1. Předmět plnění

(1) Předmětem plnění veřejné zakázky je dodávka a implementace technologií pro zvýšení kybernetické bezpečnosti informačních systémů (IS) a komunikačních systémů (KS) zadavatele v souladu se standardy kybernetické bezpečnosti (dále také jen „dodávka“, „systém“, „řešení“ nebo „technologie“) včetně nezbytných služeb, podrobná specifikace dodávek a služeb je uvedena v dalších kapitolách tohoto dokumentu. Součástí plnění je dále podpora provozu na dobu minimálně 60 měsíců po předání řešení do ostrého provozu. Řešení musí být navrženo tak, aby náklady na provoz systému byly co nejmenší.

(2) I u technických parametrů, u kterých není výslovně uvedeno, že jde o požadovanou minimální či maximální hodnotu, lze nabídnout i řešení „lepší“, tedy řešení přesahující (ve smyslu výhodnějším z pohledu užitné hodnoty) hodnotu stanoveného požadavku, ledaže ze zadávacích podmínek výslovně vyplývá, že musí být splněna přesně daná hodnota.

(3) Předmětem plnění veřejné zakázky jsou zařízení a systémy uvedené v následující tabulce, včetně služeb (komodity):

Komodita	Zajišťovaná oblast	Stručný popis položky	Jednotka	Počet jednotek
K.1	Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS	1. Zavedení řízení přístupu do sítě podle standardu IEEE 802.1X. 2. Vybudování, resp. modernizace site-to-site VPN výjezdových základen 3. Provedení plné segmentace sítě ZZS včetně VPN a WiFi Součástí je dodávka software pro řízení přístupu k fyzickým i bezdrátovým sítím na bázi protokolu IEEE 802.1X, dodávka aktivních prvků (L3 přepínače, VPN routery, WiFi AP) a implementace a související služby.	soubor	1
K.2	Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS	1. Nasazení nástrojů pro centrální správu identit (identity management) a 2. Zavedení autentizace a řízení oprávnění uživatelů v IS ZOS s využitím vícefaktorové (min. dvoufaktorové) autentizace Součástí je dodávka software pro správu identit (identity management), software pro vícefaktorovou autentizaci na koncových zařízeních včetně tabletů výjezdových skupin, integrační rozhraní IS ZOS pro integrace s identity managementem, čtečky identifikačních karet ke koncovým zařízením uživatelů IS včetně tabletů výjezdových skupin a identifikační karet podle účelu využití (kontaktních SmartCard nebo bezkontaktní), implementace a související služby.	soubor	1
K.3	Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS	1. Zavedení nástroje pro správu a řízení oprávnění privilegovaných účtů správců IS-zaměstnanců ZZS a externích uchazečů-při vzdáleném i lokálním přístupu k IS. Součástí je pořízení software pro správu privilegovaných účtů a přístupů, dále implementace a související služby.	Soubor	1
K.4	Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů	1. Zaznamenávání činností (logů) IS ZOS, KS a souvisejících systémů do externích systémů. 2. Nástroje pro kompletní správu životního cyklu (pořízení, zpracování, zobrazení, prohledávání, ochrana, uchování a archivace) logů chráněných IS a souvisejících a podpůrných systémů a technologií.	Soubor	1

Komodita	Zajišťovaná oblast	Stručný popis položky	Jednotka	Počet jednotek
		3. Pokročilé notifikační nástroje bezpečnostních a nestandardních událostí IS ZOS. Součástí je pořízení software pro komplexní správu logů (log management), hardware nebo hardwarové appliance pro běh software a implementace a související služby.		
K.5	Nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS	1. Zavedení nástroje pro kontrolu komunikace v komunikačních sítích a mezi nimi. 2. Sledování a hloubková analýza síťových toků s detekcí nestandardního a nebezpečného provozu (škodlivého kódu). 3. Pokročilé notifikační nástroje bezpečnostních a nestandardních událostí IS ZOS. Součástí je pořízení software pro analýzu, vyhodnocení a ukládání síťových toků, serveru nebo hardwarové appliance pro běh software, implementace a související služby.	Soubor	1
K.6	Nástroje pro zajišťování úrovně dostupnosti informací	1. Nástroj pro automatizaci převodu IS ZOS do ZZOS 2. Nástroj pro zajištění úrovně dostupnosti záloh IS ZOS 3. Nástroj pro zajištění vysoké dostupnosti datových úložišť serverů Součástí je pořízení software pro automatické převedení provozu mezi ZOS a ZZOS, software a serveru nebo hardwarové appliance pro bezpečné ukládání záloh a jejich ochranu proti poškození, software pro replikaci a vysokou dostupnost interních úložišť serverů, rozšíření datových úložišť stávajících serverů, pořízení 5 koncových zařízení pro ZOS a 13 koncových zařízení pro výjezdové základny ZZS KV implementace a související služby.	Soubor	1
K.7	Vozidlové komunikační jednotky	Vozidlové komunikační jednotky	ks	40
K.8	Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS	Správa identifikačních prostředků	Soubor	1

2. Popis současného stavu

Tato část Zadávací dokumentace obsahuje informace důvěrné povahy. Zadavatel poskytne uchazeči tyto informace na základě žádosti a po uzavření Dohody o ochraně informací důvěrné povahy mezi uchazečem a zadavatelem. Podmínky žádosti jsou stanoveny v kapitole 15 části 2 Zadávací dokumentace a v části 5 Zadávací dokumentace.

3. Požadované parametry technického řešení

3.1. Obecné požadavky

(1) Zadavatel při výstavbě, správě a provozu technologií striktně dodržuje hledisko technologické neutrálnosti, tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců – tuto strategii musí splňovat i řešení dodané v rámci této veřejné zakázky.

(2) Pokud uchazeč vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k řešení zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

(3) Za předpokladu, že uchazečem navržené řešení vyžaduje fyzickou infrastrukturu (např. servery, úložiště, komunikační prvky atd.) neobsaženou v popisu předmětu plnění, zahrne uchazeč do své ceny všechny náklady na její pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.

