění spolehlivosti jednotlivých subsystémů, krizové scénáře a postupy pro disaster recovery.

1.1 Oblast telefonie

Příjem tísňových volání je zajištěn na úrovni KDC a jako kritická služba má 300% zálohu. Řešení IP telefonie je navržené jako dvouvrstvá architektura. Vlastní řízení telefonie a pořizování záznamu hovoru je na úrovni KDC, část funkcionalit kontaktního centra a management nahrávek a jejich archivace je na úrovni CDC.

Systémy řízení telefonie umístěné v jednotlivých KDC musí být pro zajištění požadované míry spolehlivosti vždy zdvojené, pracující v režimu Active-Active. Pro zajištění další míry zabezpečení je hovor určený pro zpracování v rámci určitého kraje v případě nedostupnosti konektivity do hlasových bran v primární lokalitě doručen na vstupní linky „párového kraje". V případě výpadku hlasové technologie umístěné v rámci jednoho kraje bude v rámci konfigurace systémů umístěných v „párovém kraji" zajištěna přeregistrace telefonních přístrojů z takto postiženého kraje. Daného fungování bude využito v případě zachování vnitřní konektivity propojených krajských systémů. V případě výpadku obou krajských systémů, tvořících funkční pár, bude hovor směrován z veřejné sítě dle dalších nastavených kritérií (přeživ v případě HZS, přesměrování tísňových hovorů do telefonie OŘ u PČR a ZZS).

1.2 Oblast SW

Navržená architektura AAA je řešena jako 3 aktivní DC, která mají plně konzistentní data v databázi s tím, že v konzistentním stavu jsou data v databázi udržována replikačním mechanismem na úrovni ESB. Při výpadku jednoho DC jsou k dispozici dvě plnohodnotná DC. Při výpadku dvou DC je k dispozici třetí plnohodnotné DC s plně konzistentními daty a to bez přerušení provozu.

Krizové scénáře

1.2.1 Výpadek IPL na CDC

V případě, že dojde k výpadku k výpadku uzlu IPL v CDC, přebírá jeho funkcionalitu další uzel v rámci Fabric clusteru. Funkcionalita CDC není v tomto případě nijak omezena. Po jeho obnovení dohledovým centrem je uzel zapojen do Fabric clusteru a dochází k obnovení standardního režimu provozu.

V případě, že dojde k výpadku obou uzlů IPL ve Fabric clusteru v daném CDC, přestává být jako takové v rámci NIS IZS aktivní a dochází k jeho odstavení. Funkcionalita inkriminovaného CDC přebírá další CDC. MiniIPL na CDC a registruje IPL v CDC.

1.2.2 Výpadek databáze na CDC

Výpadek databáze na CDC je možný v dvojím charakteru. Databáze v rámci jedno CDC je zdvojena na dvou uzlech, které je možné v případě výpadku jednoho nahradit. Databáze je tedy plně odolná proti výpadku jednoho ze dvou nodů CDC.

V případě, že by došlo k výpadku obou uzlů databáze (ať již sehráním obou databází nebo jinou funkcionalitou CDC), dojde k odstavení provozu na dané CDC a přesměrování na další CDC. Tento zásah je možné realizovat díky použité multi-master replikaci. Replikační řešení umožní běh řešení i přes případný výpadek dvou CDC.

1.2.2.1 Scénář výpadku jednoho databázového uzlu v rámci CDC

Po výpadku aktivní databáze je automaticky přesměrována komunikace s DB pomocí failover mechanismu na druhou databázi. Poškozená databáze nebo virtuální stroj, na kterém databáze běžela je následně obnoven a zařazen do failover režimu.

1.2.2.2 Scénář výpadku dvou databázových uzlů v rámci CDC

Po výpadku obou databázových uzlů je pomocí automatizovaného monitoringu (po uplynutí timeoutu) nastavena IPL datového centra jako neaktivní. Přihlášeným operátorům je odeslána informace o nedostupnosti CDC a požadavek na novou registraci na CDC. Stejně tak je odeslána informace o nedostupnosti CDC všem krajským miniIPL, které vybírají CDC pro připojení operátorů NSPTV. Po obnovení obou DB uzlů na postiženém CDC je replikačním nástrojem enterpriseDB, dle transakčního logu dosynchronizována databáze do konzistentní podoby. Dohledové centrum na základě monitoringu zprovozní CDC jako aktivní.

1.2.2.3 Scénář výpadku databází dvou CDC

V případě výpadku funkcionality databáze na dvou CDC je veškerý provoz směrován na třetí CDC, které kapacitně dostačuje nárokům na zapojení všech operátorů. Obnova stavu databází řeší dohledové centrum, které postupně zapojí obnovené CDC a dojde k synchronizaci dat v databázích.

1.2.3 Výpadek IPL na KDC

V případě, že dojde k výpadku k výpadku uzlu miniIPL v KCD, přebírá jeho funkcionalitu další uzel v rámci Fabric clusteru. Funkcionalita KCD není v tomto případě nijak omezena. Po jeho obnovení dohledovým centrem je uzel zapojen do Fabric clusteru a dochází k obnovení standardního režimu provozu.

V případě, že dojde k výpadku obou uzlů miniIPL ve Fabric clusteru v daném KDC, přestává být miniIPL jako takové v rámci NIS IZS aktivní a dochází k jeho odstavení. Funkcionalita inkriminovaného KDC přebírá CDC. Přebírání funkcionality miniIPL KDC je realizováno v rámci automatizovaného dohledu služeb KDC. Komunikaci s telefonní službou zajišťuje IPL v CDC. V tomto případě je také nedostupný registr mapových služeb na KCD. Klienti OŘ si musejí zajistit komunikaci s předem definovaným KDC. Po obnovení funkcionality je obnovena původní komunikace miniIPL s telefonií a registr služeb na miniIPL.

1.2.4 Výpadek mapových služeb na KDC

V případě, že dojde k výpadku GISové služby na daném KDC, je nutné, aby systémy konzumující tuto službu, přešli na záložní KDC. Mechanizmus přechodu je řešen za pomoci miniIPL na KDC. MiniIPL vrací konzumujícím klientským aplikacím adresu BEST služeb na GIS, v případě lokálního výpadku jsou miniIPL vraceny adresy ze zastupujícího KDC. Výpadek služeb ArcGIS 1 (služby specifické na úrovni kraje) návrh neřeší.

Po obnovení funkcionality mapových služeb je přes miniIPL na KDC vracena opět lokální adresa mapových služeb daného KDC.

1.2.5 Výpadek konektivity na KDC (ostrovní provoz)

V případě výpadku absolutní konektivity na KDC přechází systém do režimu ostrovního provozu. Aplikace NSPTV jako taková je neaktivní v daném kraji a příjem tísňového volání je u složek ZZS a PČR přesměrován na úrovni telefonie do OŘ. U HZS je a příjem tísňového volání zajištěn přelivem hovorů do jiného předem definovaného kraje. Mapové služby pro OŘ jsou tímto výpadkem nedotčeny.

Po obnovení konektivity je příjem telefonních hovorů opět směrován na dané KDC.

V případě výpadku konektivity na ITS v KDC je možné tok datových vět z NSPTV do OŘ HZS postiženého kraje směrovat přes záložní konektivitu MPLS mezi OŘ HZS a CDC.

1.3 Oblast HW

Architektura řešení vychází z koncepce tří aktivních nezávislých DC s rozložením zátěže. Jednotlivé instance databází, souborového systému jsou rovnoměrně distribuovány přes všechna DC a využití/zátěž datového provozu je monitorována a spravována síťovým load-balancerem v HA zapojení.

V architektuře tří aktivních nezávislých CDC s rozložením zátěže na všechna tři CDC s online synchronizací databáze, souborového systému, bude nastaven nadřazený monitoring v Hypervizoru, který bude rozkládat zátěž na všechna tři DC.

Vzhledem k tomu, že je zátěž rozložena na všechna tři DC s hlavním důrazem na pražské CDC 1 a Plzeňské CDC 3 + KDC PL a Olomouc CDC 2 + KDC OL (v poměru 40+40+20), je umožněno využít část kapacity výpočetního výkonu DC v Olomouci na školení, testování a jiné servisní úkony. V případě výpadku některého DC jsou operátoři směrováni na jiné aktivní CDC. Na všech DC vždy běží celá nezávislá infrastruktura, která poskytuje operátorům stejné služby. Uživatel ve své podstatě nepozná na jaké CDC je připojen a provoz je automaticky řízen load balancery, které směrují požadavky uživatelů podle nadefinovaných pravidel. Stav datových center je monitorován z lokality nezávislé na těchto CDC/KDC.

Disaster recovery proces má popsat proces obnovy normálního provozu NIS-IZS při neočekávaném výpadku/havárii, při němž dojde k přerušení nebo omezení činnosti některé ze systémových součástí nebo výpadku více takových součástí. Příčiny výpadku mohou být následující:

- Výpadek na komunikační síti;
- Selhání HW;
- Lidská chyba (manipulace s HW, implementace nových verzí SW);
- Selhání DC (el. energie, povodně, bouřky, požáry, apod.);

Strana 50

Strana 5 (celkem stran 11)

V takovýchto případech je potřeba zajistit detekci výpadku, kontinuitu provozu, krizovou komunikaci, ochranu infrastruktury, integritu informačních systémů a obnovení provozu v době, která je definována v provozní smlouvě.

Pro detekci výpadku je nutné zařadit do infrastruktury NIS-IZS monitorovací prvek ve formě dohledového pracoviště, které bude umístěno mimo DC. Toto dohledové pracoviště bude nepřetržitě sledovat a vyhodnocovat dostupnost všech sledovaných systémů v jednotlivých DC a v případě nenadálé události a/nebo výpadku, započne proces k zajištění kontinuity provozu, zahájí krizovou komunikaci a podnikne všechny nezbytné kroky k obnovení plného provozu.

Proces zajištění kontinuity provozu spočívá v následujících krocích:

1. Detekce chyby
2. Přesměrování provozu na běžící DC
3. Stanovení příčiny a určení doby, kdy dojde k obnovení plného provozu
4. Obnova DC s výpadkem
   A. Obecná
      - Nahlášení výpadku s identifikací problému a doby jeho pravděpodobného odstranění.
      - Definovaný scénář, který je samostatně uvedený níže (např. selhání HW, viz ad. 5.2.)
      - Kontrola konzistentního stavu databázových operací.
      - Synchronizace (nebo kontrola) souborových systémů obsahujících telefonní záznamy.
      - Připojení DC zpět do provozu;
      - Kontrola desynchronizace dat ze vymilého časového okna do plné synchronního stavu.
   B. Selhání HW
      - Výměna nefunkčního HW
   C. Při lidské chybě (např. upgrade SW)
      - Obnovení VM do stavu před zásahem

Krizové scénáře

1.3.1 Výpadek jednoho centrálního DC

Po výpadku jednoho CDC budou v ostatních aktivních CDC dostupné veškeré služby NIS IZS, zátěž na aktivní 2 CDC je load balancery rozkládána v poměru 50:50. Po obnově vypadlého DC dojde k jeho uvedení do stavu shodného s aktivními DC (automaticky - dosynchronizace DB, přenesení změn na souborovém systému, manuálně – synchronizace systémových a aplikačních updatů, resp. konfigurací v případě), následně bude ručně obnoveno rozkládání zátěže opět na všechna tři CDC.

1.3.2 Výpadek dvou centrálních DC

Krizový scénář počítá s výpadkem dvou DC (najednou nebo postupně), kdy je veškerý provoz směrován na poslední zbývající CDC. Běžící CDC bude mít nastavenou automatickou politiku v Hypervizoru, který pomocí nastavených pravidel pro rozkládování systémových zdrojů zajistí přednost běhu produkčního prostředí na úkor testovacího a školícího, aby zajistilo dostatečný výkon na odbavení operátorských požadavků. Scénář obnovy počítá s postupnou obnovou nejdříve jednoho CDC a po jeho uvedení do provozu bude započata obnova zbývajícího CDC (postup bude shodný jako v případě scénáře výpadku jednoho DC).

Strana 50

Strana 6 (celkem stran 11)

a. Je odolné vůči 50 procentnímu výpadku počtu ventilátorů

b. Je odolné vůči 50 procentnímu výpadku napájecích zdrojů

c. Je odolné vůči 50 procentnímu výpadku síťových modulů

Technik vymění v rámci SLA vadný díl za běhu systému. Tyto subsystémy jsou vyměnitelné za běhu zařízení (technologie hot-plug)

d. Havárie blade serveru

Server se za běhu systému vyjme a nahradí plně funkčním serverem za běhu systému. Na něj se následně nainstaluje Hypervizor, který se zapojí do Centrální správy virtualizace, kde blade server přebere roli havarovaného serveru.

Při vyšším než 50 procentním výpadku subsystému (chlazení, zdroje, síť) se provoz automaticky pomocí load balanceru přesměruje na jiné funkční CDC a blade servery se manuálně odstaví. Následně se bude se řešit servis vadných dílů.

b) Výpadek rack serveru

a. Výpadek napájecího zdroje

b. Výpadek napájecího zdroje

c. Výpadek ventilátoru

Technik vymění v rámci SLA vadný díl za běhu systému. Tyto sub systémy jsou vyměnitelné za běhu (technologie hot-plug)

d. Závažnější závada (síť, řadič disku, CPU, RAM, základní deska atd.)

V tomto scénáři se server odstaví a technik provede potřebnou opravu. Do provozu se RACK server vrátí nainstalováním a nastavením Hypervizoru. Následně se procesně uvede do provozního stavu.

c) Diskové pole CDC/KD

a. Havárie disku (redundance dle RAID)

Technik vymění disk v rámci SLA za běhu systému. Tyto sub systémy jsou vyměnitelné za běhu (technologie hot-swap).

b. Havárie zdroje (redundance 2N)

Technik zdroj disk v rámci SLA za běhu systému. Tyto sub systémy jsou vyměnitelné za běhu (technologie hot-swap).

c. havárie řadiče

Přebírá jeho provoz druhý, v případě havárie obou (nebo příslušné police) se odstavuje diskové pole, provoz se pomocí load balanceru směruje na jiné datacentrum a technik provede výměnu dílu, otestuje a obnoví provoz diskového pole a připojí do Hypervizoru. Následně se procesně uvede do provozního stavu.

d) Archivační jednotka (HW)

a. Je odolná vůči 50 procentnímu výpadku počtu ventilátorů

1.3.3 Výpadek tří centrálních DC

Krizový scénář počítá s výpadkem tří CDC (najednou nebo postupně) a to způsobem, kdy dojde k přesměrování veškerého telefonního provozu na záložní řešení v systémech OŘ, a to do doby než bude alespoň jedno CDC zprovozněno.

1.3.4 Výpadek krajského DC

Tento scénář předpokládá nedostupnost KDC z pohledu serverové infrastruktury. Záloha pro KC zajišťuje primárně další KDC. Scénář je nutné vnímat zejména z pohledu systémů pro operační řízení (uživatelé KDC).

1.3.5 Výpadek VDI serveru

1) V tomto případě se jedná o výpadek jednoho VDI serveru v Clusteru v rámci složky (ZZS nebo PČR). Druhý server umístěný v dané lokalitě zajistí virtuální koncové stanice bez výpadku spojení. Příjem tísňových hovorů nebude nijak zasažen.

2) V tomto případě se jedná o výpadek obou VDI serverů v Clusteru v rámci složky (ZZS nebo PČR). Příjem tísňových hovorů bude v tomto případě realizován podle záložního scénáře při nedostupnosti všech pracovišť dané složky v kraji (přelив, přesměrování). V případě výpadku VDI serverů při probíhajícím hovoru se hovor neukončí. Bude možné takový hovor dovytěžit bez běžící aplikace ApNIS. V aplikaci ApNIS, u neuzavřených událostí bude umožněno i jiným operátorům dopisování informací, které byly vytěženy po pádu Clusteru VDI serverů.

1.3.6 Výpadek elektrické energie

Krizový scénář počítá s možným výpadkem napájení el. energií tak, že se předpokládá, že přívod el. energie pro potřeby napájení zařízení v serverovně DC bude rozdělen do dvou nezávislých větví, minimálně na úrovni zdvojených rozvaděčů. Do každého racku budou přivedeny dva nezávislé přívody a připojeny k PDU (Power Distribution Unit) racku, které jsou taktéž zdvojeny.

Dojde-li k výpadku jedné napájecí větve, jsou všechna zařízení v racku napájena přes zbývající PDU a odpovídající DC zdroje (které jsou v každém konkrétním zařízení taktéž zdvojeny).

Pro případ celkového výpadku dodávky el. energie od dodavatele budou v každé napájecí větvi zapojeny zdvojené UPS odpovídajícího výkonu, které umožní bezpečné uložení a zachování konzistentních stavů dat aplikací běžících v rámci NIS IZS a také případné vypnutí všech zařízení, která jsou součástí řešení NIS IZS. UPS bude schopna dodávat el. energii odpovídajícího výkonu po dobu nejméně 20 minut. K překlenutí doby přerušení dodávky el. energie bude zařízeň do el. sítě automaticky zapojen nezávislý zdroj el. energie v podobě dieselagregátu, který bude schopen dodávat minimálně takový výkon, aby byl schopen udržet provoz všech zařízení NIS IZS po libovolně dlouhou dobu, a to pouze doplňováním potřebných provozních zdrojů.

Pro případ výpadku chladícího systému DC je počítáno s jeho kompletním zdvojením v rámci celého DC v kapacitě potřebné pro udržení provozního prostředí pro všechna zařízení NIS IZS.

1.3.7 Selhání HW

Krizový scénář předchází možnému selhání jakéhokoliv HW tak, že veškerý HW je minimálně zdvojen, a to jak na úrovni základních komponent, tak i na úrovni celých DC. V případě selhání HW se počítá se zahájením servisních prací dle sjednaného SLA v provozní smlouvě.

a) Blade chassis

b. je odolná vůči 50 procentnímu výpadku napájecích zdrojů

c. je odolná vůči 50 procentnímu výpadku síťových modulů

d. je odolná vůči 50 procentnímu výpadku nosičů (tzv. serverových nosičů/modulů)

Technik vymění v rámci SLA vadný díl za běhu systému. Tyto sub systémy jsou vyměnitelné za běhu díky architektuře RAIN

V případě výpadku celé archivační jednotky přebírá automaticky celý provoz pomocí load balancéru archivační jednotka v druhém CDC. Po zprovoznění archivační jednotky je následně ručně přesměrován provoz zpět a automaticky se zahájí dosynchronizace dat.

V případě výpadku všech tří archivačních jednotek se archivovaná data ukládají na provozní diskové pole v každém CDC. Po zprovoznění jedné archivační jednotky jsou archivovaná data z provozních diskových polí automaticky přesunuta do archivační jednotky pomocí archivačního SW. Všechny 3 archivační jednotky se zprovozňují jedna po druhé a ihned do zprovoznění automaticky pomocí load balancéru a archivačního SW přechází do normálního provozního stavu. Každá zprovozněná archivační jednotka se automaticky sesynchronizuje s ostatními běžícími archivačními jednotkami.

1.3.8 Lidská chyba (manipulace s HW, nasazování nových verzí SW)

V případě lidské chyby (zpravidla chyba administrátora), se následky řeší podle typu způsobených škod, viz výše uvedené krizové scénáře. V případě nasazování nových SW release je vždy popsán mechanismus pro návrat do posledního provozního stavu. V případě zásadních změn aplikace (např. změna databázových objektů) je k nasazování vypracován podrobný scénář s tím, že bude zpravidla postupováno v následujících krocích:

1) Odstavení CDC/KDC
2) Nasazení změny
3) Otestování změny
4) Datová dosynchronizace
5) Přesměrování provozu na DC 1
6) Smoke testy
7) Odstavení DC 2 a 3
8) Nasazení změny
9) Otestování změny
10) Datová dosynchronizace
11) Obnovení plného provozu

1.4 Oblast síťové infrastruktury

1.4.1 Výpadek jednoho síťového prvku v redundanci

V případě výpadku jednoho jakéhokoliv prvku v redundanci dojde k okamžitému převzetí plné funkcionality na druhý prvek. Tato konvergence bude v řádech jednotek ms a neovlivní běžný provoz sítě. Pro příklad vypadne jeden z CE směrovačů, kontrolní mechanismy například HSRP zareaguje okamžitě změnou směrovací tabulky na druhém CE a dojde k obnovení datového okruhu. Podobně se zachová přepínačová, firewallová a load-balancerová vrstva sítě. V tomto scénáři nedojde k rozpojení datových ani telefonních spojení.

1.4.2 Výpadek obou prvků v redundanci

V případě výpadku dvou prvků v redundanci dojde k následujícím událostem.

1. Výpadek CE směrovačů

   Všechny připojené moduly systému jsou odpojeny od ITS. OS je plně nefunkční. CDC a KDC je odpojeno

2. Výpadek centrálních přepínačů CDC/KDC/OS

   OS bude plně bez jakéhokoliv připojení

   CDC/KDC budou okamžitě automaticky odpojeny od systému a bude se k nim přistupovat jako k celkovému výpadku datového centra.

3. Výpadek firewall a load-balancerů v CDC.

   CDC bude okamžitě automaticky odpojeno od systému a bude se k němu přistupovat jako k celkovému výpadku CDC. Zbylé CDC převezmou veškerou funkcionalitu za výpadlé CDC a to až do jediného zbylého CDC.

1.4.3 Výpadek CDC

V případě výpadku obou CE routerů v CDC dojde k automatickému přesměrování provozu na jiné CDC. Toto přesměrování bude iniciováno monitoringem.

1.4.4 Výpadek KDC

V případě výpadku obou CE routerů v KDC (resp. v CDC s funkcí KDC) dojde k automatickému přesměrování provozu ze všech systémů OŘ a NSPTV ZZS a PČR na jiné funkční KDC. Pracoviště NSPTV v lokalitě HZS bude v takovém případě zcela bez konektivity a bude považováno za nedostupné, příslušné tísňové hovory budou směrovány na základě pravidel pro přelivy do lokality HZS v jiném kraji.

1.4.5 Výpadek NSPTV

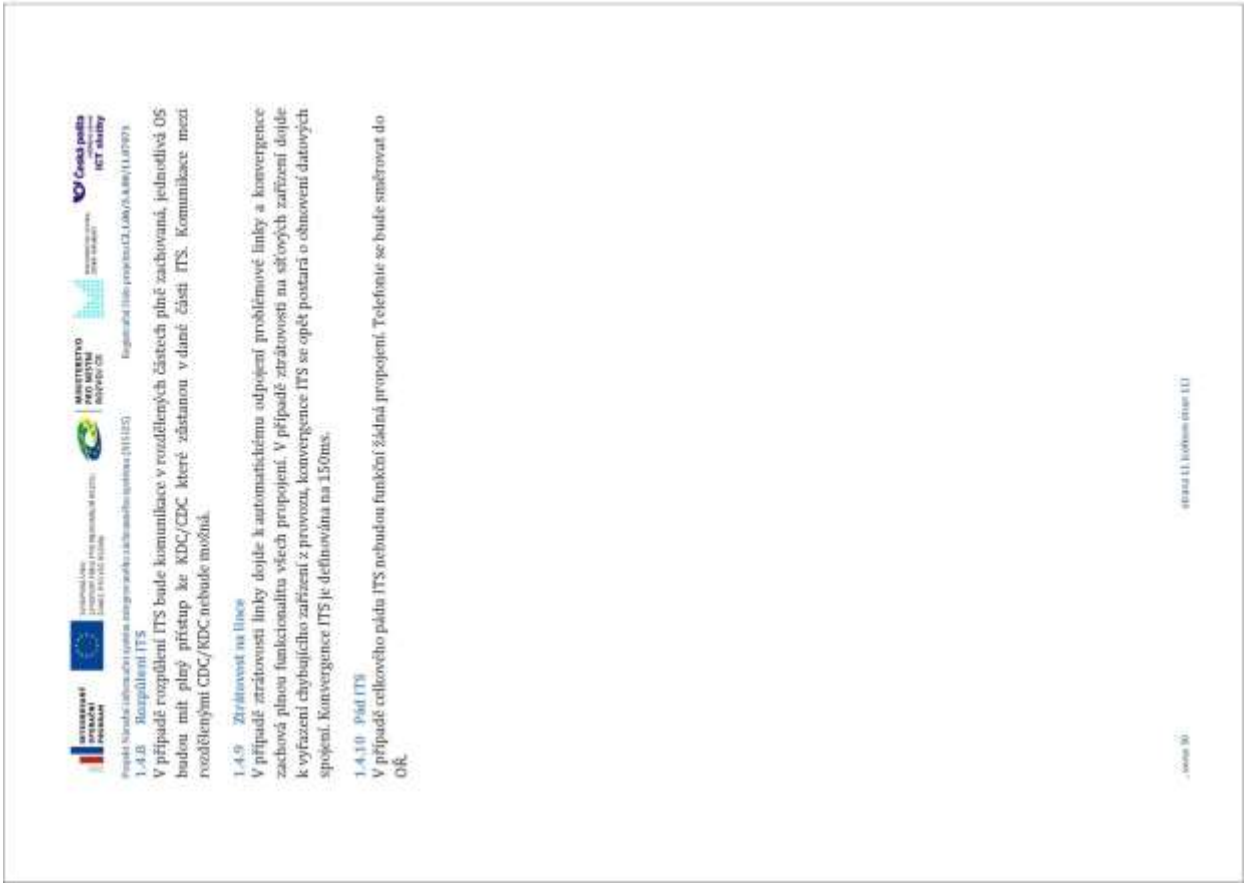
V případě výpadku obou CE routerů v lokalitě NSPTV (složky PČR, ZZS) bude taková lokalita z pohledu NIS IZS považována za nedostupnou a tísňová volání příslušná dané složce a kraji budou směrována do příslušného systému OŘ dané složky. Systémy OŘ. výjma lokality HZS budou oddělены zvláštními CE routery, tudíž je takový výpadek neovlivní.

1.4.6 Odpojení kraje od ITS

V případě odpojení celého kraje od ITS, přejde síťová infrastruktura kraje na ostrovní režim, kdy dojde k zachování plné datové komunikace v rámci kraje. Pro zajištění ostrovního režimu budou všechny směrovače v kraji v zapojení full mesh a směrování je tímto zachováno.

1.4.7 Rozdělení kraje

V případě rozdělení kraje, kdy nebude přímá komunikace mezi jednotlivými složkami, dojde k přesměrování datových toků mezi složkami a KDC pomocí okruhu sítě ITS přes republikový okruh. Toto přesměrování totiž je do 150ms, dojde však ke zvýšení latence, která by v rámci jednoho ITS okruhu nepřesáhla 30ms.



1.4.8 Rozpůlení ITS

V případě rozpůlení ITS bude komunikace v rozdělených částech plně zachovaná, jednotlivá OS budou mít plný přístup ke KDC/CDC které zůstanou v dané části ITS. Komunikace mezi rozdělenými CDC/KDC nebude možná.

1.4.9 Ztrátovost na lince

V případě ztrátovosti linky dojde k automatickému odpojení problémové linky a konvergence zachová plnou funkcionalitu všech propojení. V případě ztrátovosti na síťových zařízení dojde k vyřazení chybujícího zařízení z provozu, konvergence ITS se opět postará o obnovení datových spojení. Konvergence ITS je definována na 150ms.

1.4.10 Pád ITS

V případě celkového pádu ITS nebudou funkční žádná propojení. Telefonie se bude směrovat do OŘ.

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

H. Testování

Dokument obsahuje:	Formu zajištění, termíny dodání, instalace a zprovoznění všech dodávek.
Verze:	5.1
Schválil za Dodavatele:	Tomáš Paško
Datum aktualizace:	30/10/2013

Projekt Národní informační systém integrovaného záchranného systému (NIS IZS) Registrační číslo projektu CZ.1.06/3.4.00/11.07471

Obsah

01. Metodika ... 4
Koncept zajištění kvality ... 4
Struktura služeb zajištění kvality ... 4
02. Plánování kvality ... 5
Přínos ... 5
Plán zajištění kvality ... 5
Procesy řízení, zajištění a ověřování kvality ... 6
Organizační zajištění kvality ... 6
SW nástroje pro řízení a zajišťování kvality ... 7
Nástroj pro řízení testů ... 7
Nástroj pro zátěžové testy ... 7
Časový plán ... 7
Ověřování a validace - Testování ... 8
03. Druhy prováděných testů ... 9
Funkční testování ... 9
Integrační a systémové testy ... 9
Zátěžové testy ... 10
Bezpečnostní testy ... 11
04. Přehled rolí v procesu testování ... 12
Role na straně Zadavatele ... 12
Role na straně Dodavatele ... 13
Specifické role na straně Dodavatele ... 13
05. Artefakty procesu testování ... 15
Vstupní projektové podklady ... 15
Vstupní podklady z oblasti metodik ... 15
Výstupy z funkčního testování ... 16
06. Popis procesu testování ... 24
Začlenění testování do životního cyklu vývoje SW ... 24
Plánování testů ... 25
Příprava a provedení testů ... 26
Interní testy na úrovni subdodavatele ... 26
Systémové testování na úrovni dodavatele ... 27

Podpis/signature:.....

07. Charakteristiky kvality a metriky 30
Odkazy 33
Rejstřík 33
Akceptační testování na úrovni zadavatele 29

01. Metodika

Tato kapitola upravuje přístup ke kvalitě převáženého díla a popisuje procesy zajištění testování a kvality plánního projektu IZS.

Metodika vychází z obecně přijatých standardů (ISO 9000, ISO 9126, RUP), jejichž ověřené principy aplikuje a dále rozpracovává pro konkrétní podmínky projektu.

Koncept zajištění kvality

Metodika zajištění kvality vychází z následujících obecně přijatých a prověřených principů, jejichž spojením vytváří předpoklady pro dodání díla, jehož kvalita odpovídá požadavkům Zákazníka a minimalizuje riziko, spojená s neurčitou kvalitou výsledného produktu.

Struktura služeb zajištění kvality

Na následujícím obrázku je znázorněna dekompozice služeb v rámci zajištění kvality díla. Dominantní činností je přirozeně testování.

Model 1: Struktura služeb zajištění kvality

Cílem této struktury služeb je poskytnout zákazníkovi komplexní služby zajištění kvality v oblasti vývoje a provozu informačních systémů. Očekávaný přínos je zajištění vyšší úrovně splnění očekávání, zvýšení užitné hodnoty IS, efektivity jeho využívání v předmětu činností, minimalizace rizik, předcházení problémům.

Jedná se o ucelený soubor služeb zajištění kvality, které pokrývají celý životní cyklus IS ve všech procesech jeho realizace a provozu. Jednotlivé služby jsou navrženy tak, aby pokrývaly fázi plánování, návrhu, vyhodnocení a návrhu opatření ke zlepšení. Vytvářejí tak kompaktní celek a poskytují účinný prostředek pro komplexní zajištění kvality v oblasti IT.

Služby se týkají pouze procesů zajištění, kontroly a řízení kvality v rámci realizace a provozu IS.

02. Plánování kvality

Cíl plánování kvality je poskytnout zákazníkovi kompletní plán zajištění kvality, který vytvoří předpoklady pro kvalitní produkt a eliminuje rizika dodávky.

Přínos

Plánování kvality stanoví předem podmínky pro úspěšnou realizaci produktu a eliminuje rizika nežádoucího přístupu ke kvalitě.

Plán zajištění kvality

Výstupním artefaktem plánovací fáze zajištění kvality je plán zajištění kvality.

Plán zajištění kvality popisuje podstatné cíle v oblasti zajištění kvality projektu a všechna plánovaná opatření k zajištění kvality SW produktu v projektu, metodická a jiná ustanovení, která se vztahují ke kvalitě procesů a produktu.

Cíle kvality

Cíle kvality obsahují požadované nebo zamýšlené výstupy ve vztahu ke kvalitě produktu a projektu. Kvalitativní cíle a kritéria výstupů se proto stanovují v úvodu projektu v cílech jakosti pomocí definovaného seznamu cílových hodnot, metod měření a hodnocení charakteristik jakosti, základních kritérií akceptace výsledků projektu a způsobu jejich ověření.

Charakteristiky a kritéria kvality

Charakteristiky a kritéria kvality jsou Zadavatelem definovány v rámci akceptačních kritérií stanovených pro ověření kvality aplikace NSPTV, dimenzování HW a obecné odezev systému jako celku.

Měření a vyhodnocování kvality

Budou stanoveny měřené atributy, způsoby jejich zjišťování, zaznamenávání, vyhodnocování a reportingu. Dále budou určeny SW nástroje pro podporu měření a vyhodnocování.

Akceptační kritéria

Tato kritéria vytvářejí soubor charakteristik kvality, na základě jejichž vyhodnocení dojde k rozhodnutí, zda dílo bude převzato Zadavatelem.

Kategorizace vad

Pro stanovení závažnosti neshody zjištěné při testování je definováno 5 kategorií:

- Kritická chyba - funkce systému, které obhospodařují obchodní a technické procesy, nejsou v provozu, aplikace neumožňuje pokračovat v činnosti a neexistuje náhradní akceptovatelné řešení
- Velká chyba - chyba znemožňuje plné využití požadovanou funkčnost aplikace a má významný dopad na proces podporovaný funkčností aplikace
- Střední chyba - chyba se vyskytuje v obchodně kritickém procesu, ale je možné ji obejít
- Malá chyba - má zanedbatelný dopad na proces podporovaný funkčností aplikace

- Minimální chyba - všechny ostatní drobné chyby
- Zlepšení - nejedná se o funkční chybu aplikace, ale o nový, případně zmšnový požadavek drobného rozsahu

Závažnost doplňuje Tester při evidenci neshody. Její klasifikaci schvaluje ve fázi Interních testů Vedoucí testování Dodavatele Dodavatele, v dalších fázích testů Vedoucí testování Zadavatele.

Procesy řízení, zajištění a ověřování kvality

Řízení kvality

Řízení kvality (Quality Control, QC) je proces řízení plnění požadavků na kvalitu díla.

Zajištění kvality

Zajišťování (prověřování) kvality (Quality Assurance, QA) je proces poskytování důvěry ve splnění požadavků na kvalitu díla.

Ověřování a validace kvality

Ověřování kvality je proces zjišťování, jak jsou plněny požadavky na kvalitu díla (např. testování).

Akceptace

Zvláštní proces ověření kvality díla podle předem stanovených akceptačních kritérií, po jehož úspěšném provedení přechází užívací právo na dílo v souladu se smlouvou ze Dodavatele na Zadavatele.

Eskalace

V případě, že nedojde ke shodě v hodnocení kritérií kvality, neshod, chyb nebo dalších vlastností předmětného díla na příslušné úrovni řízení projektu, eskaluje zástupce Dodavatele vzniklý problém včetně zdůvodnění dokumentovaným způsobem na nadřízenou úroveň Dodavatele i Zadavatele.

Organizační zajištění kvality

Za zajištění kvality a její kontrolu je zodpovědný vedoucí projektu Dodavatele, který odpovídá řídícímu orgánu projektu. V užším slova smyslu má zodpovědnost za kvalitně odvedenou práci každý člen týmu Dodavatele. Dohled a metodickou pomoc v oblasti kvality zabezpečuje manažer kvality Dodavatele a v případě potřeby je také prováděn interní audit kvality projektu.

Specifikace rolí a jejich pravomocí

Na začátku projektu jsou vybráni a jmenováni dle stanovených projektových rolí členové projektového týmu na straně Zadavatele i Dodavatele. Rámcové odpovědnosti jsou definovány u popisu jednotlivých rolí, mohou být zpřesněny při jmenování a obsahují také činnosti zaměřené na splnění požadavků jakosti.

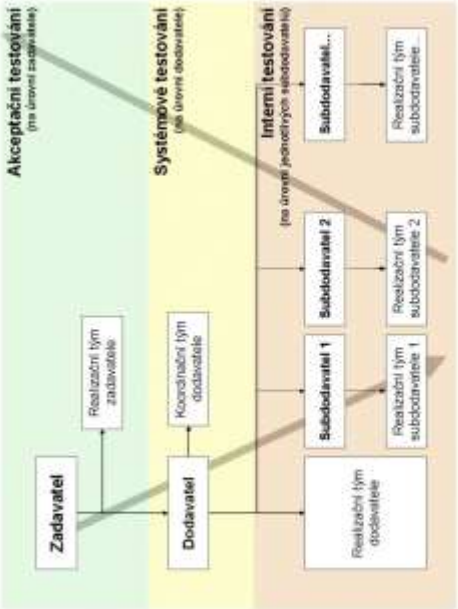
Akceptační tým

Akceptační tým je zvlášť definovaný tým Zadavatele s případnou účastí členů Dodavatele pro účely provedení uživatelských Akceptačních testů. Tento tým má za úkol prověřit výsledné

Ověřování a validace - Testování

Metodika je podkladem pro nastavení procesu testování na jednotlivých projektech.
Vzhledem k velké variabilitě SW projektů a rozdílnosti smluvně podložených požadavků Zadavatele není možné brát obecnou metodiku jako dogma, ale pouze jako zdroj informací.

Model 2: Přehled subjektů ve vazbě na etáže testů



dílo a na základě předem stanovených akceptačních kriterií vyhodnotit jeho stav a poskytnout podklady pro jeho převzetí Zadavatelem.

Běhová prostředí

Pro transparentní oddělení fází uvolnění díla do cílového provozního prostředí jsou definována různá běhová prostředí, zpravidla:

- Vývojové prostředí Dodavatele – slouží pro vývoj a Unit testy
- Testovací prostředí Dodavatele – slouží pro funkční a integrační testy Dodavatele
- Produkční prostředí Zadavatele – slouží pro pilotní a ruttinní (ostrý) provoz aplikace

SW nástroje pro řízení a zajišťování kvality

Nástroj pro řízení testů

Nástroj je nezbytnou pomůckou pro systematické řízení provádění testů a související reporting. Představuje ucelené řešení pro správu a řízení všech fází procesu testování. Nástroj zpravidla obsahuje modul pro správu testovacích požadavků ve vazbě na verze testované aplikace, modul pro plánování testů s vazbou na testovací požadavky, modul pro ukládání zdrojů pro automatizované testy s vazbou na automatizované testy, modul pro provádění a vyhodnocování běhů testů, modul pro řešení chyb testované aplikace.

Nástroj pro záťěžové testy

Nástroje jsou určeny pro tvorbu a řízení záťěžových testů, dvou a víceverstvých aplikací, včetně testování výkonnosti webových aplikací. Nástroje vytváří konzistentní, měřitelnou a opakovatelnou záťěž odpovídající reálné záťěži v provozu při maximálním zatížení všech částí systému. Dokáží měřit časové odezvy jednotlivých uživatelských činností a některé z nich monitorovat servery a sítě. Více o nástrojích pro záťěžové testování v podkapitole „Záťěžové testy".

Časový plán

Testovací práce budou probíhat po celou dobu projektu v souladu s V modelem (viz model). Nezbytnou součástí časového harmonogramu je dostatečný prostor na provedení regresních testů v plném rozsahu a záťěžových testů v závěrečné fázi projektu. Je zapotřebí počítat i s nečekaným provedením prvního kola testů a vytvořit časový prostor pro opravy zjištěných nedostatků a opakování testů tak, aby kriteria kvality dosáhla požadovaných hodnot.