(4) Pro každý softwarový produkt, který uchazeč nabídne v rámci svého řešení, budou v nabídce výslovně uvedeny všechny licenční nebo výkonové požadavky spojené s instalací a provozem řešení, včetně uvedení konkrétní infrastruktury, na které bude řešení provozováno.

(5) Uchazeč ve své nabídce detailně popíše vazby na stávající systémy Zadavatele, které jsou nezbytné pro správné fungování řešení nabízeného uchazečem.

(6) Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že uchazeč vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky – není přípustné implementovat např. další serverovou virtualizační platformu, adresářovou službu apod.

(7) Uchazeč prokáže, že všechny dodávky, které dodá Zadavateli:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

(b) mají plnou záruku od výrobce,

(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,

(d) obsahuji licenci na používání příslušného softwaru,

(e) jsou určeny pro provoz v České republice,

(f) z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

Tyto skutečnosti uchazeč doloží čestným prohlášením distributora, popř. uchazečem samotným, nelze-li prohlášení distributora získat. Zadavatel si vyhrazuje právo na zjištění původu výrobku při jejich převzetí, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

3.2. Specifické požadavky – K1 – Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS

(1) Komunikační síť ZZS KVK lze rozčlenit na 2 logické části – LAN centrály, VPN výjezdových základen. LAN je prostřednictvím firewallů dále propojena s dalšími veřejnými (internet) i neveřejnými (hlasové komunikace složek IZS) sítěmi. Výjezdové základny jsou prostřednictvím VPN připojena pouze do LAN, s jinými sítěmi mohou komunikovat pouze jejím prostřednictvím. Za součást VPN lze považovat i spoj ZOS-ZZOS, který je realizován s využitím optické komunikační infrastruktury KVK. Výjezdové základny i centrála jsou vybaveny WiFi přístupovými body. Segmentace sítě (VLAN) je jen základní (servery, transportní VLAN napojovaných sítí, ostatní zařízení), zařazování zařízení do VLAN je statické. Zařízení není při připojení do sítě identifikováno a má přístup do sítě odpovídající nastavení portu přepínače, do kterého se zařízení zapojí.

(2) Zvýšení bezpečnosti komunikační sítě bude dosaženo implementací:

(a) granulární a dynamické segmentace sítě s využitím protokolu IEEE 802.1X – zařízení bude při připojení do sítě ověřeno a podle své charakteristiky (a uživatele) mu bude na základě politik umožněn přístup do sítě a bude zařazeno do odpovídající VLAN bez ohledu na místo/způsob připojení.

(b) VPN s využitím principů SD-WAN pro dosažení vysoké dostupnosti připojení (centrála/LAN již disponuje 2 nezávislými vstupními body VPN, ale současné základnové prvky je nedokážou využít) a automatického přepnutí komunikace (VPN) výjezdových základen na ZZOS v případě výpadku ZOS

(c) centrálně spravované WIFI s aplikováním ověřování a segmentace dle 2(a) a podporou aktuálního zabezpečení komunikace WPA3-Enterprise

(3) V rámci plnění tedy bude v celé LAN implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby Active Directory s využitím technologie 802.1X.

(4) Dále bude implementován systém centrální správy, který poskytne celkový pohled na stav a konfiguraci LAN jako celku a současně umožní centrálně provádět změny konfigurace prvků LAN a vytvořením jednotně spravovaných VLAN zavést segmentaci sítě. Součástí centrálního systému bude systém řízení přístupu zařízení a uživatelů do síťové infrastruktury založený na standardu IEEE 802.1X a systém ověření původu DNS záznamů elektronickým podpisem.

(5) Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN. Součástí dodávky je vzorová konfigurace 802.1X na všech typech uživatelských koncových zařízení Objednatele (PC, notebooky, chytré telefony, tablety, tiskárny - Windows, Linux, MacOS, Android, IOS, embedded systémy periferií) a uživatelská dokumentace pro konfiguraci koncových zařízení uživateli.

(6) Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wifi bude nabízet více SSID (např. zaměstnanci, hosté, IoT) které budou obsluhovány samostatnými VLAN a budou napojeny na radius servery. Zaměstnanci budou prostřednictvím radius serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (BSSID) bude provedeno s využitím WPA3 (alternativně WPA2 dle podpory připojovaných zařízení) s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Řešení umožní použití autentizace prostřednictvím webového portálu (tzv. captive portál) s využitím jednorázových přístupových údajů a samostatných politik a restrikcí pro tento způsob autentizace.

(7) Pro WiFi budou zřízeny samostatné VLAN, které budou komunikačně odděleny od ostatních vnitřních sítí organizace. Tyto VLAN budou konfigurovány na úrovní stávajícího firewallu tak, aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a bude jim být přiřazen samostatný profil a/nebo virtuální kontext nakonfigurovaný ve firewallu.

(8) Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s přepínáním provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.

(9) Stávající VPN bude modernizována nasazením technologie SD-WAN (softwarově definované WAN), nezávislé na poskytovateli konektivity a založené na řízení na bázi vyhodnocování SLA komunikačních cesta a analýzy přenášeného provozu s možností směrování komunikace podle typu provozu, resp. druhu síťové služby.

(10) Součástí plnění je implementace pořízených technologií včetně osazení aktivních síťových prvků (přepínače, WiFi AP, VPN router) v centrále i na výjezdových stanovištích do připravených racků a na připravenou kabeláž (pasivní část LAN není součástí tohoto projektu).

3.3. Specifické požadavky – K2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS

(1) ZZS KVK provozuje nástroj pro ověřování identity uživatelů (MS Active Directory), nicméně není k dispozici systém pro řízení životního cyklu identit, jejich oprávnění v IS a sledování změn. Část aplikací IS není integrována a Active Directory a využívá vlastní databázi identit (uživatelů a účtů) a interní správu oprávnění těchto identit k jednotlivým částem a funkcím aplikace.