Jsou stanoveny dokumenty, které souvisí s jakostí produktu a projektu např. Zadávací projektový dokument, Plán projektu, dokumenty řízení změn, protokoly o testování, akceptační kriteria atd.

Technologický test je nutné opakovat alespoň 1 x ročně pro zjištění, zda bylo správně provedeno dimenzování HW, příp. příchodnost sítě ITS. Tento kompletní test bude proveden před vlastním uvedením díla do provozu (jako součást pilotních testů) a poté alespoň 1 x ročně v rámci ostrého provozu. Z důvodu dostupnosti aplikace NSPTV lze testy výpadku komponent (výpadek datového centra, výpadek ITS, záťěž na webových službách) provádět pouze na jedním datovém centru, přičemž ostatní dvě datová centra budou zajišťovat běžný provoz. V tomto servisním okně (vyhrazeném pro testování po dohodě se zákazníkem) bude dostupnost aplikace omezena z 200% redundance na 100%.

Projekt Národní informační systém integrované záchranné služby operačního střediska (NIS IZS) — Registrační číslo projektu CZ.1.06/3.4.04/11.07971

K integračnímu testování budou podkladem pro vlastní test scénáře integračních testů, dokumentace integrační platformy (IPL) jakožto servisní sběrnice pro připojené komponenty (GIS, Telefonie, rozhraní na OŘ). Součástí dokumentace integrační platformy je zejména popis služeb, jejich vstupy a výstupy, případně WSDL schéma.

Předpokladem pro integrační testování jsou následující podmínky:

- přítomnost testovacího prostředí aplikace;
- implementace dle dokumentu „Specifikace rozhraní" z 11.2.2013 v systémech OŘ;

Nedílnou součástí integračních testů je:

- provedení testu výpadku komponent aplikace (GIS, Telefonie);
- provedení testu vizualizace operační situace;
- provedení testu datové komunikace mezi NIS IZS a systémy OŘ (datovou větou); Změna stavu (složkového) a mimořádné události.
- provedení testu importních rozhraní (aktualizace RUIAN, aktualizace mapových podkladů, replikace dat centrálního GIS na krajské GIS, import databáze geografických celků od tel. operátora).

Zátěžové testy

Zátěžové (výkonnostní) testy obecně zjišťují, jak systém uspokojí požadavky na odezvu a stabilitu v odpovídajících podmínkách. Dělíme je zejména na testy, které zkoumají chování při očekávaných provozních podmínkách, a na stress testy, které zkoumají, jak se systém chová při extrémním zatížení.

Zátěžové testování ověřuje výkonnost testované aplikace vzhledem k definovaným požadavkům a cílům zátěžového testu. Zátěžový test může být využit k následujícím účelům:

- Ověřování výkonnosti testované aplikace jako součást akceptačního řízení při přebírání aplikace od jejího dodavatele;
- Ladění výkonnosti aplikace jako součást jejího vývoje;
- Zjištění výkonnostních limitů aplikace;
- Ověření chování aplikace při výpadku jednotlivých komponent HW architektury (stress test).

Celková koncepce realizace řešení je rozdělena do následujících fází:

Model 4: Fáze realizace testování

Předpoklady pro provedení zátěžového testování:

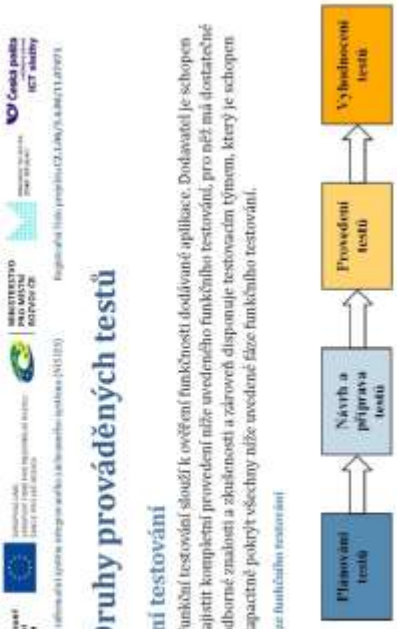
Projekt Národní informační systém integrované záchranné služby operačního střediska (NIS IZS) — Registrační číslo projektu CZ.1.06/3.4.04/11.07971

03. Druhy prováděných testů

Funkční testování

Funkční testování slouží k ověření funkčnosti dodávané aplikace. Dodavatel je schopen zajistit kompletní provedení níže uvedeného funkčního testování, pro něž má dostatečné odborné znalosti a zkušenosti a zároveň disponuje testovacím týmem, který je schopen kapacitně pokrýt všechny níže uvedené fáze funkčního testování.

Model 3: Fáze funkčního testování



Funkční testování bude probíhat na základě předem schválených testovacích scénářů předaných Dodavatelem Zadavateli. Testovací scénáře slouží k provedení dílčích funkčních testů aplikace a jejích rozhraní. Testovací scénář obsahuje zmapované požadavky, které vedly k provedení testu, vstupní a výstupní podmínky k provedení samotného testu. Dále jednotlivé kroky scénáře s označením, zda je prvkáli uživatel aplikace nebo aplikace samotná. Ke každému kroku je popsán i očekávaný výsledek (reakce aplikace).

Testovací scénáře musí být odsouhlaseny před vlastním testováním veškerými zúčastněnými složkami i dodavatelem.

Vlastní testování probíhá nejprve na straně Dodavatele a poté co je zpřístupněno i testovací prostředí Zadavateli testuje i Zadavatel (jako součást akceptačního testování). Předpokládá se dvoukolové akceptační testování. Po prvním kole se zapracují připomínky a výhrady Zadavatele, poté je provedeno druhé kolo akceptačního testování vedoucího k akceptaci díla.

Integrační a systémové testy

Integračními a systémovými testy rozumíme funkční testy vzájemného spolupůsobení jednotlivých částí (subsystémů) celého IZS. Jedná se zejména o:

Testy budou probíhat od menších celků k větším a budou vrcholit celkovými testy celého řešení, které ověří správné fungování na úrovni byznys procesů.

Provádí se obdobně jako funkční testování, testy však probíhají na testovacím prostředí, kde jsou připravena rozhraní na prostředí okolních spolupracujících systémů. Testy budou pokrývat operace, které jsou prováděny za hlavní body funkčnosti při integraci dílčích komponent celého systému včetně všech rozhraní.

Navrhujeme, aby integrační testy probíhaly vícekolově na dílčích verzích SW dle předem naplánovaného harmonogramu, aby se co nejdříve začaly ověřovat dílčí části řešení včetně vazby na okolí.

- Dodaný HW pro finální produkt NIS IZS:
- Provedena implementace řešení do všech krajských operačních středisek;
- Stejný HW a konfigurace po celou dobu testování (zajištění stejných podmínek)
- Stejná konfigurace sítě pro všechny testy (zajištění stejných podmínek)
- Reboot po provedení testu (zajištění stejných podmínek) a příprava dalšího testu.

Předpokládané scénáře zátěžových testů:

- Simulace příchozích volání pro normální zatížení ve špičce (1600 příchozích hovorů za hodinu a jejich distribuce na pracoviště NIS IZS)
- Simulace příchozích volání pro extrémní zatížení (min. 3000 příchozích hovorů za hodinu a jejich distribuce na pracoviště NIS IZS)
- Simulace příchozích zpráv „Poloha SaP" na vstupní rozhraní IPL
- Simulace příchozích zpráv „Aktualizace MU" na vstupní rozhraní IPL
- Simulace příchozích zpráv „Založení MU" na vstupní rozhraní IPL

Pro provedení testu rozhraní IPL existuje celá řada komerčních i nekomerčních nástrojů. Vzhledem k tomu, že je zasílání zpráv obsluhováno serverem Apache komponentou Active MQ, nabízí se využití integrovaného Apache Benchmarku pro simulaci zátěže.

Nástroj poskytuje konfiguraci:

- počtu zaslaných zpráv;
- počtu simulovaných konkurenčních bodů, ze kterých jsou zprávy zasílány
- výstupu výsledků testu do csv.

Životaschopnost komponenty Active MQ kontrolovat v průběhu testu v její administraci.

Bezpečnostní testy

Celé řešení IZS bude provozováno uvnitř zabezpečené sítě Zadavatele. Bezpečnostní testy proto budou mít zejména charakter ověření autentizace a autorizace k systému tak, aby nemohlo dojít ke zneužití údajů ze strany pracovníků Zadavatele. Přestože toto riziko je mnohem menší, než pokud by byl systém veřejně dostupný, nelze ho podceňovat.

04. Přehled rolí v procesu testování

Kapitola obsahuje role, které se testování přímo účastní nebo s procesy testování souvisejí. Pro každou roli je uveden popis jejích předpokládaných činností a zodpovědností ve vazbě na testování.

Role na straně Zadavatele

Tabulka 1: Role účastníci se testování na straně Zadavatele

Role	Popis činnosti
Vedoucí projektu Zadavatele	• Podílí se na řízení celého projektu na úrovni zadavatele. • Zajišťuje poskytnutí potřebných zdrojů (HW, SW, kapacity) na úrovni zadavatele. • Řídí realizační tým zadavatele. • Spolupracuje s Vedoucím projektu Dodavatele na tvorbě harmonogramu projektu • Účastní se projektových schůzek při ukončení relevantních stádií testů • Řeší problémy, které jsou na něj eskalovány.
Koordinátor testování Zadavatele	• Organizuje a řídí přípravu a provedení akceptačních testů. • Spolupracuje s Koordinátorem testování dodavatele při plánování systémových testů. • Schvaluje testovací dokumentaci – testovací scénáře, testovací případy.
Správce testovacího prostředí Zadavatele	• Instaluje verze předávaných subsystémů do testovacího prostředí • Inicializuje výchozí stav DB (systémová a uživatelská data) • Provádí zálohy a obnovy systémů a DB. • Udržuje přehled o stavu verzí jednotlivých subsystémů instalovaných do testovacího prostředí.
Tester Zadavatele	• Připravuje testovací dokumentaci pro akceptační testy na straně Zadavatele. • Provádí akceptační testy podle schválené testovací dokumentace. • Eviduje zjištěné neshody. • Vyplňuje záznamy o výsledcích akceptačních testů.

Role na straně Dodavatele

Tabulka 2: Role účastnící se testování na straně Dodavatele

Role	Popis činností
Vedoucí projektu Dodavatele	• Podílí se na řízení celého projektu – koordinuje práci jednotlivých subdodavatelů. • Ve spolupráci se subdodavateli vytváří harmonogram předávání subdodávek a kontroluje jeho plnění • Zajišťuje poskytnutí potřebných zdrojů (HW, SW, kapacity) pro činnosti spadající do kompetence dodavatele. • Řídí realizační tým dodavatele. • Ve spolupráci s Vedoucím testování definuje rozsah interních testů. • Spolupodílí se na definici rozsahu systémových a akceptačních testů.
Vedoucí vývoje Dodavatele	• Předává pracovníkům připravujícím interní, systémové a akceptační testy všechny potřebné informace o testovaném systému • Organizačně se podílí na přípravě testovacích dat • Řídí vývoj subsystému v souladu s platným harmonogramem • Přiděluje řešitele k neshodám nalezeným v průběhu všech stádií testů • Kontroluje řešení chyb v souladu s platným harmonogramem • Schvaluje klasifikaci nalezených neshod • Provádí vyhodnocení vývojových testů a vytváří protokoly v souladu s metodikou a platným harmonogramem.
Koordinátor testování Dodavatele	• Ve spolupráci s Vedoucími testování a s Koordinátorem testů zadavatele definuje rozsah a způsob provedení systémových testů (funkční, integrační a zátěžové) a organizuje činnost pracovníků Dodavatele, kteří se na těchto testech podílejí. • Koordinuje a řídí systémové testy
Správce testovacího prostředí Dodavatele	• Instaluje předávané subsystémy do testovacího prostředí. • Inicializuje výchozí stav DB (systémová a uživatelská data) • Provádí zálohy a obnovy systémů a DB. • Udržuje přehled o stavu verzí jednotlivých subsystémů instalovaných do testovacího prostředí.

Specifické role na straně Dodavatele

Tabulka 3: Specifické role účastnící se testování na straně Dodavatele

Role	Popis činností
Analytik vývoje Dodavatele	• Poskytuje konzultace Analytikovi testování při tvorbě testovacích scénářů a definici testovacích dat. • Spolupodílí se na přípravě testovacích dat. • Informuje Vedoucího testování Dodavatele, případně Analytiky testování o změnách ve schválené analytické dokumentaci.
Programátor	• Vytváří vlastní sw produkt • Provádí vývojové testy. • Opravuje detekované chyby

Role	Popis činností
Správce testovacího prostředí Dodavatele	• Instaluje veškerý aplikační sw potřebný pro testování na servery i pracovní stanice testerů. • Instaluje verze aplikace do testovací prostředí v souladu s pokyny Vedoucího vývoje a Vedoucího testování. • Spolupracuje při tvorbě a implementaci testovacích dat. • Provádí zálohy a obnovy DB.
Vedoucí testování Dodavatele	• Ve spolupráci s Vedoucím projektu Dodavatele definuje rozsah interních testů a harmonogram interních testů • Organizuje a řídí testovací tým Dodavatele • Účastní se systémových a akceptačních testů
Analytik testování Dodavatele	• Spolupracuje s Analytikem testování Dodavatele na tvorbě testovacích scénářů • Vytváří testovací dokumentaci pro daný subsystém: • Testovací scénáře • Testovací případy • Definuje požadavky na testovací data a podílí se na jejich tvorbě
Tester	• Provádí interní a systémové testy podle testovací dokumentace v souladu s platným harmonogramem • Eviduje výsledky provedení testů • Eviduje nalezené neshody • Informuje Vedoucího testování Dodavatele o případných problémech

05. Artefakty procesu testování

V rámci této kapitoly jsou definovány vstupní dokumenty, které jsou zdrojem informací pro přípravu testů a testovací dokumentace a dokumenty, které jsou vlastním výstupem z jednotlivých stádií testování.

Vstupní projektové podklady

Tabulka 4: Vstupní projektové podklady

Název dokumentu	Popis obsahu	Role zodpovědná za předání
Projektová dokumentace	• Zadavatelem schválené dokumenty, které jsou na projektu postupně vytvářeny: • Katalog uživatelských požadavků • Katalog systémových požadavků • Analytická dokumentace (Funkční specifikace) • Technická specifikace • Popis architektury celého systému • Uživatelská příručka (je-li k dispozici) • Instalační příručka (je-li k dispozici)	Vedoucí projektu Dodavatele
Harmonogram projektu	• Harmonogram celého projektu, s rozpracováním fáze vývoje jednotlivých subdodávek	Vedoucí projektu Dodavatele
Akceptační kritéria	• Požadavky zadavatele na funkčnost, výkonnost, bezpečnost systému. • Požadavky zadavatele na způsob ověřování systému – zadavatelem požadované typy testů apod. • Požadavky zadavatele na způsob převzetí systému (požadavky na akceptační testování apod.).	Vedoucí projektu Zadavatele

Vstupní podklady z oblasti metodik

Tabulka 5: Vstupní podklady z oblasti metodik

Název dokumentu	Popis obsahu	Role zodpovědná za předání
Obecná metodika testování	• Popis projektových rolí • Popis artefaktů, šablony • Nastavení procesu pro interní, systémové a akceptační testy pro subjekty zadavatel, dodavatel	Vedoucí testování Dodavatele
Typy testů	• Obsahuje stručnou charakteristiku různých typů testů • Základní specifikaci testu • Účel testu • Vhodnost použití • Podpůrné testovací nástroje	Vedoucí testování Dodavatele
Slovník pojmů	• Obsahuje základní pojmy z oblasti testování a navazujících oblastí, včetně anglických ekvivalentů	Vedoucí testování Dodavatele
Stručné postupy pro AT	• Obsahuje základní postupy pro tvorbu automatizovaných testů. • Popis rolí souvisejících s AT • Artefakty - definice vstupů a výstupů z AT • Pokyny pro vytváření skriptů • Pokyny pro management skriptů • Pokyny pro spouštění skriptů • Pokyny pro reportování výsledků testů • Best Practises pro vytváření skriptů	Vedoucí testování Dodavatele

Výstupy z funkčního testování

Tabulka 6: Výstupy z funkčního testování

Název dokumentu	Popis obsahu	Role zodpovědná za předání
Definice přístupu k testům (interní, systémové, akceptační)	Bude vytvořen jeden dokument pro všechna stádia testů (interní, systémové, akceptační) - bývá to tak zpravidla v případě, kdy se projekt řídí centrálně metodikami Zadavatele, případně Dodavatele. Dokument zpravidla obsahuje: • Definici jaká stádia testů budou na projektu probíhat (interní, systémové, akceptační) • Specifikaci jaké typy testů budou v rámci jednotlivých stádií testů realizovány. • Nastavení postupů pro jednotlivá stádia testování na projektu, • Definici požadavků na testovací dokumentaci, šablony. • Definici počtu kol pro jednotlivá stádia testů, které budou realizovány. • Definici požadavků na podpůrné testovací nástroje. • Definici požadavků na lidské zdroje (testovací tým) – role, které se testování účastní, jejich práva a povinnosti.	Koordinátor testování zadavatele / Koordinátor testování dodavatele Část pro interní testy: Vedoucí testování Dodavatele

Název dokumentu	Popis obsahu	Role zodpovědná za předání
Harmonogram testování	Harmonogram testování je součástí projektového harmonogramu. Harmonogram zahrnuje: • období pro plánování – příprava a schválení metodických a rozsahových dokumentů pro jednotlivá stádia testování • období na přípravu testovací dokumentace – testovací scénáře, testovací případy a testovací data • termíny předání dokumentace ke schválení ze strany zadavatele / dodavatele • termíny vlastního provedení jednotlivých stádií testů	Koordinátor testování zadavatele / Koordinátor testování dodavatele ve spolupráci s Vedoucím projektu Část pro interní testy – Vedoucí projektu ve spolupráci s Vedoucím testování
Definice rozsahu testů (část pro interní testy)	Dokument obsahuje: • Definici testovacího týmu Dodavatele – zařazení konkrétních pracovníků Dodavatele do definovaných rolí. • Vazbu na ostatní subjekty – doplnění konkrétních pracovníků na straně zadavatele a dodavatele do rolí Koordinátorů testů, s nimiž bude Vedoucí testování komunikovat při upřesňování požadavků na testování a návrhu scénářů testů. • Sumarizaci požadavků na interní testování – vychází se z akceptačních kritérií zadavatele. Kromě funkčních požadavků by měly obsahovat i tzv. nefunkční požadavky – např. vzhled GUI, validace, číselníky, požadavky na jazykové mutace, nápovědu, na dokumentaci, na výkonnost, doby odezvy aj. • Definici způsobu přípravy testovacích dat (předpokládané současnosti všech subjektů). • Dokument podléhá schválení ze strany zadavatele a dodavatele.	Vedoucí testování Dodavatele i Zadavatele

Název dokumentu	Popis obsahu	Role zodpovědná za předání
Definice rozsahu testů (část pro systémové testy)	Dokument obsahuje: • Definici testovacího týmu pro systémové testy: • tým pro funkční testy – zařazení konkrétních pracovníků subdodavatelů do rolí definovaných v tomto dokumentu, • tým pro integrační testy – pracovníci dodavatele, subdodavatelů • tým pro zátěžové testy, případně pro jiné typy testů požadované zadavatele. • Vazbu na ostatní subjekty – doplnění konkrétních pracovníků na straně zadavatele a dodavatele do rolí Koordinátorů testů. • Sumarizaci požadavků na systémové testy – vychází se z požadavků definovaných v Plánu interních testů pro jednotlivé subdodávky. • Definice počtu kol pro jednotlivé typy testů, které budou realizovány. • Organizace pracovišť pro jednotlivé testovací týmy (ve vazbě na harmonogram). • Definici adresářové struktury, kde bude uložena testovací dokumentace. • Definici způsobu přípravy testovacích dat (předpokládané současnosti všech subjektů). • Přístupy k podpůrným testovacím nástrojům pro pracovníky testovacích týmů. • Definici testovacího prostředí, na kterém budou testy prováděny (identifikátor testovacího prostředí, způsob identifikace verzí subsystémů v testovacím prostředí, konfigurace, přístupy) •	Koordinátor testování Dodavatele i Zadavatele

Název dokumentu	Popis obsahu	Role zodpovědná za předání
Definice rozsahu testů (část pro akceptační testy)	Dokument obsahuje: • Definici testovacího týmu pro akceptační testy: • tým pro funkční testy – zařazení konkrétních pracovníků zadavatele do rolí definovaných v tomto dokumentu, • tým pro integrační testy – pracovníci zadavatele, dodavatele • tým pro zátěžové testy, případně pro jiné typy testů požadované zadavatele. • Vazbu na ostatní subjekty – doplnění konkrétních pracovníků na straně všech subjektů, jejichž součinnost bude požadována v průběhu akceptačních testů. • Sumarizaci požadavků na akceptační testy – vychází se z požadavků definovaných v dokumentu Definice přístupu k testům. Na žádost zadavatele mohou být tyto požadavky redukovány. • Organizace pracovišť pro jednotlivé testovací týmy (ve vazbě na harmonogram). • Definici adresářové struktury, kde bude uložena testovací dokumentace. • Přístupy k podpůrným testovacím nástrojům pro pracovníky testovacích týmů. • Definici testovacího prostředí, na kterém budou testy prováděny (identifikátor testovacího prostředí, způsob identifikace verzí subsystémů v testovacím prostředí, konfigurace, přístupy)	Koordinátor testování Zadavatele i Dodavatele
Testovací dokumentace	Testovací dokumentace je vytvářena testovacím týmem subdodavatele v průběhu přípravy a provádění interních testů. Slouží jako vstup pro systémové testy na úrovni dodavatele a může sloužit jako podklad pro akceptační testy na úrovni zadavatele. Testovací dokumentace obsahuje: • Testovací scénáře – návrh oblastí a průchodů, které budou funkčně testovány • Testovací případy – rozpracování scénářů na podrobnou úroveň – popis postupu při testu a očekávaného chování aplikace ve vazbě na testovací data (obsahují i testovací data potřebná pro provedení testů) • Testovací data – specifikace a příprava probíhá za součinnosti všech zúčastněných subjektů. Testovací data mohou být přímo součástí testovacích případů nebo v samostatných souborech.	Analytik testování subdodavatele
Záznam výsledků testů	V případě, kdy není použit podpůrný testovací nástroj, který umožňuje automatickou evidenci výsledků testů, jsou výsledky provedených testovacích případů průběžně zaznamenávány do připravených formulářů, včetně vazby na případnou evidovanou neshodu.	Tester subdodavatele (interní testy) / (systémové testy) Tester zadavatele (akceptační testy)

Název dokumentu	Popis obsahu	Role zodpovědná za předání
Protokol o provedení interních testů	Dokument se vytváří při ukončení stádia interních testů a předání aplikace k systémovým testům. Dokument zpravidla obsahuje: • Název a verzi testovaného subsystému. • Obsahuje identifikátory jednotlivých testovacích případů ve vazbě na testovací scénář a záznam o stavu jejich provedení: • OK – test proběhl bez chyby (skutečné chování aplikace odpovídá popsanému očekávanému chování) • ERR – test proběhl s chybou – protokol obsahuje jednoznačný identifikátor chyby • Statistické přehledy o počtu detekovaných chyb, tříděné dle závažnosti. • Obsahuje kompletní seznam a popis neodstraněných chyb, s nimiž je subsystém předáván k systémovému testu. • Obsahuje metriku – počet chyb detekovaných v průběhu interních testů na jednotku kódu (KLOC – na tisíc programových řádků). Počítají se řádky celého subsystému. Protokol podepisuje Vedoucí projektu a Vedoucí testování subdodavatele.	Vedoucí testování subdodavatele

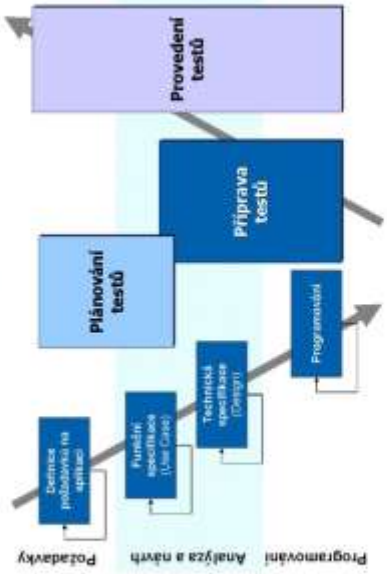
Název dokumentu	Popis obsahu	Role zodpovědná za předání
Protokol o provedení systémových testů	Dokument se vytváří při ukončení stádia systémových testů a předání aplikace k akceptačním testům. Může být rozdělen do částí pro funkční, integrační a jiné typy testů. Jednotlivé části obsahují: • Název a verzi testovaného subsystému. • Identifikátor testovacího prostředí, na němž byly testy prováděny. • Identifikátory jednotlivých testovacích případů ve vazbě na testovací scénář a záznam o stavu jejich provedení: • OK – test proběhl bez chyby (skutečné chování aplikace odpovídá popsanému očekávanému chování) • ERR – test proběhl s chybou – protokol obsahuje jednoznačný identifikátor chyby • Statistické přehledy o počtu detekovaných chyb, tříděné dle závažnosti • Kompletní seznam a popis neodstraněných chyb, s nimiž je subsystém předáván k akceptačnímu testu. • Závěr – obsahuje dohodu Vedoucích projektů o termínech a verzích, v nichž budou odstraněny chyby nebo realizovány případné změnové požadavky. • Obsahuje metriku – počet chyb detekovaných v průběhu systémových testů na jednotku kódu (KLOC – na tisíc programových řádků). Počítají se řádky celého subsystému. Protokol podepisuje Vedoucí projektu dodavatele, Koordinátor testování dodavatele, Vedoucí projektu subdodavatele a Vedoucí testování subdodavatele.	Koordinátor testování dodavatele

Podpis/signature:……

06. Popis procesu testování

Začlenění testování do životního cyklu vývoje SW

Model G: Testování v průběhu životního cyklu vývoje SW



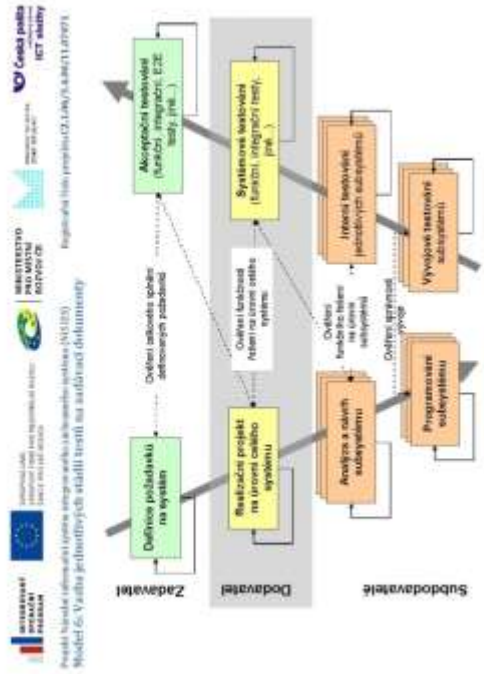
Testování je možno rozdělit do 3 fází – plánování, příprava a vlastní provedení testů. Plánováním testů je potřeba se zabývat již v úvodních projektových fázích a zahrnout do něj všechna požadovaná stádia testů (interní, systémové, akceptační) a subjekty, které se na projektu podílejí.

V případě, že není definována metodika testování ze strany zadavatele nebo dodavatele, je potřeba v této fázi nastavit procesy, definovat zodpovědnosti a výstupy.

S přípravou testů je vhodné začít již po schválení funkční specifikace ze strany zadavatele. Kvalita připravených testů a scénářů je závislá na kvalitě analytické dokumentace a na zvládnutí procesu změnového řízení ze strany vedení projektu.

Vlastní provedení testů v jednotlivých stádiích probíhá v cyklech. Nejvíce cyklů je realizováno v průběhu internich testů, kdy jsou postupně zvolňovány dílčí funkcionality aplikace. Efektivita testování v tomto stádiu je závislá na organizaci vývojových prací, tak aby mohly být pro testování uvolňovány smysluplné funkční celky a na kvalitě vývojového testování.

Název dokumentu	Popis obsahu	Role zodpovědná za předání
Akceptační protokol za testování	Závěrečný protokol pro vyhodnocení a ukončení stádia akceptačních testů. Dokument obsahuje: • Název a verzi testovaného subsystému. • Shrnutí průběhu akceptačních testů. • Identifikátor testovacího prostředí, na němž byly testy prováděny. • Identifikátory jednotlivých testovacích případů ve vazbě na testovací scénář a záznam o stavu jejich provedení: • OK – test proběhl bez chyby (skutečné chování aplikace odpovídá popsanému očekávanému chování) • ERR – test proběhl s chybou – protokol obsahuje jednoznačný identifikátor chyby. • Statistické přehledy o počtu detekovaných chyb, tříděné dle závažnosti. • Kompletní seznam a popis neodstraněných chyb s nimiž je subsystém akceptován. • Závěr: • rozhodnutí o akceptaci subsystému – může nabývat těchto hodnot – Akceptován, Akceptován s výhradou, Neakceptován. V případě neakceptace obsahuje protokol rámcový návrh dalšího postupu. • obsahuje dohodu Vedoucích projektů o termínech a verzích, v nichž budou odstraněny zjištěné chyby nebo realizovány případné změnové požadavky. • Obsahuje metriku – počet chyb detekovaných v průběhu systémových testů na jednotku kódu (KLOC - na tisíc programových řádků). Počítají se řádky celého subsystému. • Protokol podepisuje Vedoucí projektu dodavatele, Koordinátor testování dodavatele, Vedoucí projektu subdodavatele a Vedoucí testování subdodavatele.	Koordinátor testování zadavatele



Model 6: Vazba jednotlivých stádií testů na nadřazené dokumenty

Vývojové testy (white-box) ověřují správnost kódu. Zpravidla probíhají na 2 úrovních – Unit testy ověřují správnost daného kusu kódu a Assembly testy ověřují spolupráci jednotlivých elementárních programových komponent mezi sebou (jedná se vlastně o integrační testy na té nejnižší úrovni).

Interní testy ověřují správnost funkcí jednotlivých modulů oproti detailnímu návrhu. Testy končí na úrovni definovaných rozhraní mezi moduly a dalšími spolupracujícími systémy zadavatele.

Systémové testy ověřují funkcionalitu celého systému na úrovni realizačního projektu, případně globálního návrhu. Potřebné detaily jsou přebírány z detailního návrhu.

Akceptační testy ověřují celkové splnění definovaných požadavků zadavatele.

Realizace dalších typů testů (zátěžové, bezpečnostní ... apod.) může a nemusí být vázána na provedení testů funkčních a integračních, to je závislé na typu a účelu testu. Například zátěžové testy, jejichž cílem je ladění aplikace již v průběhu jejího vývoje mohou být prováděny průběžně ve vazbě na vývoj aplikace apod.

Pořadí typů testů opět může být různé, rovněž jejich zařazení do stádia systémových nebo akceptačních testů je závislé od konkrétního systému a požadavků zadavatele.

Plánování testů

Plánování všech stádií testů probíhá již ve fázi tvorby požadavků a analytické dokumentace.

Kroky procesu

- Plánování akceptačních testů – funkčních
- Plánování akceptačních testů – integračních
- Plánování systémových testů – funkčních
- Plánování systémových testů – integračních
- Plánování interních testů

Příprava a provedení testů

Interní testy na úrovni subdodavatele

Cílem interního testování je ověřit funkcionalitu předávaného subsystému před startem systémových testů a v průběhu ověřování vytvořit testovací dokumentaci, podle které budou provedena i další stádia testů (systémové, případně akceptační).

Příprava i realizace interního testování na úrovni jednotlivých subdodavatelů probíhá zpravidla zcela v režii jednotlivých subdodavatelů.

Rozsah testování na úrovni subdodavatelů zahrnuje standardně tyto typy testů:

- Vývojové unit a assembly testy – organizuje a provádí vývojový tým.
- Interní testy modulů. V případě, kdy bude subsystém rozdělen do samostatných modulů, které budou postupně předávány k testování, bude probíhat postupně ověřování těchto modulů.
- Interní funkční a integrační testy, ověřující funkčnost spolupráce jednotlivých modulů vytvářených jedním subdodavatelem (pokud spolu tyto moduly komunikují) a v případě rozhraní dílčí části systému na jiný systém, je v rámci této fáze ověřována i správnost přenosu dat do rozhraní mezi systémy (umožňuje-li to charakter projektu).

Kroky procesu

- Příprava testovacích nástrojů
- Příprava testů a dat
- Příprava testovacího prostředí
- Předání verze aplikace
- Provedení testů
- Hodnocení testů
- Ukončení testů

Vstupní kritéria pro zahájení provedení interních testů

- Moduly předané do interního testování prošly vývojovými testy a zjištěné chyby byly opraveny.
- Je připraveno funkční testovací prostředí.
- Existuje schválená analytická dokumentace, na jejímž podkladě jsou vytvářeny testovací případy.
- Byly definovány testovací scénáře, případně dopředu připraveny testovací případy.

Výstupní kritéria pro ukončení interních testů

- Byly připraveny a provedeny testovací případy pro všechny definované testovací scénáře.
- Aplikace neobsahuje žádné chyby se závažností Kritická nebo Velká.

Systémové testování na úrovni dodavatele

Na interní testy na straně subdodavatele navazují systémové testy na úrovni dodavatele. Cílem systémového testování na úrovni dodavatele je:

- Ověřit funkčnost předávaných subsystémů v jednotném testovacím prostředí.
- Ověřit integraci mezi předávanými subsystémy, vyvíjenými odlišnými subdodavateli a případně, je-li to již v této fázi možné, dalšími provozními systémy na straně zadavatele.
- Seznámit pracovníky testovacího týmu zadavatele s vyvíjeným sw a s testovacími případy, které ověřují splnění požadavků zadavatele.
- Vytvořit finální testovací dokumentaci pro akceptační testy, schválenou zadavatelem.

Za organizaci, řízení a plánování systémových testů (funkčních, integračních a případně jiných typů testů) zodpovídá Koordinátor testování dodavatele. Testy plánuje ve spolupráci s Vedoucími testování subdodavatelů a s Koordinátorem testování zadavatele. Testů se účastní testovací týmy subdodavatelů a testeři zadavatele. Testy probíhají podle testovací dokumentace připravené pro interní testy a podle testovací dokumentace pro integrační testy (jsou-li tyto součástí systémových testů).

Kroky procesu – funkční testy

- Příprava nástrojů pro evidenci neshod
- Příprava a údržba testovacího prostředí a dat
- Příprava testů a dat
- Předání verze aplikace
- Provedení funkčních testů
- Hodnocení testů
- Ukončení funkčních testů

Kroky procesu – integrační testy

Integrační testy v této fázi jsou určeny k ověření spolupráce jednotlivých subsystémů (částí systému) vyvíjených různými subdodavateli a k ověření vazeb na ostatní spolupracující systémy v prostředí Zadavatele.

Integrační testy jsou součástí testů systémových a řídí se stejným procesem. V níže uvedených krocích jsou popsány pouze specifické činnosti související pouze s integračními testy.

- Příprava a údržba testovacího prostředí a dat
- Příprava testů
- Provedení testů
- Hodnocení testů
- Ukončení integračních testů

Vstupní kritéria pro zahájení funkčních a integračních testů

- Subsystémy předané do testování prošly interními testy a splnily kritéria pro jejich ukončení.
- Je předán protokol o provedení interních testů.
- Je připraveno funkční testovací prostředí pro systémové testy
- Byla potvrzena připravenost okolních systémů k integračnímu testu.
- Byly vytvořeny testovací scénáře a testovací případy.
- Byla definována a vytvořena testovací data pro systémové funkční a zejména integrační testy.

Vstupní kritéria pro ukončení funkčních a integračních testů

- Byly provedeny všechny testovací případy pro všechny požadované testovací scénáře.
- Byla provedena všechna kola systémových testů dle specifikace v dokumentu Definice přístupu k systémovým testům (případně v dokumentu Definice rozsahu testů).
- Aplikace neobsahuje žádné chyby se závažností Kritická nebo Velká.
- Všechny zúčastněné subjekty se shodly na termínech oprav zbylých chyb a na termínech a verzích, do nichž budou zahrnuty případné změnové požadavky.

Akceptační testování na úrovni zadavatele

Cílem akceptačního testování je validace předávaného systému nebo jeho části ze strany zadavatele. Z tohoto důvodu je potřeba, aby akceptační testy probíhaly v režii zadavatele a aby se jich účastnili pracovníci, kteří znají velmi dobře problematiku, kterou daný subsystém řeší nebo se přímo podíleli na definici zadání ze strany zadavatele.

Akceptační testy probíhají podle testovací dokumentace, která byla pro tyto účely vytvořena v průběhu předcházejících stádií testů (interních a systémových) a schválena ze strany zadavatele.

Výstupy z akceptačního testování jsou jedním z podkladů pro akceptaci dodávky na obchodní úrovni.

Kroky procesu – funkční testy

- Příprava nástrojů pro evidenci neshod
- Příprava a údržba testovacího prostředí a dat
- Příprava testů
- Provedení testů
- Hodnocení testů
- Ukončení funkčních testů

Kroky procesu – Integrační a E2E testy

Cílem integračních testů je ověřit funkcionalitu dodávaného systému ve vazbě na okolní spolupracující systémy zadavatele. V první fázi je potřeba ověřit okolí všech dotčených systémů – tato část zpravidla probíhá v rámci systémových testů. V druhé fázi se realizují tzv. E2E (End-to-End) testy, kdy si Business útvary zadavatele definují kritické procesy, které jsou pak v rámci E2E testů ověřeny.

Integrační testy jsou součástí testů akceptačních a řídí se stejným procesem. V níže uvedených krocích jsou popsány pouze specifické činnosti související pouze s integračními testy.

- Příprava a údržba testovacího prostředí a dat
- Příprava testů
- Provedení testů
- Hodnocení testů
- Ukončení integračních testů

Vstupní kritéria pro zahájení funkčních a integračních testů

- Subsystémy předané do testování prošly systémovými testy.
- Ze strany subdodavatelů byly opraveny všechny chyby, případně realizovány změnové požadavky, v souladu se závěry uvedenými v Protokolu o ukončení systémových testů.
- Je předán Protokol o provedení systémových testů.
- Je připraveno funkční testovací prostředí – byla potvrzena připravenost k akceptačnímu testu.
- Jsou připraveny testovací případy pro všechny schválené testovací scénáře, které budou realizovány v rámci akceptačních testů.
- Jsou připravena potřebná testovací data.
- V případě integračních testů je potvrzena připravenost ze všech okolních spolupracujících systémů zadavatele.