(2) Uživatelé se v IS autentizují pomocí uživatelského jména a hesla, s ohledem na rychlost přihlašování (i ve stresové situaci) není implementována politika silných hesel. Pro přístup k některým

systémům jsou používány sdílené obecné identity typu „operator1“. Není zaveden jednotný způsob ověřování identity uživatelů pro všechny IS a technologie.

(3) Výše uvedené se týká i specifických pracovišť v sanitních vozech, kde jsou používány tablety. Na těchto pracovištích jsou požadavky na jednoduchost a rychlost autentizace (i v terénu) velmi vysoké.

(4) Zvýšení úrovně zabezpečení v oblasti správy a ověřování identit uživatelů a správců bude dosaženo:

(a) Implementací nástroje pro automatickou správu identit (identity management) – systém bude vycházet z údajů v personálním systému a na základě předdefinovaných politik bude řídit celý životní cyklus identit včetně jejich nastavování jejich oprávnění v řízených systémech. Veškeré změny budou zaznamenávány. Nástroj pro správu identit bude jediným nástrojem pro řízení životního cyklu identit, tj. správci např. nebudou zakládat účty v Active Directory přímo, ale pouze prostřednictvím nástroje pro správu identit.

(b) Zavedením dvoufaktorové autentizace všech uživatelů s přístupem do IS ZOS – jako první autentizační faktor budou použity identifikační karty, jako další PIN karty nebo jiný údaj („tajemství uživatele“). Pracovníkům OS bude navíc automatizován proces přihlášení k IS – po úspěšném přihlášení do operačního systému budou uživateli automaticky spuštěny předdefinované aplikace podle uživatelova profilu a uživatel bude do těchto aplikací automaticky přihlášen (SSO – single-sign-on). Dvoufaktorová autentizace do aplikace MZD bude zavedena v nově pořízených vozidlových komunikačních jednotkách i na stávajících vozidlových tabletech pro MZD. Standardem bude používání kontaktních karet SmartCard či tokenů, u vybraných uživatelů (pracovníci OS) budou využívat bezkontaktní karty pro rychlejší přihlášení a migraci uživatelů mezi pracovišti při zachování stavu aplikací včetně rozpracovaných činností. V budoucnu lze podle stavu technologického rozvoje a vývoje legislativy (ochrany osobních údajů) očekávat i využívání jiných faktorů (např. biometrických) pro autentizaci – řešení by na tento stav mělo být připraveno.

(5) Systém pro správu identit (Identity management – IDM) bude koncipován jako ústřední systém správy ICT. Bude kopírovat organizační strukturu Zadavatele a umožní automatizaci úkonů spojených se správou identit v informačních systémech Zadavatele a zvýší úroveň kybernetické bezpečnosti.

(6) Automatizací správy identit dojde k odstranění nebo alespoň významnému omezení rutinních činností správců systémů spojených se správou identit a dále ke zrychlení reakcí na změny v organizace (např. změny oprávnění v systémech při změně pozice zaměstnance), snížení chybovosti způsobené ručním zadáváním údajů do systémů a/nebo nedodržením procesů (např. včasným nenahlášením odchodu zaměstnance všem správcům systémů nedojde včas nebo vůbec ke zrušení přístupových účtů zaměstnance) a získání okamžitého detailního přehledu o stavu identit a jejich oprávnění v systémech Zadavatele.

(7) Na IDM budou navázány hlavní informační systémy Zadavatele – adresářová služba Active Directory, groupware a specializované aplikace a informační systémy uvedené v Popisu současného stavu prostřednictvím jejich API nebo integrací s Active Directory. IDM tak vytvoří jeden autorizovaný zdroj informací ohledně uživatelů a jejich práv přístupů k jednotlivým systémům, tím bude současně provedena konsolidace identit, která je nezbytná pro realizaci budoucí uvažovaných projektů spojených s identitami – realizaci nařízení Evropské unie č. 910/2014 eIDAS o elektronické identifikaci a důvěryhodných službách pro elektronické transakce.

(8) IDM poskytne uživatelům základní službu „Přístup k systémům synchronizovaným s IDM“. Tato služba je realizována v procesech přístupu do systému, přístup k aplikacím synchronizovaným s IDM apod. V případě, že jsou poskytovány aplikace externím subjektům, zajistí IDM přihlášení k aplikacím pro externí subjekty. V IDM budou vytvářeny role a těm se přidělovány oprávnění pro jednotlivé aplikace. Role budou naplňovány konkrétními uživateli. Tímto způsobem mohou být definovány role pro všechny zaměstnance a nový zaměstnanec automaticky při nástupu získá všechna potřebná oprávnění, a naopak při ukončení pracovního poměru bude zřejmé, že mu všechna přístupová práva byla odebrána.

(9) V rámci IDM dojde k přiřazení zaměstnanců k pracovním pozicím a rolím pro umožnění řízení oprávnění, pracovních postupů (workflow) apod. založeném na rolích. IDM bude využívat vhodné

(rozšířené, nepovinné apod.) atributy poskytované personálním systém pro optimalizaci správy životního cyklu identit a její usnadnění a zpřesnění.

(10) Součástí IDM bude detailní logování prováděných změn pro možnost zjištění uživatelských oprávnění v libovolném času v minulosti (od nasazení systému).

(11) Implementace systému bude provedena v souladu s § 19 Nástroj pro řízení přístupových oprávnění Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

3.4. Specifické požadavky – K3 – Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS

(1) V současné době se je správa většiny prvků IS a KS ZZS KVK na základě servisní smlouvy prováděna externími subjekty, jejichž specialisté/správci přistupují k prvkům vzdáleně, převážně prostřednictvím VPN. Přihlášení správce do VPN je zaznamenáváno, ale jeho další činnost v IS již monitorována ani zaznamenávána není (s výjimkou běžného logování v jednotlivých prvcích, pokud jej provádí) a ani řízena. Většina správců disponuje tzv. privilegovanými účty, tj. účty s vysokými (administrátorskými) oprávněními ke spravovaným a souvisejícím prvkům. ZZS KVK nemá kontrolu nad správou a využíváním těchto účtů u jednotlivých subjektů.

(2) Zvýšení úrovně zabezpečení v oblasti řízení přístupových oprávnění interních i externích správců bude dosaženo implementací nástroje pro správu a kontrolu privilegovaných uživatelů (tzv. PIM (privileged identity management) a PAM (privileged access management). Nástroj zajistí oddělení správců od privilegovaných účtů. Privilegované účty budou ve správě nástroje a správcům bude po přihlášení k nástroji na základě politiky umožněno použít zprostředkované přihlášení ke spravovanému systému s využitím privilegovaného účtu, ale bez jeho znalosti. Současně bude veškerá činnost správce nezměnitelně zaznamenávána. Nástroj zajistí automatickou pravidelnou obměnu (rotaci) hesel spravovaných privilegovaných účtů. Nástroj bude využíván i pro řízení a monitorování činnosti interních správců ZZS KVK.

(3) Navrhované řešení musí monitorovat aktivity identifikovaných privilegovaných účtů (tj. uživatelů používajících účty s vysokou úrovní oprávnění), a tím minimalizovat bezpečnostní rizika spojená s přístupem ke zdrojům příslušných systémů.

(4) Privilegované účty umožňují přístup ke zdrojům příslušných systémů včetně manipulace s nimi, a proto jsou významným bezpečnostním rizikem. Dále znalost přihlašovacích údajů může být sdílena mezi více uživateli, tudíž odpovědnost za případné zneužití by mohla být velice těžko dohledatelná. Tato rizika se vztahují na všechny systémy, počínaje operačními systémy, databázemi, síťovými prvky, komplexními informačními systémy distribuovanými jako produkt, nebo vyvinutými na míru.

(5) Důležitou požadovanou řešenou oblastí je detailní audit užití a aktivity privilegovaných účtů. Aktivita bude zaznamenávána nahráváním uživatelských relací s využitím tzv. „jump serveru“ – snímáním obrazovky a logování uživatelského vstupu (key-logging). Každá akce (stisk klávesy, změna obrazovky apod.) privilegovaného účtu je nahrávána ve video formátu a je jednoznačně přiřazena konkrétní osobě. Nahrávky jsou zabezpečeným způsobem přenášeny do centrálního úložiště, kde jsou dlouhodobě uchovávány a je v nich možno kontextově vyhledávat. Takové nahrávky budou klíčovým důkazem, kterým je možné uživateli jednoznačně prokázat veškeré jeho aktivity. Nedílnou součástí je také zajištění auditní stopy správy privilegovaných účtů.

(6) Systém zajistí komplexní správu privilegovaných identit (účtů, uživatelů) a bezpečnou správu jejich hesel a SSH klíčů a zajistí personalizaci sdílených účtů.

(7) Systém zajistí oddělení rolí (Segregation of Duties) a zavedení kontroly „čtyř očí“ (Dual Control

(8) Součástí komodity bude vybudování monitorovaného serveru/appliance, který bude sloužit pro provádění vzdálené správy externími partnery – jejich veškerá činnost tak bude zaznamenávána. Server bude bezpečně publikován do internetu prostřednictvím stávajícího firewallu a veškerá komunikace probíhající přes internet musí být šifrována bez potřeby využití VPN apod.

3.5. Specifické požadavky – K4 – Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

(1) V současné době nevlastní ZZS KVK žádný nástroj pro (centrální) zaznamenávání činnosti (logů) IS a KS navazujících systémů. Činnosti jsou v některých systémech zaznamenávány lokálně, ale bez jednotné politiky, dlouhodobého ukládání a ochrany logů před změnou, přetečením apod. Chybí tak nástroj pro podporu řešení případných kybernetických událostí a incidentů poskytování konsolidovaných informací před vznikem a v průběhu události/incidentu. Absence nástroje také neumožňuje efektivně analyzoval chování IS, KS a souvisejících systémů z pohledu kybernetické bezpečnosti, ale i z pohledu běžného provozu pro účely zavádění preventivních opatření předcházejících výskytu nestandardního provozního stavu a/nebo opatření k zamezené jeho opakování.

(2) Zvýšení úrovně zabezpečení v oblasti řízení přístupových oprávnění interních i externích správců bude dosaženo:

(a) Implementací nástroje pro správu logů (tzv. log management) - zavedením komplexního systému pro správu logů dojde ke centralizovanému sjednocení různých bází bezpečnostních a provozních záznamů, které jsou poskytovány různými typy hardwarových zařízení, dále různými provozovanými operačními systémy a aplikacemi, včetně všech nástrojů implementovaných v rámci tohoto projektu. Zaznamenané činnosti budou k dispozici na jednom místě ve sjednoceném formátu při zachování jejich dostupnosti, důvěrnosti a integrity. Systém zajistí uložení dat k okamžitému prohlížení a prohledávání minimálně po dobu 12 měsíců a bude umožňovat archivaci starších záznamů s možností rychlé obnovy archivu v případě potřeby. Systém musí zajistit integritu archivu.

(b) Pořízením vyhrazeného serveru nebo hardwarové appliance pro provoz nástroje pro správu logů, aby byla zajištěna nezávislost nástroje na infrastruktuře ZZS KVK a tím schopnost zaznamenávání její činnosti i v nestandardních provozních stavech (přetížení, start, nestabilita apod.)

(3) Požadované řešení je standardní Log/Event Management, který musí umožnit být v budoucí rozšíření o další systémy (např. systém SIEM) nebo napojení na služby SOC (Security operations center).

(4) Řešení umožní sofistikovanou, transparentní a opakovatelnou pokročilou analýzu, spojenou s řešením běžných provozních i bezpečnostních událostí/incidentů a upozorňováním na ně, a to z kritických i nekritických a podpůrných systémů a aplikací. Řešení musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, primárně v českém jazyce a dále variantně v jazyce anglickém, bez nutnosti používat SQL (či obdobnou „programátorskou“) syntaxi pro definici či úpravu reportů.