Výstupní kritéria pro ukončení funkčních a integračních testů

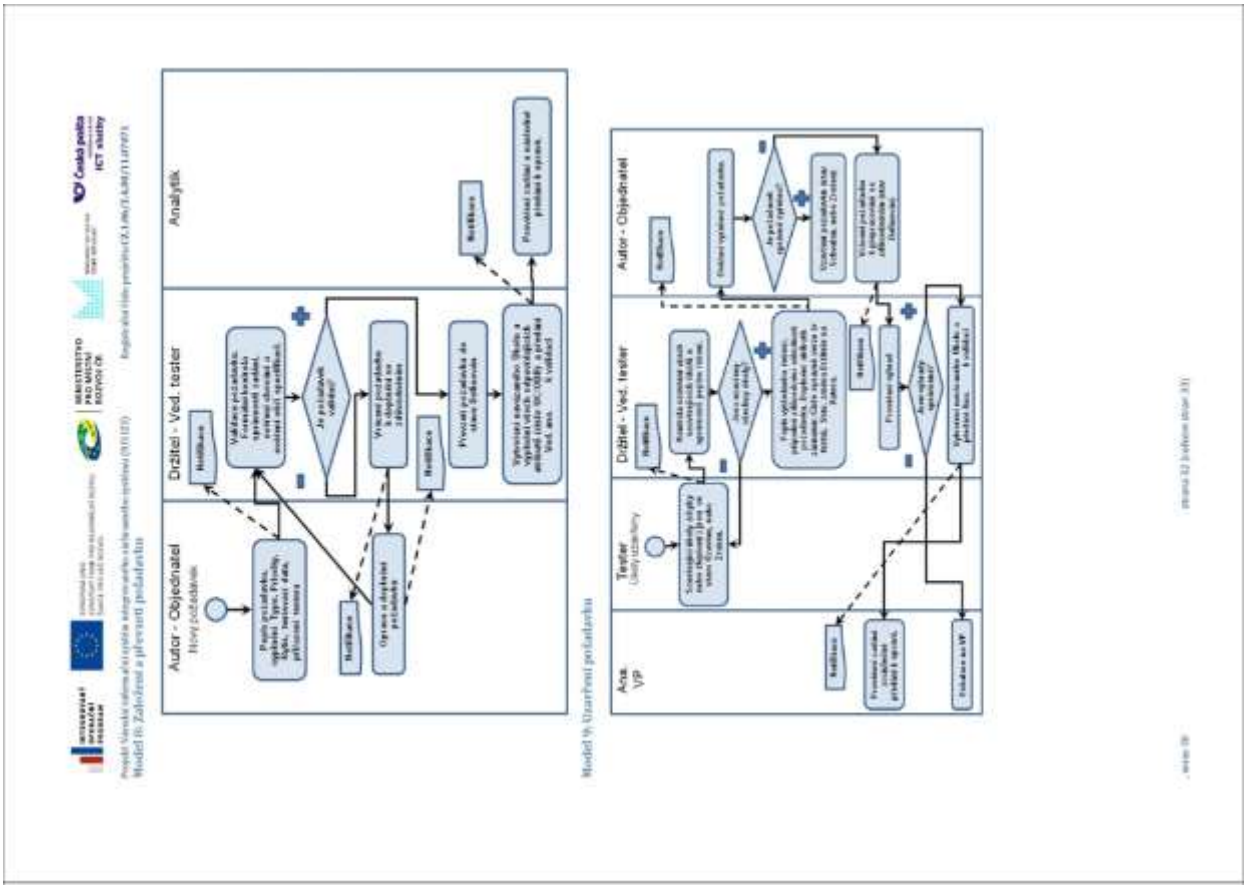
- Byly provedeny všechny testovací případy pro všechny schválené testovací scénáře.
- Byla provedena všechna kola akceptačních testů dle specifikace v dokumentu Definice přístupu k testům (případně v dokumentu Definice rozsahu testů).
- Aplikace neobsahuje žádné chyby se závažností Kritická a Velká.
- Všechny zúčastněné subjekty se shodly na termínech oprav zbylých chyb a na termínech a verzích, do nichž budou zahrnuty případné změnové požadavky.

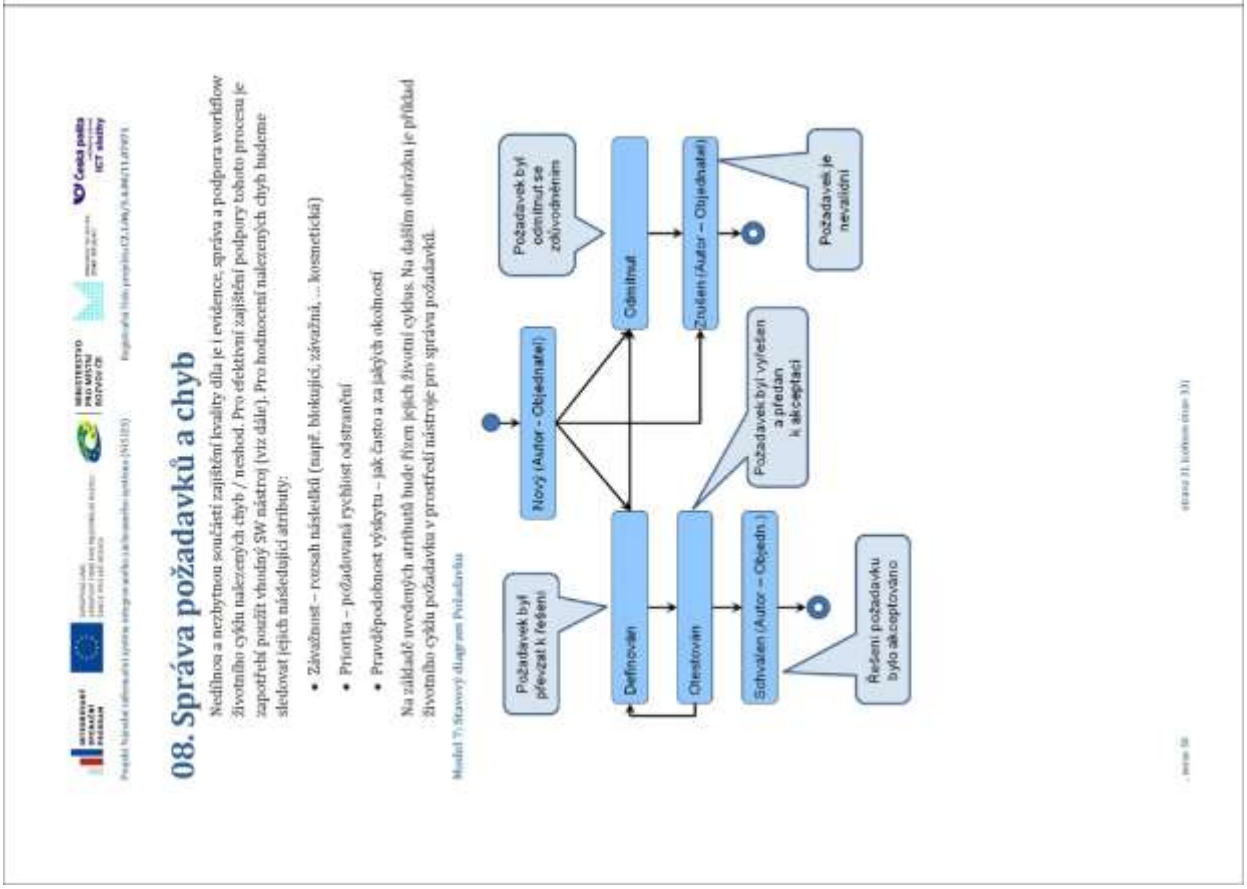
07. Charakteristiky kvality a metriky

Metriky slouží k vyhodnocování procesu testování, k odhalování nedostatků v dodržování nastavených procesů a v konečném důsledku ke zlepšování a zefektivňování procesu. Aby mohlo dojít k vyhodnocení, je potřeba v průběhu interních testů řádně evidovat všechny nalezené neshody v některém z podpůrných nástrojů a dodržovat postupy definované pro životní cyklus neshody v závislosti na použitém nástroji.

V rámci procesu testování jsou sledovány tyto základní kategorie ukazatelů:

- Chybovost SW
  - Počet chyb detekovaných v průběhu interních testů, pro jednotlivé závažnosti. V případě vývoje nového softwarového produktu, kdy je možno získat informaci o počtu zdrojových řádků testovaného softwarového produktu, je možno vyhodnotit počet chyb na jednotku zdrojového kódu. Tento ukazatel je pak možno srovnat s ostatními projekty.
- Vývoj počtu chyb v průběhu interních testů – graf závislosti počtu chyb na čase pro období interních testů.
  - Počet chyb řešených v průběhu reklamační doby pro jednotlivé závažnosti. Ukazatel se vyhodnocuje po skončení reklamační doby.
- Časová náročnost testování
  - Tento ukazatel je vyhodnocován při ukončení projektu. Jedná se o poměr člověkodnů vykázaných na testování k celkovému počtu člověkodnů vykázaných na celý projekt.


Autor - Objednatel
Nový požadavek
Držitel - Ved. tester
Analytik
Notifikace
Je požadavek správný?
Notifikace
Notifikace
Provádět zadání a schválení přehled k opravě.
Model 6: Zadávání a převzetí požadavku
Tester
Ana. VP
Autor - Objednatel
Notifikace
Model 9: Uzavření požadavku


08. Správa požadavků a chyb
Nedílnou a nezbytnou součástí zajištění kvality díla je i evidence, správa a podpora workflow životního cyklu nalezených chyb / neshod. Pro efektivní zajištění podpory tohoto procesu je zapotřebí použít vhodný SW nástroj (viz dále). Pro hodnocení nalezených chyb budeme sledovat jejich následující atributy:
• Závažnost – rozsah následků (např. blokující, závažná, ... kosmetická)
• Priorita – požadovaná rychlost odstranění
• Pravděpodobnost výskytu – jak často a za jakých okolností
Na základě uvedených atributů bude říšen jejich životní cyklus. Na dalším obrázku je příklad životního cyklu požadavku v prostředí nástroje pro správu požadavků.
Model 7: Stavový diagram Požadavku
Nový (Autor – Objednatel)
Definován
Otestován
Schválen (Autor – Objedn.)
Odmítnut
Zrušen (Autor – Objednatel)
Požadavek byl převzat k řešení
Požadavek byl odmítnut se zdůvodněním
Požadavek byl vyřešen a předán k akceptaci
Řešení požadavku bylo akceptováno
Požadavek je nevaliční

Odkazy

Rejstřík

Model 1: Struktura služeb zajištění kvality 4
Model 2: Přehled subjektů ve vazbě na stádia testů 8
Model 3: Fáze funkčního testování 9
Model 4: Fáze realizace testování 10
Model 5: Testování v průběhu životního cyklu vývoje SW 24
Model 6: Vazba jednotlivých stádií testů na zadávací dokumenty 25
Model 8: Stavový diagram Požadavku 31
Model 9: Založení a převzetí požadavku 32
Model 10: Uzavření požadavku 32

Tabulka 1: Role účastnící se testování na straně Zadavatele 12
Tabulka 2: Role účastnící se testování na straně Dodavatele 13
Tabulka 3: Specifické role účastnící se testování na straně Dodavatele 13
Tabulka 4: Vstupní projektové podklady 15
Tabulka 5: Vstupní podklady z oblasti metodik 15
Tabulka 6: Výstupy z funkčního testování 16

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

I. Školení uživatelů

Dokument obsahuje:	Typy školení všech rolí, jejich obsah a formu zajištění.
Verze:	5.1
Schválil za Dodavatele:	Tomáš Faško
Datum aktualizace:	30/10/2013

Registrační číslo projektu CZ.1.06/3.4.00/11.07071

Obsah

1.Metodika školení 3
2.Specifikace školení 4
S1 Školení operátorů 4
S2 Školení supervizorů 5
S3 Školení administrátorů 6
S4 Školení vedoucích skupin 8
S5 Školení vedoucích IZS 10

1. Metodika školení

S ohledem na množství operátorů, směnný typ provozu a specifickou problematiku budou operátory Zadavatele školit vybrané osoby (školitelé) z řad Zadavatele, které vyškolí Dodavatel v rámci školení S2.

Školitelé Zadavatele budou vyškoleni během 2 běhů dvoudenního školení S2 v časovém rozmezí šesti týdnů, tedy v termínech T až T + 42.

Na straně Dodavatele bude vyškolen ve vlastní režii odpovídající počet pracovníků pro administraci, monitoring, dohled a podporu 1. a 2. úrovně celého systému NIS, jejich školení bude probíhat separátně od školení pracovníků Zadavatele a jeho popis není tedy předmětem tohoto dokumentu.

Z každého kraje a složky a generálních ředitelství bude detailně proškolen jeden administrátor informačního systému, dále budou proškoleni specializovaní administrátoři na GIS.

Školení uživatelů Zadavatele bude organizováno podle rolí a předpokládá se v rozsahu uvedeném níže. Ve školení na úroveň S2 je zahrnuto školení S1. Pro školení na úrovni S3 je nezbytné absolvovat školení S2. Pro osoby školené na úrovni S4 a S5 je nutné absolvovat i školení S2 pro blízké seznámení se s aplikací.

Stupně školení (řazeno vzestupně od nejnižšího po nejvyšší):

- S1 Školení operátorů (toto školení provádí Zadavatel)
- S2 Školení supervizorů (toto školení provádí Dodavatele, vybraní supervizoři budou školiteli Zadavatele)
- S3 Školení administrátorů GIS (toto školení provádí Dodavatel)
- S4 Školení vedoucích krajských složek (toto školení provádí Dodavatel)
- S5 Školení vedoucích složek (toto školení provádí Dodavatel)

Celkový plán školení, vč. plánovaného počtu účastníků sumarizuje následující tabulka:

PLÁN ŠKOLENÍ						
Skupina	Rozsah	Počet osob	Složky			Počet dní
S1	Kraj – operátor	500	HZS	PČR	ZZS	1-2
S2	Kraj – supervizor	300	HZS	PČR	ZZS	2
S3	Kraj – administrátor	20	HZS			2
S4	Kraj - vedoucí složky na kraji	50	HZS	PČR	ZZS	2
S5	ČR - vedoucí pracovníci centrálních orgánů IZS	5	HZS	PČR	ZZS	2

Podpis/signature:.....

2. Specifikace školení

Specifikace školení blíže popisuje jednotlivé stupně školení podle rolí, pro které je určeno. Návrh školení včetně časového rozsahu, navrhované lokality jeho konání, počtu školených osob a především cíle daného školení s determinovanými body osnovy je popsán dále.

V souvislosti s přípravou školení bude pro všechny typy Školení Dodavatelem zpracována školící dokumentace, která bude Zadavateli k dispozici pro vlastní využití. Školící dokumentace se předpokládá následující:

- Uživatelská dokumentace daných oblastí
- Výuková a školící dokumentace
- Prezentace ze školení

Všechny tyto materiály budou účastníkům Školení k dispozici v tištěné verzi v množství jednoho výtisku.

S1 Školení operátorů

Školitelé

Školitelé pro jednotlivé bloky Školení budou nominováni Zadavatelem z řad pracovníků Zadavatele, kteří prošli školením S2.

Rozsah

Doporučený rozsah jednoho Školení je 1 - 2 dny. Doporučený počet osob na jedno Školení je 12-18.

Lokalita

Školení bude probíhat v prostorách jednotlivých uživatelů v lokalitách krajů. V těchto prostorách je nutno mít k dispozici, nebo ve spolupráci s Dodavatelem zajistit vzorové pracoviště NSPTV s koncovými prvky na testovací systémy Dodavatele.

Počet školených osob

Předpokládaný počet školených osob ze strany uživatelů je 500.

Termíny školení

T_1 až T_1 + 21

Konkrétní termíny Školení bude určovat Zadavatel v závislosti na potřebách a aktuální situaci v dané lokalitě. Školení uživatelů budou probíhat postupně v jednotlivých krajích a složkách podle postupného oživování systému NIS.

Předpokládáme, že tato Školení budou aktivně probíhat i po masivním prvotním Školení operátorů zejména v souvislosti s nástupy nových zaměstnanců, nebo doškolováním.

Cíle Školení

Cílem Školení je seznámit operátory s ovládáním aplikace NSPTV v takové míře, aby byli schopni je efektivně ovládat od příjmu a vytěžení tísňového volání přes sdílení informací o události s OŘ po nahlížení na reporting událostí. Samozřejmostí je rovněž práce s GIS.

Obsah Školení

Školení pokrývá především následující oblasti práce se systémem:

- Seznámení novinek v aplikaci
- Pozadí změn – teoretická část
- Hodnocení základních obrazovek
- Seznámení s ovládacími prvky a klávesovými zkratkami
- Lokalizace místa volání a místa události a způsoby jejího zadání
- Ovládání místopisného vyhledavače
- Klasifikace událostí
- Práce se souřadnicemi a rajonizace
- Ovládání obrazovky GIS
- Klasifikace hovorů a jejich průběh
- Uživatelská práce s telefonií
- Uživatelská práce se záznamy hovorů
- Připojení nebo konference
- Přehled probíhajících hovorů
- Editace událostí
- Práce v chybovými stavy aplikace
- Práce se základními reporty
- Osobní nastavení
- Nouzový provoz systému
- Servis desk

V úvodu bude operátorům představen samář nových funkcionalit, jako poznání těchto změn bude provedena krátká teoretická přednáška na téma architektury a koncepce nového systému. Následně budou v rámci Školení všichni účastníci detailně seznámeni se základními obrazovkami, rozmístění zobrazovaných informací a s nimi spojené ovládací prvky. Tedy zjednodušeně, kde najdou na obrazovce které informace, která pole musí být vyplněna a jakými tlačítky se spouštějí které činnosti v aplikaci a jaké klávesové zkratky jsou připojeny k jednotlivým ovládacím prvkům.
Školený bude proveden všemi hlavními poli všech obrazovek, zejména lokalizací, místopisným vyhledávačem, klasifikací události, tabulkami se součinností a rajonizací.
V rámci výuky GIS bude Školeno především následující:

- Vyhledávání v místopise
- Práce s mapovým oknem
- Ovládání mapy
- Obsah mapové kompozice
- Upřesnění polohy události pomocí mapy
- Informace o poloze
- Měření vzdálenosti

Operátorů budou Školeni k průběhu hovorů, jejich klasifikaci a metodiky konferencí a připojeních, a k metodám práce s telefonií z pozice uživatele. Zároveň budou proškoleni k práci se záznamy hovorů, zejména jejich přehrání a vyhledání.
Nakonec budou operátoři proškoleni pro práci se základními reporty, editaci událostí, nastavení osobního nastavení a s možnými chybovými stavy aplikace, nouzovým provozem systému a pravidly používání Servis desku jako takového.

S2 Školení supervizorů

Školitelé

Školitelé pro jednotlivé bloky Školení budou nominováni z řad pracovníků Dodavatele. Pro každý blok budou k dispozici dva Školitelé současně, kteří budou zvoleni tak, aby byly v maximální možné míře pokryty jak procesní, tak technické znalosti prostředí.

Rozsah

Rozsah jednoho Školení bude 2 na sebe navazující dny. Doporučený počet osob na jedno Školení je 12-18.

Lokalita

Školení bude probíhat v prostorách určených Zadavatelem na úrovni krajů, které budou upřesněny vždy nejméně 14 dní před termínem Školení.

Počet školených osob

Celkový počet vyškolených osob ze strany uživatelů bude maximálně 300.