(5) Nabízené řešení musí zachovávat originál logů za účelem bezpečnostního auditu, a to v souladu s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů.

(6) Řešení musí umožnit snadné a rychlé multikriteriální vyhledávání pro účely analýz, auditů, a podporu běžného provozu komplexního řešení ICT infrastruktury ZZS KVK.

(7) Pro zajištění požadavků bezpečnosti musí řešení LM konfigurovatelným uživatelským oddělením rolí a ochranou centralizovaných logů před neoprávněným přístupem k citlivým datům.

(8) Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace.

(9) Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu.

(10) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může se jednat o jediné zařízení, softwarový nástroj či appliance nebo o řešení složené z více samostatných a vzájemně kompatibilních komponent. Zařízení umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Ukládání všech informací do bude prováděno

jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých.

(11) Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích na straně firewallu za pomoci jeho SSO agentů či logů a dalších přístupových a autentifikačních systémů (např. RADIUS logy). Dále budou získávány informace o překladu zdrojových, vnitřních IPv4 adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení.

(12) Bude umožňovat uchování každého záznamu v jeho nezměněné podobě, ale zároveň bude schopný dávat jednotlivé události ihned do souvislostí a vyhodnocovat riziko a případné bezpečnostní události aktivně notifikovat, resp. reportovat.

(13) Zdroje dat pro budou vybrány z tzv. primárních a podpůrných (technických) aktiv zadavatele. K jejich určení bude využito Vyhlášky č.317/2014 Sb. o významných informačních systémech a jejich určujících kritérií přiměřeně uzpůsobených a aplikovaných na prostředí zadavatele (zadavatel neprovozuje významný informační systém). Nezbytné konfigurace zdrojových (popř. dalších navázaných) systémů jsou součástí plnění.

(14) Implementace systému bude v provedena v souladu s § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

3.6. Specifické požadavky – K5 – Nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS

(1) V současnosti nemá ZZS KVK implementovánu žádnou technologii umožňující detekovat a identifikovat bezpečnostní události na úrovni síťového provozu, o této události informovat zodpovědné osoby a tuto (a související) události uložit pro následnou analýzu. ZZS KV tak nemá (kromě UTM funkcionalit stávajícího firewallu a antivirových systémů) žádnou možnost zachycení kybernetické událostí jinak než detekcí nestandardního chování IS a/nebo KS (ke kterému ovšem nemusí u mnoha typů kybernetických událostí dojít). ZZS KVK také nemůže efektivně analyzovat chování IS, KS a souvisejících systémů z pohledu kybernetické bezpečnosti, ale i z pohledu běžného provozu a chování uživatelů IS a KS pro účely zavádění preventivních opatření předcházejících výskytu nestandardního provozního stavu a/nebo opatření k zamezení jeho opakování.

(2) Zvýšení úrovně zabezpečení v oblasti detekci kybernetických bezpečnostních událostí vůči IS ZOS bude dosaženo:

(a) Implementací nástroje pro sledování a hloubkovou analýzu síťových toků (netflow) na perimetru sítě a v libovolném jejím segmentu dle požadavků. Nástroj zajistí tzv. „viditelnost sítě“ – vizualizaci síťového provozu v grafické podobě pro získání detailního přehledu o veškeré síťové komunikaci, zařízeních a chování uživatelů v reálném čase. Nástroj dokáže „porozumět“ obvyklým komunikačním protokolům a na základě analýzy komunikace detekovat bezpečnostní hrozby a nestandardní chování aplikací a systémů. V případě detekce bezpečnostní události notifikuje správce a současně aktivně reaguje a automaticky blokuje nebezpečný provoz nebo umožní jeho manuální blokování. Nástroj bude ukládat historii síťového provozu (resp. síťových toků) po dobu min. 1 měsíc pro účely operativní analýzy a podpory při řešení kybernetických incidentů nebo provozních problém. Současně bude ukládat získané informace a také informace o své činnosti (změny konfigurací, aktualizace) do nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů.

(b) Pořízením vyhrazeného serveru nebo hardwarové appliance pro provoz detekci kybernetických bezpečnostních událostí, aby byla zajištěna nezávislost nástroje na infrastruktuře ZZS KVK a tím schopnost zaznamenávání její činnosti i v nestandardních provozních stavech (přetížení, start, nestabilita, kybernetická událost/incident apod.)

(3) Systém musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.

(4) Systém zajistí detailní viditelnost do síťové komunikace s drill down prokliky na veškerá uložená data.

(5) Všechny komponenty systému musí být instalované v interním prostředí zadavatele („on premise“) a použití externích komponent nebo cloudových služeb se nepřipouští.

(6) Řešení bude obsahovat řešení uživatelských scénářů / způsobů použití v různých situacích (provoz, událost, incident) a umožní implementovat vhodné operátorské, správcovské (a další vhodné) role a profily

(7) Systém zajistí integritu uložených logovaných událostí a toků

(8) Systém bude disponovat pokročilou behaviorální analýzou, tj. detekcí nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, detekce provozních problémů) a bude umožňovat detekci anomálií vzhledem k dlouhodobému profilu chování zařízení na síti.

3.7. Specifické požadavky – K6 – Nástroje pro zajišťování úrovně dostupnosti informací

(1) Pro provoz aplikací a systémů využívá ZZS KVK virtualizační platformu založenou na VMware vSphere a sestavenou ze 3 fyzických serverů. Disková kapacita platformy je tvořena interními disky serverů. Disková a paměťová (RAM) kapacita serverů není dostatečná pro zajištění provozu v režimu vysoké dostupnosti (high-availability), tj. platforma nemá dostatek zdrojů pro překlenutí výpadku jednoho ze serverů a není tak schopna zajistit dostatečnou dostupnost výpočetních zdrojů hostovaným aplikacím a systémům. Současně nejsou kapacity dostatečné pro provoz nově pořizovaných nástrojů a systém diskové virtualizace již není výrobce podporován.

(2) Zálohování IS ZOS je prováděno automaticky pokročilým zálohovacím systémem Veeam Backup & Recovery a zálohy jsou ukládány na 2 nezávislá síťová úložiště NAS umístěná v různých lokalitách (ZOS a ZZOS). Zálohovací systém zálohy plně kontroluje, tj. při jeho kompromitaci či poškození může dojít k znepřístupnění záloh.

(3) Koncová zařízení operátorských pracovišť operačního střediska a výjezdových základen jsou provozována s operačními systémy Windows 7, pro které již výrobce neposkytuje podporu a bezpečností aktualizace. Hardware koncových zařízení nedisponuje podporou pro aplikaci šifrovacích mechanismů (chybí TPM čip) a nemá podporu výrobce pro instalaci aktuální verze operačního systému.

(4) ZZS KVK provozuje ZZOS, do kterého jsou replikovány klíčové aplikace IS ZOS nezbytné pro zajištění operačního řízení. Přepnutí provozu IS ZOS do ZZOS (a zpět) vyžaduje provedení sady přesně navazujících úkonů a určitou odbornou znalost pro vyhodnocení stavu jednotlivých kroků a řízení jejich provádění. ZZS KVK nemá nástroje pro automatizaci těchto úkonů a nemůže tak zajistit spolehlivou (a rychlou) dostupnost IS ZOS v ZZOS v případě potřeby.

(5) Zvýšení úrovně dostupnosti informací bude dosaženo:

(a) Rozšířením diskové a paměťové kapacity serverů – pro zajištění potřebných kapacit budou do serverů doplněny disky a paměťové moduly RAM a bude implementován software pro automatickou replikaci dat a zajištění jejich dostupnosti v případě výpadku některého serveru. Adekvátně bude navýšena kapacita serverů v ZZOS, aby byla zachována schopnost ZZOS provozovat IS ZOS. Současně bude rozšířena kapacita síťového úložiště NAS pro ukládání záloh, aby odpovídala nárůstu požadavků na rozšíření datové kapacity serverů.

(b) Modernizací systému diskové virtualizace tak, aby byla zachována současná funkcionalita (především vysoká dostupnost a výkon), kompatibilita se serverovou virtualizací

(c) Implementací bezpečného datového úložiště pro zálohy – požadováno je zařízení s nastavitelnou retencí ukládaných dat (záloh) tak, aby uložená data nebylo možné po určitou

(nastavitelnou) dobu změnit. Z pohledu zálohovacího systému půjde o zařízení typu WORM (Write One, Read Many).

(d) Pořízením koncových zařízení – tím bude zajištěna odolnost koncových zařízení (a tím i celého IS ZOS) proti napadení. Nová koncová zařízení budou vybavena aktuálním operačním systémem s podporou výrobce a zajištěnými bezpečnostními aktualizacemi a hardwarovou podporou pro implementaci šifrování obsahu interního úložiště a možností bezpečného ukládání citlivých dat (např. šifrovacích klíčů).

(e) Implementací nástroje pro automatické přepnutí provozu IS ZOS mezi ZOS a ZZOS a zpět. Je požadován nástroj, který zajistí rekonfiguraci dotčených systémů a síťových služeb (zejména DNS) tak, aby IS ZOS byl dostupný uživatelům v ZZOS a výjezdových základnách z prostředí ZZOS.

(6) V rámci komodity bude vybudováno bezpečné úložiště pro ukládání dat, která musí být ochráněna proti jakékoli modifikaci po určenou dobu (retenční lhůtu). Jedná se např. o zálohy databází, kritická nestrukturovaná data, ale kompletní zálohy virtuální serverů apod. Úložiště umožní konfigurovat více kategorií chráněných dat a odpovídajících retenčních lhůt. Data bude možné ukládat pomocí běžných síťových protokolů, např. SMB/CIFS.

(7) Úložiště bude nativně spolupracovat se stávajícím zálohovacím systém pro možnost přímého ukládání záloh kritických dat a jejich ochrany před zničení škodlivým kódem (např. ransomware) nebo jiným způsobem.

(8) V rámci komodity budou implementována nově pořízená koncová zařízení operačního střediska a výjezdových stanovišť včetně migrace pracovních (služebních) uživatelských dat a zprovoznění vícefaktorové autentizace uživatelů dodanými identifikačními prostředky.

3.8. Specifické požadavky – K7 – Vozidlové komunikační jednotky

(1) Vozidlové komunikační jednotky (déle jen jednotky) zásahových (převáženě sanitních) vozidel budou sloužit pro provoz aplikace MZD (Mobilní zadávání dat), EKP (Elektronická kniha pacienta) a IS ZOS, které budou poskytovat posádce informace potřebné pro provádění zásahu a současně i pro poskytování zpětné vazby o jeho průběhu, včetně procesu předávání pacienta do zdravotnických zařízení. Popis procesů při používání aplikací v jednotkách bude uchazeči předán po zahájení realizace projektu.

(2) Jednotky budou upevněny ve vozidlech tak, aby umožnily bezproblémové ovládání během jízdy a současně byly snadno vyjímatelné a použitelné mimo vozidlo a nezávisle na něm. Jednotky budou podporovat standardní formy bezdrátové komunikace (LTE, WiFi, Bluetooth) pro zajištění on-line komunikace v různých podmínkách a prostředí. Uchazeč poskytne technickou podpora montáže do vozidel (samotná montáž zařízení do vozidel není předmětem plnění).

(3) Jednotky musí být odolné proto nešetrnému zacházení včetně pádu na zem při zachování mobility a snadného ovládání.

(4) Technické provedení jednotek je požadováno ve formátu „tablet“, tj. ploché zařízení s dotykovým ovládáním prostřednictvím displeje, bateriovým napájením, integrovanými komunikačními prvky a sloty/konektory pro periférie a integrovanými bezpečnostními komponenty (TPM chip, čtečka otisků prstů, čtečka čipových karet). Displej musí umožňovat „ruční podepisování“ prstem či předmětem (perem, stylusem apod.) Jednotky budou vybaveny operačním systémem, kompatibilním se stávajícími aplikacemi MZD, EKP a IS ZOS a nově dodávanými technologiemi.