Termíny Školení

T_1 až T_3 + 21

Předpokládané termíny jednotlivých běhů Školení jsou následující:

- 1. běh - T_{21} až T_{22} + 1
- 2. běh - T_{23} až T_{24} + 1
- 3. běh - T_{25} až T_{26} + 1
- 4. běh - T_{27} až T_{28} + 1

Školení je termínově plánované v tomto rozsahu především kvůli časové alokaci zaměstnanců Zadavatele. Vzhledem k jejich sníženému provozu bude nezbytné na každém kraji zajistit konání Školení minimálně 3x, plán tedy počítá se čtyřmi termíny Školení v každém kraji. Zadavatel se může s Dodavatelem domluvit na úpravě termínů Školení v závislosti na aktuální situaci.

Cíle Školení

Cílem Školení je seznámit účastníky Školení s architekturou aplikace NSPTV, logikou jejího fungování, procesním nastavením a funkcionalitou v takovém rozsahu, aby byli schopni nejen aplikaci ovládat, ale rovněž sami zaškolovat operátory a definovat požadavky na nastavení aplikace a řešit ve spolupráci s administrátorem chybové stavy aplikace. Školení S2 je tedy také Školením Školitelů.

Obsah Školení

- Architektura systému
- Správa znalostí operátorů
- Práce s telefonií
- Nastavení pravidel
- Lokální a celorepublikový reporting
- Exporty dat včetně nahrávek hovorů
- Servis desk

V rámci Školení budou supervizoři Školeni především z technických a metodických částí systému. Architektura systému zde bude detailně vysvětlena a budou představeny hlavní dopady nové architektury oproti architektuře současné. Zejména pak vzhledem k architektuře budou Školeny nové možnosti telefonie.
Dále budou Školeni v základních správovských rolích, především správě nastavení pravidel. Následně na blok správovských dovedností budou účastníci extenzivně Školeni k reportingu, exportům dat a práce se Servis deskem, zejména co se týče rozšířených funkcionalit oproti úrovni S1.
Nakonec bude zařazena metodická sekce, kde budou účastníci Školení proškoleni vzhledem ke správné znalosti operátorů - budou proškoleni k provádění „S1 Školení operátorů".

S3 Školení administrátorů

Školitelé

Školitelé pro jednotlivé bloky Školení budou nominováni z řad pracovníků Dodavatele. Pro každý blok budou k dispozici dva Školitelé současně, kteří budou zvoleni tak, aby byly v maximální možné míře pokryty jak procesní, tak technické znalosti prostředí.

Rozsah

Rozsah jednoho Školení bude 2 na sebe navazující dny. Doporučený počet osob na jedno Školení je 8 - 12.

Lokalita

Školení bude probíhat v Praze ve Školicích prostorách Dodavatele, které budou upřesněny vždy nejméně 14 dní před termínem Školení.

Počet školených osob

Celkový počet vyškolených osob ze strany Zadavatele bude maximálně 20.

Termíny Školení

$T_3 - T_3+8$

Předpokládané termíny jednotlivých běhů Školení jsou následující:

- 1. běh – T_3 až $T_3 + 1$
- 2. běh – $T_3 + 7$ až $T_3 + 8$

Zadavatel se může s Dodavatelem domluvit na úpravě termínů Školení v závislosti na aktuální situaci.

Cíle Školení

Cílem Školení je doplnit Školení supervizorů o specifické činnosti související se správou dat a řešením chybových stavů. Administrátor by rovněž měl mít znalosti v oblasti instalace a konfigurace pracoviště a správy uživatelských účtů. V případě řešení problémů a požadavků přesahujících kompetence a znalosti administrátora zajišťuje řešení ve spolupráci se Servis deskem Dodavatele.

Obsah Školení

- Importy dat
- Tvorba nových reportů
- Správa geografické DB
- Správa uživatelských účtů
- Kartodiagramy
- Řešení chybových stavů
- Instalace a konfigurace pracoviště
- Správa rajonizačních tabulek
- Správa číselníků
- Fungování a komunikace se Servis deskem

V rámci Školení administrátorů budou účastníci vzděláni ve všech oblastech administrativy systému a zejména oblast GIS. Jedná se především o správu uživatelských rolí, geografické DB a rajonizačních tabulek, zejména v oblasti konfigurace služeb a úprav drobných chyb. Řešení chybových stavů všech komponent týkajících se GIS od DB až po koncová zařízení je pak druhým velkým blokem Školení v rámci úrovně S3. Konkrétně tedy budou v rámci Školení GIS Školeny následující oblasti:

- Základy práce se systémem GIS serveru
- Publikace mapových služeb
- Aktualizace geodatabáze, koncepce a obsluha potřebných nástrojů
- Obsah geodatabáze
- Aktualizace mapových dlaždic
- Zabezpečení služeb
- Nastavení služby místopisného helperu
- Správa rajonizace

Vzhledem ke koncovým pracovištím bude tedy Školena i instalace a konfigurace. Kromě těchto technických dovedností budou vyučovány oblasti ryze administrativní - importy dat z předem definovaných zdrojů, tvorby šablon nových reportů a mimo jiné i kartodiagramů.
Nakonec bude Školena interakce se Servis deskem, především v oblasti rozšířených možností oproti nižším úrovním Školení.

S4 školení vedoucích složek

Školitelé

Školitelé pro jednotlivé běhy školení budou nominováni z řad pracovníků Dodavatele. Pro každý běh budou k dispozici dva školitelé současně, kteří budou zvoleni tak, aby byly v maximální možné míře pokryty jak procesní, tak technické znalosti prostředí.

Rozsah

Doporučený rozsah jednoho školení je 2x jeden den, přičemž nemusí jít o dva na sebe navazující dny. Doporučený počet osob na jedno školení je 8 - 12.

Lokalita

Školení bude probíhat v prostorách Zadavatele v lokalitách dle jeho uvážení a kapacit. V těchto prostorách je nutno mít k dispozici, nebo ve spolupráci s Dodavatelem zajistit vzorové pracoviště NSPTV s konektivitou na testovací systémy Dodavatele.

Počet školených osob

Předpokládaný počet školených osob ze strany Zadavatele je maximálně 50 (samostatně jednotlivé kraje 225).

Termíny školení

$T_1 - T_1 + 21$

Termíny školení bude určovat Zadavatel v závislosti na potřebách a aktuální situaci v dané lokalitě. Školení uživatelů budou probíhat postupně v jednotlivých krajích a složkách podle postupného oživování systému NIS.

Cíle školení

Cílem školení je doplnění základních znalostí obsluhy aplikace o správu uživatelských účtů a znalostní báze operátorů a obsluhu lokálního reportingu.

Obsah školení

- Správa uživatelských účtů
- Správa znalostí operátorů
- Lokální reporting
- Exporty dat včetně záznamů hovorů
- Práce se Servis deskem

Na této úrovni školení budou školeni vedoucích krajských složek, kteří budou školeni především z pokročilých administrátorských funkcí a správy znalostí operátorů.
V rámci správy znalostí operátorů bude představena metodika pro komplexní zajištění proškolenosti operátorů a celkové úrovně školení 51-53. Tato metodika bude klíčová pro udržování dlouhodobé vzdělanosti uživatelů. Vedle toho budou školeny pokročilé administrativní funkce, zejména správa uživatelských účtů, import a export dat z definovaných zdrojů, dostupné pokročilé funkce pro práci se Servis deskem a práce s lokálními reporty, přičemž bude školeno jak jejich vytváření, tak jejich interpretace a tedy přijímání.

S5 školení vedoucí pracovníky centrálních orgánů IZS

Školitelé

Školitelé pro jednotlivé běhy školení budou nominováni z řad pracovníků Dodavatele. Pro každý běh budou k dispozici dva školitelé současně, kteří budou zvoleni tak, aby byly v maximální možné míře pokryty jak procesní, tak technické znalosti prostředí.

Rozsah

Doporučený rozsah jednoho školení je 2x jeden den, přičemž nemusí jít o dva na sebe navazující dny.

Lokalita

Školení bude probíhat v Praze ve školicích prostorách Dodavatele, které budou upřesněny vždy nejméně 14 dní před termínem školení.

Počet školených osob

Předpokládaný počet školených osob ze strany Zadavatele je 5.

Termíny školení

$T_1 - T_1 + 21$

Termíny školení bude určovat Zadavatel v závislosti na potřebách a aktuální situaci v dané lokalitě. Školení uživatelů budou probíhat postupně v jednotlivých krajích a složkách podle postupného oživování systému NIS.

Cíle školení

Cílem školení je doplnění znalostí obsluhy aplikace zejména o znalosti související s konfigurací pravidel procesního serveru a reportingu.

Obsah školení

- Celonárodní reporting
- Nastavení pravidel
- Nastavení reportingu
- Práce se Servis deskem

Toto školení bude poskytnuto určeným osobám vedení složek na celostátní úrovni. V rámci této úrovně budou školeny především reportingové funkce a pokročilá komplexní nastavení. Z hlediska reportingu se jedná především o možnosti celostátního reportingu a průvod rozsahem služeb poskytovaných v kontextu nastavení reportingu jako takového.
Dále bude školeno nastavování business pravidel v systému a práce se Servis deskem, která bude z této pozice stanovena eskalačními procedurami.

PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)

projektu
Národní informační systém integrovaného záchranného systému (NIS IZS)

část

J. Telefonie a nahrávání

Dokument obsahuje:	Popis subsystému, který bude zajišťovat služby spojené s příjmem hlasových hovorů, jejich směrováním a nahráváním.
Verze:	5.1b
Schválil za Dodavatele:	RNDr. Vladimír Příbramský
Datum aktualizace:	17/4/2014

1. Obsah

1. Obsah ... 2
2. Definice subsystému ... 3
3. Využití subsystému v projektu NIS IZS ... 5
3.1 Užití „White listu" ... 5
3.2 Užití „Black listu" ... 6
3.3 Způsob směrování hovorů v rámci složek IZS ... 6
4. Technická specifikace řešení ... 8
4.1 IP telefonie ... 8
4.1.1 Systém IPT musí podporovat následující: ... 10
4.2 Napojení k veřejné telefonní síti ... 11
4.2.1 Požadavky na SIP řešení ... 12
4.2.2 Požadavky na ISDN řešení ... 12
4.2.3 Požadavky na koncová zařízení pro napojení operátorů ... 13
4.3 Koncová zařízení ... 14
4.3.1 Požadavky na IP telefon ... 15
4.4 Požadavky na agenty a zpracování hovorů ... 15
4.4.1 Požadavky na agentské funkce ... 16
4.4.2 Požadavky zpracování hovoru ... 17
4.5 Nahrávání hovorů ... 18
4.5.1 Požadavky na nahrávání hovorů ... 19
4.6 Analytické nástroje ... 20
4.6.1 Požadavky na analytické nástroje ... 20
4.7 Implementace ... 21
4.7.1 Proces implementace subsystému ... 21

Podpis/signature:.....

2. Definice subsystému

Subsystém pro telefonii zahrnuje vytvoření, dodávku a následnou technickou podporu technologií IP telefonie, funkcí směrování hovorů v rámci systémů Národního informačního systému integrovaného záchranného systému (NIS IZS) a jejich nahrávání. Na uvedený subsystém následně navazují hlasové systémy jednotlivých složek (HZS, PČR a ZZS).

Součástí subsystému je dodávka 309 operátorských licencí pro operátory rozmístěné ve 14 krajích České republiky – 104 pro HZS, 80 pro PČR a 125 pro ZZS. Agentská aplikace bude spolupracovat s lokálně umístěným telefonním přístrojem agenta a s dalšími částmi softwarového vybavení, které agent dle zadávací dokumentace projektu potřebuje k výkonu své práce.

Subsystém zahrnující bloky pro IP telefonii (dále jen „IPT"), směrování hovorů (dále jen „CC") a jejich nahrávání (dále jen „RBC") bude dodán jako dvou dvouvrstvá architektura. První úroveň bude zahrnovat decentralizované součásti systému umístěné v jednotlivých krajských datových centrech (dále „KDC"), případně sídlech operačních řízení jednotlivých složek IZS (dále jen „OŘ"). Druhá úroveň systému bude poskytovat funkci replikace a archivace nahrávek.

V rámci standardního funkčního stavu stejně jako v případě krizových scénářů, kdy dojde k rozpadu napojení systémů v KDC vůči centrálním komponentám umístěným v CDC jsou decentralizované systémy telefonie schopny plnohodnotně autonomního fungování v rámci daného kraje, včetně zajištění přelivů hovorů mezi kraji.

Konektivita na TELCO operátora bude zajištěna napojením hlasových bran umístěných v jednotlivých KDC na nejbližší připojný bod sítě zvoleného TELCO operátora. Tento operátor zajistí koncentraci příchozích hovorů pro jednotlivé pilotní čísla IZS (112, 150, 155, 158) od všech ostatních telekomunikačních operátorů, přes které mohou být volání v rámci České republiky směrována. V rámci jednání s daným TELCO operátorem budou dohodnuta pravidla pro směrování příchozích hovorů na základě geografické příslušnosti volajícího tak, jak byly zjištěny v rámci signalizace daného hovoru.

Připojná konektivita jednotlivých KDC bude zajištěna prostřednictvím SIP trunku a/nebo euroISDN 30 linek v závislosti na dostupnosti daných technologií v jednotlivých krajích a garantované dostupnosti konkrétního typu připojení v síti zvoleného TELCO operátora.

Systém musí být dodán v zapojení, umožňujícím 200% zajištění poskytované služby. Daného zajištění bude dosaženo zdvojením primárních částí jednotlivých komponent systému a způsobem přepadu hovorů mezi jednotlivými lokalitami.

Další nedílnou součástí je dodávka systému nahrávání hovorů v režimu „total recording" a poskytování těchto nahrávek ostatním složkám IZS dle dopředu sjednaných podmínek a pravidel.

Součástí směrování hovoru je kontrola volajícího v rámci tzv.: „Black listů" a „White listů" související s eliminací, nebo naopak preferováním volajícího v rámci NIS IZS.

Dále zadání bude systém poskytovat programová rozhraní (dále jen „API") a další funkcionalitu vyžadované pro napojení dalších součástí systému NIS IZS.

Součástí dodávky bude i řešení pro laboratorní ověřování změnových požadavků a implementaci nových verzí systémů před jejich samotným nasazením do produkčního prostředí. Dané laboratorní prostředí bude odpovídat produkčnímu prostředí z pohledu typu použitých komponent i jejich zapojení. Od produkčního prostředí bude nicméně striktně oddělena, aby změny prováděné na tomto systému nemohly ovlivnit systém produkční. Fyzické umístění daného vybavení bude dále diskutováno se zadavatelem.

3. Využití subsystému v projektu NIS IZS

Dodávaný systém je určen pro příjem všech tísňových linek integrovaného záchranného systému (112, 150, 155 a 158). Systém bude postaven jako dvouúrovňová infrastruktura se 14 samostatnými celky, implementovanými ve 14 KDC a dále pak komponentami umístěnými v CDC, poskytující jednotlivým krajským systémům pouze dodatečné informace při mezikrajských přelivech hovorů.

Telefonní operátor bude předávat hovory dle sjednaných směrovacích pravidel na vstupní linky jednotlivých krajských systémů. Primárním kritériem pro předání hovoru konkrétnímu KDC je informace identifikující lokalitu volajícího (kraj), tak jak byla zjištěna prostředky sítě samotného TELCO operátora. Identifikace původu volání bude předána operátorem jako doplňující informace (NRN - definice viz **Číslovací plán síťových směrovacích čísel**) o příchozím hovoru v rámci jeho signalizace pro možnosti dalšího využití v rámci systémů NIS IZS. Implementovaný systém musí tuto informaci správně identifikovat a oddělit od původního čísla volajícího a tuto informaci použít pouze v rámci rozhodovacích kroků v rámci směrování hovorů. Následným krokem je kontrola „Black listů" a „White listů". V případě, že číslo volajícího není zahrnuto ani v jednom ze zmiňovaných seznamů, je hovor směrován dále přímo na operátora pro jeho další odbavení.

Hovor je odbaven agentem, který jej řeší nebo dále s hovorem operuje tak aby došlo k řešení celé požadavku. Řešením může být převzetí požadavku a ukončení hovoru, konferování hovoru s jinou složkou IZS, přesměrování hovoru na jinou složku IZS, konference s interním účastníkem/účastníky, případně externím účastníkem/účastníky, příposlech. Po celou dobu, kdy je hovoru účasten kdokoliv z interních uživatelů NSPTV, bude hovor nahráván.

3.1 Užití „White listu"

Pokud bude hovor vyhodnocen jako záznam ve „White listu", je nutné, aby systém byl schopen směrovat tento hovor dle požadavku tohoto listu, tj. například směroval takovýto hovor na specifického agenta, specifické číslo, případně hovor preferoval před ostatními volajícími.

„White Listy" jsou spravovány samostatně každou složkou IZS a pro systém příjmu tísňových hovorů bude číslo volajícího v rámci daného listu ověřeno, s uvedením důvodu vložení, útvar, další postup, datum od kdy do kdy (den – den), poskytnutím důvod, proč je dané číslo v daném seznamu zahrnuto, či informace o osobě spojené s daným číslem volajícího. Pokud v rámci směrování hovoru dojde k identifikaci volajícího jako osoby zahrnuté ve White listu, lze konfiguračně nastavit, aby jeho číslo v rámci aplikace operátora zpracovávajícího daný hovor bylo maskováno nebo zcela skryto. Stejně tak bude číslo volajícího skryto nebo maskováno v rámci nahrávek systému pro záznam hovorů.

3.2 Užití „Black listu"

Pokud je číslo volajícího nalezeno na „Black listu" je s hovorem nakládáno dle dohodnutého scénáře, tedy:

1. Úroveň – varování (číslo v aplikaci NSPTV červenou barvou), ale hovor bude spojen

2. Úroveň – hovor ukončen, příp. ukončen s hláškou.

Blacklist funguje pro každou složku zvlášť. Blacklist je celostátní pouze u HZS, ostatní používají pouze na krajské úrovni. Operátoři PČR budou upozorněni, že číslo je uloženo na blacklistu jiné složky. Veřejné telefonní automaty se do blacklistu nezařazují. Zařazování do blacklistu musí mít kontrolu na veřejné automaty.

3.3 Způsob směrování hovorů v rámci složek IZS

Z pohledu příjmu tísňových volání je veškerý provoz na všechna 4 tísňová čísla základních složek IZS směrován jednotně na vstupní linky jednotlivých KDC.

V případě standardního chování systému je hovor odbaven vždy agentem NSPTV, příslušným danému tísňovému číslu a původu volání (kraj). U příchozího hovoru je na základě obdržené informace od volajícího založena v aplikačním rozhraní agenta nová událost. Ze strany NSPTV agenta je s takto odbavovaným hovorem dále nakládáno způsobem, definovaným složkou IZS, pro kterou je daný hovor určen (předání hovoru na OŘ dané složky, ukončení hovoru po aplikačním založení události….).

V případě nově příchozího hovoru do konkrétního KDC a nedostupnosti volného NSPTV agenta registrovaného v dané lokalitě je ze strany systému umístěného v daném KDC kontaktován nadřízený systém umístěný v CDC lokalitě s dotazem na způsob distribuce. Systém bude umožňovat v souladu s požadavkem AI_NSPTV verze 7 následující možnosti (nastavitelné dle dohodnutých pravidel):

- přeliv hovoru na jiné pracoviště/operátora NSPTV v daném kraji (jiná role než odpovídá přijímanému číslu),
- přeliv hovoru na jiného operátora v příslušné roli v ostatních krajských pracovištích NSPTV (v případě PČR a ZZS vždy přeliv v rámci složky)
- přesměrování hovoru do operačního řízení příslušné složky (případ tzv. ostrovního provozu v rámci kraje)

V rámci aktualizace prováděcího konceptu před spuštěním pilotního provozu NSPTV bude se všemi složkami detailně specifikováno iniciační nastavení pravidel přelivů tísňových volání. Jednotlivá pravidla budou administrátorsky měnitelná a kombinovatelná, takže v průběhu provozu NSPTV bude možno toto iniciační nastavení pružně měnit dle požadavků složek IZS.

V případě, že v celém NIS IZS systému není volný ani jeden NSPTV agent, dojde k zařazení daného hovoru v rámci frontovacího mechanismu (dále jen „Queuing") daného KDC, do kterého byl hovor TELCO operátorem směrován.

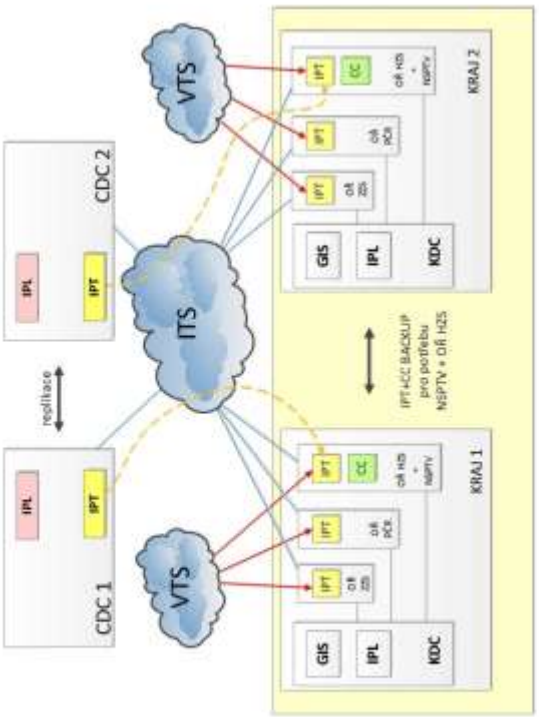
Podpis/signature:……

4. Technická specifikace řešení

S ohledem na požadované snížení náročnosti na umístění všech částí IPT je nutné, aby všechny SW komponenty dodávaného řešení podporovaly virtualizaci a to minimálně v podobě nejpoužívanějších platforem jako VMware, Citrix, nebo Hyper-V.

4.1 IP telefonie

Řešení IPT bude postaveno jako jednovrstvá architektura, kde komplexní příjem včetně požadovaných předností při nedostupnosti tísňových volání bude zajištěn 14 samostatnými systémy, umístěnými v jednotlivých KDC, navzájem signalizačně propojenými.



Model 1: Schéma rozdělení komponent mezi jednotlivé dotčené systémy

Prvky umístěné v jednotlivých KDC budou pro zajištění požadované míry spolehlivosti vždy zdvojené (Call Control Primary – Back Up). Pro zajištění další míry zabezpečení je hovor určený pro zpracování v rámci určitého kraje signalizován operátorem v případě nedostupnosti

V případě rozpadu konektivity mezi KDC a CDC dochází ke ztrátě části programové funkčnosti systému pro dané KDC. V daném stavu nejsou agenti NSPTV schopni zakládat nové události do systému a v takovém případě je nutné automatizovaným způsobem ukončit provoz daného KDC z pohledu příjmu nové příchozích hovorů tísňového volání. Daného chování je docíleno terminováním konektivity na hlasových branách, kterou dané KDC používá k příjmu tísňových volání. Aplikační vrstva agentského systému zajistí přepojení daného agenta na funkční systém v párovém kraji, pokud je vnitřní konektivita mezi danými kraji stále funkční. Tímto krokem zajistí systém dostupnost maximálního možného množství agentů pro nabír nové příchozích tísňových volání.

V případě, že je do sítě TELCO operátora signalizován nový hovor s geografickou příslušností určitého kraje a TELCO operátor není schopen daný hovor do KDC v dané oblasti doručit z důvodu nedostupnosti funkční konektivity do KDC, případně z důvodu zaplnění všech dostupných příchozích kanálů daného KDC, zajistí směrování hovorů vlastní sítí na další KDC s dostupným vstupním kanálem.

V případě, že síť TELCO operátora není schopna doručit tísňová volání do žádného z KDC systémů, dojde ke směrování daných hovorů na vstupní linky telefonních systémů jednotlivých OŘ, které zajistí jejich zpracování. Jako primární, bude brán systém OŘ s geografickou příslušností, odpovídající lokalitě volajícího zjištěné v rámci signalizace.

komunikačních sítí) do síťové signalizace a v souladu s tímto předpisem ji vyhodnotí. Systém musí umožňovat zpracování všech typů lokalizační informace dle platných právních předpisů.

Pozn.: Přístup k tísňovým voláním je podle zákona povinen zajistit poskytovatel veřejně dostupné telefonní služby, tzn., že tato povinnost se vztahuje i na poskytovatele hlasové služby VoIP, kteří službu poskytují v kategorii veřejně dostupné telefonní služby, tj. na ty, kteří využívají pro poskytování služby geografická telefonní čísla. Všechno případech se lokalizace VoIP účastníků PSTN platnou legislativou, tedy Vyhláškou o lokalizaci a identifikaci volajícího při volání na čísla tísňových volání. V případě nemobilního přístupu (v ČR je pro hlasové služby poskytované na nemobilním základě vyčleněno zvláštní rozsah čísel s přístupovým kódem 910 pro veřejné komunikační sítě určené pro přenos hlasu prostřednictvím internetového protokolu) však nemohou být z technického hlediska splněny některé požadavky kladené na veřejně dostupnou telefonní službu, např. zajištění lokalizace volajícího pro tísňová volání.

Dále uvedená tabulka obsahuje očekávaný počet E1 interface pro napojení jednotlivých KDC na síť TELCO operátora. Kapacitní výpočet vychází z původního požadavku, předpokládající 820 vstupních a 300 výstupních hlasových kanálů na celý systém.

Kraj	E1 interface - Primary		E1 interface - Backup		Celkem
	TV	OŘ	TV	OŘ	
Hlavní město Praha	5	1	5	1	12
Jihočeský	3	2	3	2	10
Jihomoravský	4	2	4	2	12
Karlovarský	3	1	3	1	8
Královéhradecký	2	1	2	1	6
Liberecký	3	1	3	1	8
Moravskoslezský	4	0	4	0	8
Olomoucký	3	2	3	2	10
Pardubický	3	1	3	1	8
Plzeňský	3	2	3	2	10
Středočeský	4	2	4	2	12
Ústecký	3	2	3	2	10
Vysočina	3	1	3	1	8
Zlínský	2	1	2	1	6
Celkem	**45**	**19**	**45**	**19**	**128**

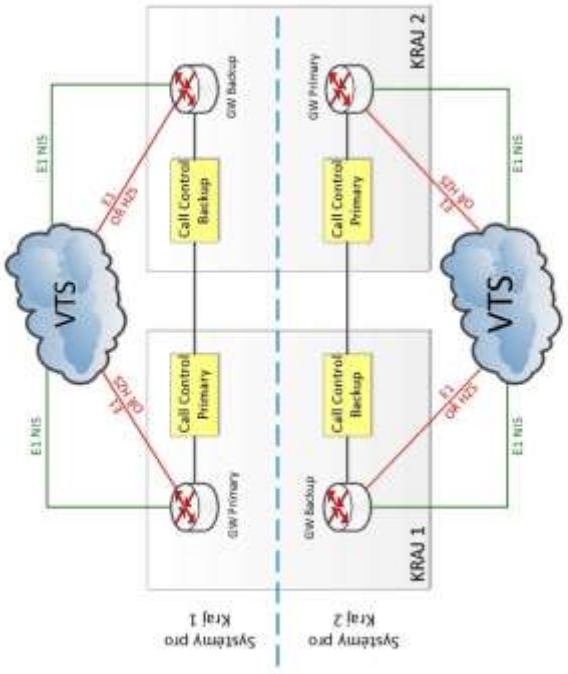
Výpočet kapacit navrhovaný pro jednotlivá KDC bude v rámci předimplementační fáze dodávky finálně diskutován se zadavatelem. Dané počty uvádíme pro možnost předběžného zkoumání možností TELCO operátora v jednotlivých lokalitách.

4.1.1 Systém IPT musí podporovat následující:

- Současnou signalizaci hovorů do více než jednoho KDC
- Softwarové části systému musí být schopny provozu ve virtuálním prostředí.

konektivity do hlasových bran v primární lokalitě na vstupní linky kraje, který bude v rámci organizace NIS IZS systému zvolen jako „nárazový kraj". V případě výpadku hlasové technologie umístěné v rámci jednoho kraje bude v rámci konfigurace systémů umístěných v pro něj definovaném párovém kraji zajištěna možnost přeregistrace telefonních přístrojů z takto postiženého kraje. Daného fungování bude využito v případě zachování vnitřní konektivity takto virtuálně propojených krajských systémů. Zdvojení prvků + přeregistrace tak zajišťuje požadovanou 200% záložní službu. V případě, že dojde spolu s výpadkem technologie na daném kraji i k rozpadu vnitřní konektivity s párovým krajem, bude takto duálně směrovaný hovor odbaven přímo agenty párového kraje. V případě výpadku obou krajských systémů bude hovor směrován operátorem dle dalších nastavených kriterií (např. do telefonie OŘ).

Dané řešení je návrh ze strany dodavatele zvyšující celkovou odolnost systému. Nic nepochopitelně nebrání tomu, umístit záložovaný pár vždy v jedné lokalitě, pokud by navrhované řešení odporovalo požadavkům zadavatele.



Model 2: Schéma redundantního zapojení TELCO komponent v párových krajích

Technologie IPT musí být schopna přijmout informaci o poloze volajícího vloženou způsobem stanoveným platnými technickými předpisy (**síťový plán signalizace veřejných**

- Systém musí umožnit programové řízení vstupních kanálů hlasové brány (online/offline) pro možnost aktivace záložního směrování na straně TELCO operátora
- Systém musí podporovat automatickou přeregistraci zařízení v případě výpadku jeho části
- Systém musí být odolný proti výpadku jednoho uzlu či více uzlů zároveň
- Systém musí poskytovat informace o hovorech, které byly tímto systémem realizovány a na základě nich umožnit tarifikaci hovorů, včetně jejich rozúčtování na jednotlivé lokality, nebo složky IZS.
- Podpora SMNP – aktivní monitoring systému
- Autorizace konfigurace koncového zařízení
- Podpora Java Telephony API (JTAPI) verze minimálně 1.2
- Podpora CSTA Phase 3 (ECMA-323)
- Systém musí mít management nástroj pro nastavení systému jako celku i pro nastavení detailních hodnot jednotlivých jeho částí
- Chování všech softwarových komponent jako clusteru – tj. konfigurují se pouze v jednom místě a pouze jednou, pro všechny uzly daného clusteru. Systém musí zajistit případnou automatickou distribuci konfigurace z primárně konfigurovaného uzlu systému.
- Systém musí umožnit konferenční hovory v jakékoli kombinaci externích a interních účastníků, v počtu odpovídající maximálnímu počtu agentů, jejichž telefonní přístroje budu k danému systému registrovány. Pro každou takto ustavenou konferenci jsou počítání 3 účastníci. Systém musí při požadavku operátora zajistit konferenci až stran, v jakékoliv kombinaci externích a interních účastníků.
- Synchronizace uživatelské databáze z externího systému (např. LDAP)
- Autentizace uživatelů variantně lokální, nebo proti externímu autentizačnímu serveru
- Umožnit napojení na jednotlivé systémy složek IZS pomocí IP trunk napojení s protokolem SIP nebo H.323, nebo pomocí ISDN PRI/BRI přípojky. Typ připojení je závislý na množinách ústředny OŘ dané složky. V případě IP trunk bude pro bezpečné oddělení jednotlivých částí sítě použit odpovídající bezpečnostní prvek (SBC s implementací Back-to-Back agent) nebo router H.323 na H.323 či kombinace SIP to H.323. Přístupná forma propojení musí být dána jako požadavek na součinnost dodavatele jednotlivých IPT (projektů KSP) systémů v ostatních složkách IZS, s tím že je požadovaná součinnost projektů KSP v zajištění rozhraní SIP trunku.
- Umožnit příjem modemového spojení pro budoucí potřebu e-call systémů
- Všechna zařízení zapojená v předávání hovorů a signalizace musejí podporovat označování dat pomocí QoS. Požadovány jsou následující úrovně:
  - Expedited Forwarding (EF), tj. prioritní fronta, pro přenos hlasu, v kodeku G.711, hlasový provoz bude označen DSCP 46 (EF)
  - Assured Forwarding (AF) pro hlasovou signalizaci a konfiguraci telefonů, hlasová signalizace bude označena DSCP 24 (CS3)

4.2 Napojení k veřejné telefonní síti

Napojení na veřejnou telefonní síť bude realizováno skrze síť zvoleného TELCO operátora. Tento zajistí koncentraci volání od všech ostatních TELCO operátorů.

Napojení telefonních operátorů bude realizováno pomocí ISDN PRI nebo SIP, dle dostupnosti dané konektivity v jednotlivých vstupních místech systému IZS a míře spolehlivosti dané technologie v rámci sítě zvoleného TELCO operátora.

V každé lokalitě musí být systém schopen přijmout a zpracovat hovory v počtu, odpovídajícím součtu všech vstupních kanálů u linek, kterými je daný kraj připojen do TELCO sítě, viz předchozí tabulka. Hovory, které nebude možné zpracovat agenty dané lokality z důvodu jejich plného vytížení, budou směrovány na jinou lokalitu, nebo umístěny do vstupní fronty – bude konfigurovatelné dle požadavku jednotlivých složek IZS.

Množství vstupních linek KDC musí umožnit práci všech agentů NSPTV, kteří mohou být k systému daného KDC připojeni. V rámci kapacity přípojných linek bude systém koncipován tak, aby umožnil pro každý příchozí hovor, připojit minimálně jednoho externího účastníka do konference spolu s volajícím a operátorem, zpracovávajícím příslušný hovor.

Každé KDC bude dále vybaveno mechanismem pro frontování hovorů, které není možné obsloužit k němu registrovaným NSPTV agentem, ani přepojit vnitřní sítí na jiné KDC z důvodu nedostupnosti volného agenta v ostatních lokalitách. Počet portů pro frontování hovorů, u kterých není možné zajistit okamžité směrování na agenta musí pro každé KDC odpovídat počtu vstupních kanálů linek, kterými mohou být do daného KDC směrovány příchozí hovory tísňového volání.

4.2.1 Požadavky na SIP řešení

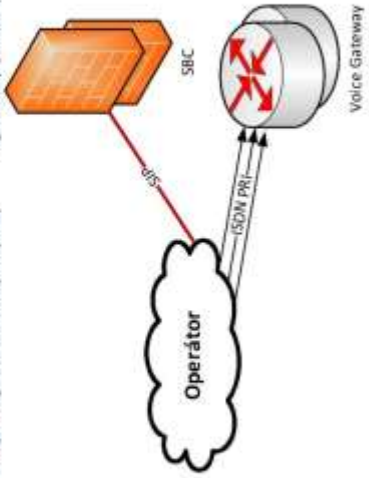
- Podpora SIP podle RFC3261 a navazujících. Transport přes UDP i TCP.
- Odezva na sledování dostupnosti pomocí SIP Options Ping
- Generování SIP Options Ping proti vzdálené straně, odpovídající reakce na zjištěný stav - např. směrování hovorů jinou cestou.
- SIP signalizace i RTP přenos telefonie bude možné ukrýt za jednu nebo více IP adres. Tato adresa/adresy budou z pohledu externího subjektu jediné uzly IP komunikace, se kterými bude hovor sestaven. Signalizace ani RTP nebude procházet přímo mezi IP telefonem NIS- IZS operátora a externím subjektem.
- Kódování hlasu v kodek G.711 A-law s vypnutí detekcí ticha (VAD)
- Tónová volba in-band podle RFC 2833, nebo out-of-band pomocí SIP NOTIFY
- Všechna zařízení zapojená v předávání hovorů a signalizace musejí podporovat označování dat pomocí QoS. Požadovány jsou následující úrovně:
  - Expedited Forwarding (EF), tj. prioritní fronta, pro přenos hlasu, v kodeku G.711, hlasový provoz bude označen DSCP 46 (EF)
  - Assured Forwarding (AF) pro hlasovou signalizaci a konfiguraci telefonů, hlasová signalizace bude označena DSCP 24 (CS3)

4.2.2 Požadavky na ISDN řešení

- Rozhraní ISDN E1 PRI se signalizací Q.931, EuroISDN.
- Rozhraní E1 se signalizací Q.SIG, formát ISO

4.2.3 Požadavky na koncová zařízení pro napojení operátorů

- V případě technologické realizovatelnosti daného požadavku musí telefonní operátor své přípojky přivést na vstupní místa NIS IZS zdvojeně z jiné ústředny a jinou trasou.
- Přípojka pro SIP musí splňovat:
  - Fyzické rozhraní: 100/1000 Ethernet v režimu full duplex se zapnutou automatickou detekcí duplexu a rychlostí.
  - Po celé trase mezi NIS IZS a volajícím musí operátor zajistit odpovídající kvalitu služby pro hovor v kodeku G.711 A-law, tj. v obou směrech prioritní obsluhu pro pásmo 80 kb/s na hovor
  - Operátor zodpovídá za omezení maximálního počtu současných hovorů na lince tak, aby nebyl překročen limit nastavené kvality služby (jedná se o SIP trunk, u kterého je možné administrativně definovat množství současných hlasových kanálů, které jsou operátorem do daného trunku směrovány. Bez dané konfigurační možnosti není možné na SIP trunku zaručit kvalitu hovoru, neboť pro jednotlivé hovory není vybrazen samostatný kanál jako je tomu například u ISDN technologie)
- Přípojka pro ISDN PRI musí splňovat:
  - Fyzické rozhraní: ITU-T G.703, symmetric 120 ohm, framing a CRC v nastavení pro ISDN
- V případě SIP přípojky musí TELCO operátor musí zajistit signalizaci příchozího hovoru na dvě zvolená datová centra zároveň (funkce paralel ringing - souvisí s navrhovaným záložovaným řešením vstupních linek)
- V případě nedostupnosti daného datového centra, či pro případ zahlcení všech vstupních kanálů jednoho datového centra zajistí operátor automatický přepad nové signalizovaných hovorů na další datová centra, dle předem definovaných pravidel směrování.
- Jestliže se hovor nepodaří spojit ani do jednoho KDC, hovor musí být TELCO operátorem směrován do systému telefonie OŘ
- NIS-IZS přebírá hovor okamžikem signalizace jeho spojení (SIP "200 OK" resp. ISDN "CONNECT"). Po spojení hovoru do NIS IZS nebude operátorovi signalizován žádný požadavek na převzetí hovoru do jiné lokality.
- Jestliže je celá trasa hovoru vedena protokolem IP a je pod kontrolou operátora, tj. volající používá IP telefon registrovaný k SIP službě operátora a operátor ho dále směruje po IP do NIS-IZS, musí být SIP signalizace doplněna o lokalizační informace volajícího podle specifikace RFC6442 a RFC6443
- Operátor je povinen ignorovat požadavek ze strany volajícího na potlačení identifikace volajícího, tak aby byl schopen signalizovat hovor do NIS-IZS s plnou identifikací volajícího



Model 3: Napojení operátora v jednom DC

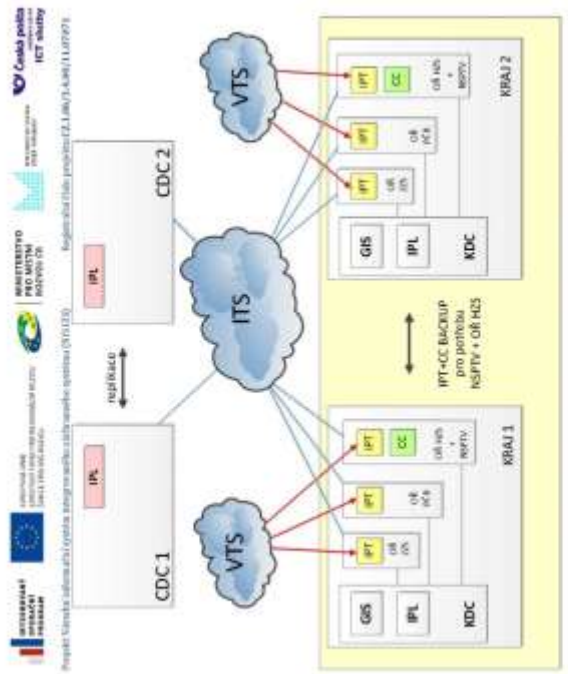
4.3 Koncová zařízení

Spolu s IPT bude dodáno také 309 ks telefonních aparátů pro agentská pracoviště NSPTV (104 pro HZS, 80 pro PČR a 125 pro ZZS) a náhlavní soupravy v počtu 309 základen a 1236 sluchátek v provedení (viz výsledek jednání o náhlavních soupravách). Každý aparát musí splňovat dále popsané podmínky a být schopen bez nutnosti manuální rekonfigurace pracovat ve spojení s kterýmkoliv telefonním systémem zapojeným do virtuálního páru (cluster). V rámci napojení telefonního přístroje na systém řízení hovoru (dále jen „Call control") v rámci daného KDC musí být telefonní přístroj schopen přeregistrace mezi jeho jednotlivými uzly bez nutnosti jeho restartu.