3.9. Specifické požadavky – K8 – Správa identifikačních prostředků

(1) Pro správu identifikačních prostředků, které budou nositeli elektronických identit bude implementován systém pro centrální správu životního cyklu těchto prostředků ((re)iniciace, přidělení uživateli včetně nahrání certifikátu v zastoupení, uživatelské prodloužení certifikátů, odvolání certifikátů apod.). Autentizační (doménové) certifikáty budou vydávány interní certifikační autoritou, které bude součásti PKI (public key infrastucture) vybudované v rámci dodávky. Řešení umožní i správu kvalifikovaných certifikátů externích (veřejných) certifikačních autorit, jejichž certifikáty budou

využívány k podepisování elektronických dokumentů, klíčových operací uživatelů, vytváření kvalifikovaných elektronických pečetí apod.

(2) Doporučení vhodných certifikačních služeb pro implementaci, přičemž si zadavatel vyhrazuje možnost stanovit požadavek na implementaci konkrétní certifikační služby od konkrétního kvalifikovaného poskytovatele certifikačních služeb dle § 9 odst. 2, písm. e) zákona č. 227/2000 Sb. (https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx) a uchazeč je povinen stanovenou certifikační službu implementovat. Pro jednoznačnost zadavatel výslovně uvádí, že bude zvolen jeden konkrétní kvalifikovaný poskytovatel.

(3) Součástí dodávky systému pro správu identifikačních prostředků bude i rozhraní PKCS#11 (https://cs.wikipedia.org/wiki/PKCS_11) pro přístup ke kartám a certifikátům na kartách i na koncových HW zařízeních.

(4) Implementace systému bude provedena v souladu s § 19 Nástroj pro řízení přístupových oprávnění Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

3.10. Specifické požadavky – povinné parametry řešení

(1) V dále uvedených tabulkách jsou uvedeny minimální požadované (povinné) parametry dodávaného řešení.

(2) **Účastník ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Účastník tedy uvede konkrétní technické parametry nabízeného zboží, vč. uvedení výrobce a obchodního / typového označení jednotlivých komponentů. Údaje o výrobci a obchodním (či typovém) označení budou uvedeny a doloženy v tabulkách povinných parametrů; konkrétní parametry mohou být buď rovněž doplněny do tabulky, nebo mohou být doloženy jinde v nabídce např. formou katalogových listů apod., v takovém případě ale musí být v tabulce odkázáno na část nabídky, ve které je možné naplnění parametru ověřit.**

(3) **Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí prokazovat (nepostačuje pouze potvrzení či zkopírování požadavku Zadavatele), že nabízené řešení jednoznačně splňuje všechny požadavky.**

(4) **Uchazeč musí všechny povinné parametry splnit, v případě nesplnění je jeho nabídka vyloučena.**

(5) Požadavky na zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS:

Komodita K.1 - Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém řízení přístupu do sítě podle standardu IEEE 802.1X	Provedení	Softwarová appliance pokročilého NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS server a databáze uživatelů a zařízení.		
	Nastavení přístupů	Nastavení síťového přístupu uživatelů a zařízení podle politik min. pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém		
	Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN		
	Základní autentizační metody	Min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty		
	Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází - Active Directory, LDAP, ODBC		
	Nezávislá autentizace a autorizace	Úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, ale autorizace proti externí SQL databázi.		
	Rozšířená autentizace a autorizace	Podpora autentizace a autorizace min. LDAP, Microsoft Active Direcory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta).		
	Kontexová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory.		
	Externí identity	Podpora autentizace externími identitami - min. Microsoft, Google.		
	Komplexní autorizace	Autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. pro omezení celkového času online či objemu přenesených dat za delší časové období		
	Dynamická autorizace	Podpora RADIUS CoA podle RFC3576. Možnost změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení.		
	Izolace klientů	Zpracovávání syslog zpráv z externích zdrojů, vyhledávání definovaných událostí a automatizovaná reakce na ně. Minimálně v rozsahu příjmu zpráva ze stávajícího firewallu a izolace konkrétního klienta na základě těchto zpráv.		
	Zpracování syslog	Vestavěná podpora tvorby a úprav vlastních parserů, syslog zpráv pro napojení na další systémy třetích stran		
	Bezpečnost	Podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)		
	Správa	Vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení		

Komodita K.1 - Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS				
	Portál	Captive portál pro uživatele a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně. Integrovaná podpora úpravy vzhledu		
	Rychlé přihlášení	Podpora přihlášení prostřednictvím QR kódu. Zapamatování úspěšně autentizovaných/registrovaných klientů a zjednodušení opakovaných přihlášení (např. jen potvrzení uvítací/informační) stránky.		
	Registrace	Podpora samoobslužné registrace s ověřením SMS, e-mailem apod.		
	Ochrana identit	Veškeré identitní údaje v systému budou uložena ve výrobcem dodané a podporované šifrované databázi, které bude nativní součástí dodaného produktu, s minimální enkrypcí uložených dat ve standardu AES min. 128-bit.		
	Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení např. tiskárny, modality, technologické prvky, IoT.		
	Vysoká dostupnost	Integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru min. 2 appliance. Druhá appliance není součástí dodávky.		
	Licence	Licence pro min. 500 konkurenčních koncových zařízení ověřovaných pomocí 802.1X bez omezení počtu uživatelů.		
	Automatizace a integrace	REST-API rozhraní min. pro základní funkce AAA, příjem syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Tvorba/modifikace vlastních parserů syslog.		
	Kompatibilita	Appliance určena pro provoz v prostředí stávající serverové virtualizace		
	Záruka	Záruka min. 60 měsíců v místě instalace, včetně podpory výrobce a nároku na nové verze software včetně aktualizací.		
WiFi přístupový bod (AP) 23x	Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na stěnu nebo strop		
	Frekvence	činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly s podporou standardu OFDMA		
	Anténní systém	interní systém pro min. 2x 2 MIMO, optimalizovaný pro montáž na strop		
	Přenosové rychlosti	SU-MIMO 5GHz min 1200Mbps, SU-MIMO 2.4 GHz min. 550Mbps		
	Standardy	podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN		
	Řízení klientů	automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma)		
	Rušení	průběžná detekce non-WiFi rušení a spektrální analýza		
	Multi SSID	podpora vysílání min. 8 SSID (WiFi sítí) současně, podpora přiřazení každého SSID samostatné VLAN		
	Zatížení	min. 250 přiřazených (asociovaných) klientů na radiový modul		
	Porty	min. 1x 1Gb, PoE s podporou standardů 802.3at a 802.3af		
	Úsporné napájení	podpora standardu 802.3az - Energy-Efficient Ethernet (EEE)		
	Řízení provozu	klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu		
	Řízení kvality služeb	automatické řízení kvality služeb (QoS) pro hlas a video		
	Současná obsluha více klientů	Popdora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output		
	Bezpečnost	Detekce cizích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu		