Nastavení systému DHCP, DNS pro automatickou konfiguraci telefonních přístrojů bude upřesněno v rámci aktualizace prováděcího konceptu před zahájením pilotního provozu NSPTV.

V rámci dodávky bude část dodávaných operátorských pracovišť schopná práce v tzv. „Hybridním režimu", kdy stejnému operátorovi bude umožněno pracovat jak v režimu Příjem tísňových volání, tak v režimu Operačního řízení. I přes práci stejného ajenta v těchto dvou režimech bude každý takový agent vybaven dvěma zcela nezávislými telefonními přístroji, z nichž každý bude napojen na vlastní telefonní (call control) systém. S ohledem na absenci jednotné logiky řízení daných telefonních systémů je v tomto případě plně v odpovědnosti zadavatele, aby na úrovni organizace práce daných agentů zajistil, že daný agent nebude v jeden okamžik současně aktivní v obou telefonních (call control) systémech. V krajním případě by totiž mohla nastat situace, kdy na daného agenta bude směrován hovor jak ze systému telefonie NSPTV, tak z telefonie OŘ.

Výjimku z předchozího popisu tvoří pouze hybridní operátoři OŘ HZS, kteří budou vybaveni pouze jedním telefonním přístrojem, sloužícím funkce pro zpracování tísňových hovorů a



Model 4: Schéma logiky pro směrování hovorů na jednotlivé agenty NSPTV

4.4.1 Požadavky na agentské funkce

- Přihlášení / odhlášení agenta z/do systému
- Změny stavů agenta. Minimálně možnost přepínáním stavů mezi Aktivní, Zaneprázdněn, Pauza (případně odpovídající stavy cílově zvolené technologie pro řízení agentů NSPTV)
- Možnost klasifikovat důvody NOT-READY
- Možnost klasifikovat hovor
- Agent nemá pevně přidělené číslo konkrétního telefonního přístroje tzv. Free seating
- Plné ovládání přiřazeného telefonu z agentské aplikace v rozsahu minimálně:
  - Přijmutí hovoru
  - Vytvoření odchozího hovoru
  - Přidržení hovoru
  - Předání hovoru
  - Vytvoření konference
  - Připojech
  - Ukončení hovoru
- Automatické převedení agenta na jiný řídící server v případě výpadku serveru, na který byl agent do daného okamžiku registrován a to bez ztráty aktuálního stavu agenta.
- Vytočení telefonního čísla z agentské aplikace pro agentem registrovaný telefon

telefonních funkcí operátora OŘ HZS. S ohledem na to, že k funkcím stejného telefonního přístroje agenta bude přes programové API telefonního systému přistupovat jak aplikační vybavení NSPTV systému, tak aplikační vybavení OŘ HZS, je odpovědností zadavatele, aby na úrovni organizace práce daných agentů zabránil ovládání daného telefonu oběma agentskými aplikačními platformami zároveň.

4.3.1 Požadavky na IP telefon

- Napájení telefonu ze sítě podle standardu 802.3af nebo 802.3at nebo přes externí zdroj.
- Podpora VLAN 802.1q možnost tagování rámců dle 802.1p
- Podpora audio kodeků G.711, G.729 a G.722
- Integrovaný min. 100 Mbps přepínač pro připojení operátorské stanice za telefon s podporou VLAN
- Autentizace telefonu do sítě protokolem 802.1x
- Proxy autentizace 802.1x pro počítač, který je připojen za telefonem
- Minimálně 2" displej telefonu
- Obousměrný hlasitý poslech
- Možnost ovládání hovoru jak prostřednictvím agentské aplikace, tak i ručně při zachování identického chování systému. Připojení náhlavní soupravy konektorem RJ-9 s dostatečným výkonem, aby nebyly nutné náhlavní soupravu vybavovat dodatečným zesilovačem
- Náhlavní souprava musí umožnit operátorovi příjem i zakončení hovoru, bez nutnosti provedení těchto funkcí prostřednictvím HW telefonu, či aplikace
- Uživatelské rozhraní v češtině
- V případě výpadku Call control systému schopnost telefonu dokončit aktuálně probíhající hovor, pokud je tento realizován mezi telefonním přístrojem agenta, umístěného ve stejné lokalitě, do které je směrován příchozí hovor z TELCO sítě.

4.4 Požadavky na agenty a zpracování hovorů

Součástí IPT subsystému je dodávka komponent sloužících pro směrování příchozích hovorů a řízení práce agentů, kteří tyto hovory zpracovávají. Systém by měl být plně integrovatelný s řešením IP telefonního systému a zároveň umožňovat poskytování informace o činnostech souvisejících se zpracováním příchozího hovoru dalším systémům prostřednictvím definovaných API.

Navržené řešení musí umožňovat modifikaci způsobu vyhodnocení lokalizačních údajů při změně principu určování polohy v mobilní komunikační síti (zejména v souvislosti se zvýšením přesnosti určování polohy při tísňovém volání).

U hovorů z pevné telefonní sítě získá aplikační logika směrování hovorů lokalizační a identifikační údaje z databáze vedené podle příslušného právního předpisu.

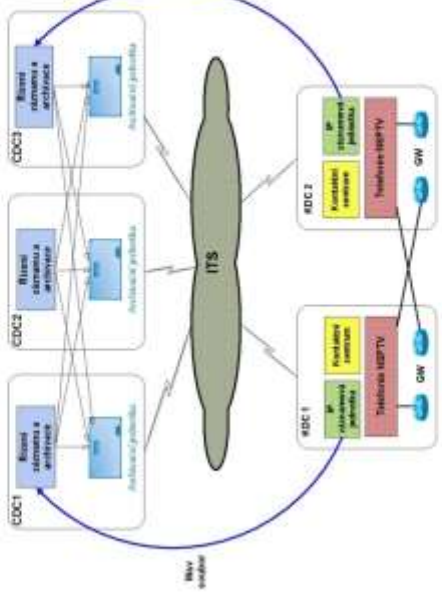
4.5 Nahrávání hovorů

Dodávaný systém musí zajistit nahrávání všech hovorů v režimu tak zvaného „Total recording". Řešení musí být zdvojené tak aby eliminovalo výpadek jednoho systému a zajistilo nahrání 100%. V případě nahrání konkrétního hovoru více samostatnými systémy musí systém umožnit cílové uložení a prezentaci nahrávek tak, aby jedna konkrétní nahrávka nebyla v systému prezentována dvakrát.

Řešení musí umožnit dostupnost aktivních nekomprimovaných nahrávek minimálně po dobu 3 měsíců a archivaci všech nahrávek v komprimovaném formátu minimálně po dobu 5 let. Pro přístup k archivovaným hovorům bude existovat aplikační podpora umožňující jejich vyhledání, přehrání a případný export.

Technické nároky (např. výpočetní výkon) na HW budou definovány ve fázi, kdy bude znám konkrétní produkt/řešení nahrávacího systému.

Předpokládaná architektura nahrávacího systému:



4.4.2 Požadavky zpracování hovoru

- Před zahájením směrování hovoru na konkrétního agenta aplikovat „Black Listy" a „White Listy". White listy i Black listy jsou uvažovány jako lokálně umístěné v NSPTV a spravovatelné ze strany jednotlivých složek IZS.
- V průběhu směrování umožnit k hovoru přidat další data z externích systémů a ta zobrazit v agentské aplikaci, případně přeslat v signalizaci CTI/TAPI
- Směrování hovoru na základě externích dat
- Upřednostnění hovoru ve frontě na základě informací z „White Listu", změnu priority hovoru v případě delší doby čekání atp.
- Pronta hovorů a automatické vybírání hovorů z fronty dle definovaných pravidel
- Funkce pro frontování hovorů, které není možné směrovat na agenta NSPTV v žádném KDC k jejich okamžitému odbavení. Kapacitně musí systém poskytnout možnost frontovat hovory v rozsahu všech vstupních kanálů ze sítě TELCO operátora
- Možnost řadit agenty do znalostních skupin a směrovat hovory dle znalostních skupin.
- Výběr odpovídajícího agenta metodou Longest Available Agent nebo jinou definovanou metodou, standardně používanou v systémech kontaktních center
- Systém řízení agentů musí poskytovat rozhraní pro napojení dalších subsystémů NIS IZS

Předpokládá se dvouúrovňová architektura řešení nahrávacího subsystému. IP záznamové jednotky budou umístěny v KDC a budou nahrávat veškerou komunikaci agentů NSPTV. Z důvodu redundance budou tyto nahrávací komponenty řešení zdvojeny. Vlastní nahrávání bude řešeno jako pasivní z důvodu požadované redundance záznamových jednotek. Interní hovory, resp. příslušný RTP stream musí vždy projít aktivním datovým prvkem v KDC. Okamžitě po skončení hovoru je nekomprimovaný záznam replikován do CDC do centrálního modulu Řízení záznamu a archivace. V rámci tohoto modulu předpokládáme i dodávku archivačního SW, který bude zajišťovat ukládání komprimovaných souborů na 3 archivační jednotky v centrálních datových centrech. Modul Řízení záznamu a archivace musí umožnit dostupnost nahrávek pro záznamové systémy OŘ složek IZS.

4.5.1 Požadavky na nahrávání hovorů

- Nahrání 100% hovorů
- Archivace hovorů v nekomprimované podobě po dobu 3 měsíců/ a následnou komprimaci do formátu MP3 a jejich uchování po dobu dalších 5 let
- Automatizovaný management nahrávek i k nim přináležících metadat (minimálně relokace z jednoho datového úložiště na druhé, mazání, archivace a znovuzpřístupnění archivovaných nahrávek)
- Redundance nahrávání v každém KDC s tím že každý jednotlivý nahrávací systém musí být schopen nahrát veškerý provoz směrovaný do nebo v rámci příslušného KDC, pokud je účastníkem daného hovoru, nebo konference agent NSPTV
- Nahrávání externího hovoru (např. mezi účastníkem z veřejné telefonní sítě a agentem NSPTV)
- Nahrávání interního hovoru (mezi dvěma telefonními přístroji uvnitř systému, je-li alespoň jeden z nich přiřazen operátorovi NSPTV)
- Nahrávání konference mezi volajícím, agentem NSPTV a libovolným dalším účastníkem (interním, nebo externím)
- Zajištění neměnnosti již provedené nahrávky
- Součástí záznamu hovoru jsou i základní identifikátory hovoru:
  - Volané číslo včetně geografické informace o místě vzniku hovoru
  - Volající číslo (s výjimkou maskovaných hovorů volajících obsažených ve White listu, pokud bude maskování požadováno)
  - Identifikátor agenta NSPTV, nebo jeho telefonní číslo
  - Identifikátor hovoru, tak jak je uveden v záznamech Call control systému
  - Datum a čas započetí hovoru, čas ukončení, délka hovoru
  - Další identifikátory, které je schopen nahrávací systém dostat v rámci signalizace probíhajícího hovoru, či od systému směrovací logiky hovorů
- Nahrávky jsou ve formátu umožňujícím odlišení směrů volaný a volající
- Záznamový systém musí umožnit oddělené přehrávání obou směrů hovoru
- Záznamový systém musí umožňovat přiřazení pravý/levý reproduktor pro přehrávaný kanál/kanály
- Umožnění zpřístupnění nahrávek pro nahrávací systémy operačních řízení jednotlivých složek IZS dle předem sjednaných kritérií a oprávnění

- Přímý přístup k systému a jeho ovládání a konfiguraci, přehrávání nahrávek a práce s nahrávkami (sestavování výběru, filtrování, export atd.) v rámci záznamového systému přes webové rozhraní s podporou šifrovaného přenosu https
- Logování přístupu a práce s nahrávkami s možností identifikace konkrétního uživatele, který danou operaci uskutečnil (=auditní logování)
- Export nahrávek i k nim příslušných metadat do složky IZS pouze pro oprávněné osoby
- Integrace nahrávacího systému se systémem agentské aplikace umožňující přímý přístup k nahrávkám daného agenta za definovanou dobu od jejich pořízení přímo z prostředí agentské aplikace.
- Přístup agenta k nahrávkám hovorům, dle definovatelných oprávnění (např.: hovory v rámci daného KDC, hovory samotného agenta, všechny hovory, ...)
- Umožnění free seating u agenta (agent může sedět na kterémkoliv pracovišti systému a systém jej musí správně identifikovat)
- Záznamový systém musí být flexibilní z pohledu rozšiřování – pro navyšování operátorských míst, počtu hovorů, prodlužování doby online uložení nebo archivace (do počtu 300 operátorů musí jít o jednoduché rozšíření)
- Systém musí umožňovat další zpracování hovoru – hlasové analýzy

4.6 Analytické nástroje

Součástí řešení musejí být i analytické nástroje pro aktivní sledování a reportování aktuálního stavu systému a historických trendů počtu volání pro jednotlivé lokality, tak aby bylo možné na zjištěné údaje reagovat případnými administrativními kroky ze strany řídících pracovníků NIS IZS. Analytické nástroje musí poskytovat i sumarizované přehledy v minimálně půlhodinových, hodinových a denních rozpadech a stejně tak umožnit přístup k informacím o konkrétním hovoru.

4.6.1 Požadavky na analytické nástroje

- Tabulkové zobrazení v HTML formátu
- Možnost exportu zobrazených do minimálně CVS a XML formátu
- Pro vybrané přehledy zobrazit data v grafické formě (sloupcový, čarový a koláčový graf)
- Nástroj musí umožnit vytváření vlastních návrhů sestav a ty následně zpracovávat a zobrazovat včetně exportu zobrazených dat
- Minimální zobrazované hodnoty pro každý hovor:
  - Číslo volajícího (s výjimkou případně maskovaných hovorů z White listu)
  - Volané číslo
  - Datum a čas přijetí hovoru
  - Délka hovoru
  - Informace o přesměrování hovoru, včetně identifikace linky na kterou byl hovor směrován
  - Informace o stavu hovoru (statusové kódy)
  - Unikátní identifikátor z IP telefonního systému pro jednoznačné párování dat s nahraným hovorem
- Minimální zobrazované hodnoty pro souhrny:

Podpis/signature:.....

- Počet hovorů na vstupu
- Počet hovorů ukončených funkcí „Black List"
- Počet hovorů označených ve „White List"
- Počet hovorů ukončených před jejich přijetím agentem (Abandon hovory)
- Počet hovorů převzatých agentem
- Počet konferenčních hovorů
- Průměrná délka hovoru v časovém období
- Maximální délka hovoru v časovém období
- Počet hovorů ukončených na agentském pracovišti
- Počet hovorů ukončených předáním na jiné složky (dělení dle složek)
- Počet hovorů ukončených předáním na externí číslo
- Průměrná délka fronty
- Průměrný čas čekání ve frontě
- Maximální čas čekání ve frontě

- Souhrnné reporty zobrazovat v množinách
  - Celý systém v uvedeném období
  - Rozdělení / omezení podle vstupních čísel (112,150,155,158)
  - Rozdělení / omezení dle krajů
  - Rozdělení / omezení dle agentů nebo skupiny agentů
- Časové omezení – granularita a minimální nejdelší doba výběru
  - Půlhodina (minimálně do rozsahu 48 půlhodin)
  - Hodina (minimálně do rozsahu 24 hodin)
  - Den (minimálně do rozsahu 31 dnů)
  - Týden (minimálně do rozsahu 8 týdnů)
  - Měsíc (minimálně do rozsahu 3 měsíců)

4.7 Implementace

Součástí dodávky řešení je i jeho kompletní konfigurace v rámci všech lokalit, do kterých bude systém rozvržen.

4.7.1 Proces implementace subsystému

- Instalace a konfigurace hlasových bran/SBC ve všech 14 KDC
- Konfigurace a registrace všech telefonních přístrojů v systému, jejich nastavení pro práci s primárními i záložním systémem.
- Konfigurace systému na předávání lokačních informací do navazujících systémů NIS IZS
- Konfigurace systému pro „Black list" umožňující zařadit hovor do jedné z následujících skupin a tím definovat způsob jeho zpracování dle požadavku definovaném v rámci funkčního prototypu. Blacklist bude dvoustupňový
  1. Úroveň – varování, ale povolí hovor,
  2. Úroveň – hovor bude ukončen, příp. dojde k přehrání hlášky a následně bude hovor ukončen

  Blacklist funguje pro každou složku zvlášť. Blacklist je celostátní pouze u HZS, ostatní používají pouze na krajské úrovni. Operátoři PČR budou upozorněni, že číslo je uloženo na blacklistu jiné složky.

U Black listu bude uvedeno číslo volajícího, důvod vložení, útvar, další postup, datum od kdy do kdy (den –den). Za správu odpovídá OO PP. Operátor bude upozorněn, že volá osoba z BL.
Veřejné telefonní automaty se do blacklistu nezařazují. Zařazování do blacklistu musí mít kontrolu na veřejné automaty.

- Konfigurace systému pro „White list", umožňující zařadit hovor do jedné nebo více následujících skupin:
  - Je poskytnuta informace o zařazení do zvláštní skupiny včetně zobrazení potřebných informací,
  - Dle skupiny je hovor upřednostněn ve frontě čekajících hovorů
  - Dle skupiny je hovor směrován na konkrétního agenta, skupinu agentů
  - Dle skupiny může být maskováno číslo volajícího

  White list (dále jen WL) – bude uvedeno číslo volajícího, důvod vložení, útvar, další postup, datum od kdy do kdy (den –den), vkládá VS IOS KRP, za správu odpovídá KRP. Mimo PČR se nesmí objevit (reporting), že se jedná o osobu na WL. Stejně tak pokud se jedná o sálové akce, nesmí se objevit, že se jedná o osobu z WL. Osoba z WL má vždy přednost, hovor bude spojen na 1.volného operátora 158.
- Instalace a konfigurace funkcí pro směrování hovorů na agenty
- Instalace a konfigurace nahrávacího systému tak, aby bylo zajištěno pořízení 100% nahrávek za hlasovými bránami a SBC, které byly zpracovány agentem NSPTV
- Nastavení oprávnění na systému nahrávání pro agenty a další oprávněné osoby definované zadavatelem systému v rámci předimplementační fáze projektu.

TATO STRANA JE PONECHÁNA PRÁZDNÁ