Komodita K.1 - Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS				
		Integrovaný bezpečnostní modul TPM pro uložení citlivých údajů (přihlašovací údaje, šifrovací klíče apod.)		
	Virtuální kontrolér	Virtuální, vysoce dostupný kontrolér obsažený ve firmware každého přístupového bodu. Umožňuje kompletní centrální správu WiFi infrastruktury (i prostřednictvím VPN) a řízení jejího provozu včetně roamingu klientů bez potřeby externích systémů - cloud, management aplikace/appliance apod.		
	WPA	podpora standardu WPA3 (Wi-Fi Protected Access III)		
	IoT a lokalizace	integrovaná hardwarová podpora standardu 802.15.4 (Zigbee) a Bluetooth 5.0		
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, web rozhraní.		
	Správa frekvenčního pásma	automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference		
	Záruka	záruka min. 60 měsíců		
Přístupový přepínač 5x	Základní parametry	L2/3 přepínač v rackovém provedení		
	Porty a propustnost	48x 1 GB RJ-45 PoE+ + 4x 1Gb SFP (nesdílené), min. 104 Gb/s		
	Směrování	min. statické směrování na L3 vrstvě pro IPv4 I IPv6		
	Propustnost	neblokovaná architektura		
	Automatizace VLAN	Podpora protokolu MVPR pro automatické zjišťování a přiřazení		
	Agregace portů	podpora LACP		
	Dualstack	IPv4 a IPv6 dualstack včetně podpory ACL a QoS		
	VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření		
	Ověřování uživatelů a zařízení	podpora 802.1X		
	PoE	podpora standardů 802.3af a 802.3at (PoE+ 30W/port), celkový PoE výkon min. 370W		
	Hlučnost	maximální hlučnost max. 30 dB při plné zátěži		
	Zrcadlení portů	Zrcadlení provozu portů pro diagnostiku a bezpečnostní monitoring, min. 4 zrcadlené skupiny		
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní, podpora uložení více konfigurací a min. 2 obrazů firmware pro bezpečný a jednoduchý upgrade		
	Automatizace a integrace	Integrované REST API rozhraní pro ovládání síťových funkcí		
	Záruka	min. 60 měsíců, oprava do 2 pracovních dnů v místě instalace, včetně nároku na opravné verze firmware		
VPN router 13x	Porty	min 5x 1GbE (min. 1x WAN), USB pro ext. modem		
	Základní funkce	Koncové VPN zařízení s podporou SD-WAN a integrovaným firewallem		
	Počet současných spojení	min. 500 000		
	Propustnost SSL VPN	min. 400 Mbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 25 klientů		
	Propustnost SSL inspekce	min. 300 Mbps		
	Propustnost firewallu	min. 5 Gbps pro libovolnou velikost paketu		
	Virtualizace	min. 5 virtuálních kontextů		

Komodita K.1 - Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS				
	Vysoká dostupnost	režimy Active/Passive i Active/Active se společnou konfigurací		
	Dualstack	podpora současného běhu IPv4 a IPv6		
	Aplikační kontrola	detekce aplikací pro definici směrování SD.WAN		
	Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení		
	Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu		
	Management a monitoring	HTTP/S, SSH, SNMP, syslog,		
	SD-WAN	integrovaná podpora SD WAN-min. rozkládání zátěže a vysoká dostupnost více internetových přípojek, řízení na základě SLA provozu		
	Sledování toků	export síťových toků (Netflow nebo ekvivalent)		
	Standardní funkce	NAT, statické a dynamické routování, publikace interních serverů		
	Kompatibilita	Kompatibilita se stávajícími firewally pro plné využití VPN a SD-WAN funkcí		
	Záruční servis	Záruční servis na min. 60 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Výměna vadného zařízení max. následující pracovní den po nahlášení závady v místě instalace, včetně nároku na aktualizace firmware a SD-WAN funkcí		

(6) Požadavky na zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém pro správu identit (Identity management - IDM)	Základní funkce	Systém pro správu identit - Identity management (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.		
	Licence	Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.).		
		Minimální počet spravovaných uživatelů je 1000		
	Škálovatelnost	Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů - minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh.		
	Evidence aplikací a rolí	Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.		
	Uživatelské role	Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.		
	Historizace	Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti.		

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	Automatizace	Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.).		
	Logování	Systém bude poskytovat auditní logy ve formátu vhodném pro systém typu správy logů (Log management)		
	Logování systému	Systém obsahuje logování min. následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log)		
	Správa identit	Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury.		
	Systematizovaná místa	Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu.		
	Podpora eIDAS	Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.		
	Vysoká dostupnost	Systém musí být možno nasadit na více serverů v režimu vysoké dostupnosti.		
	Požadavky na portál - obecné	IDM bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému.		
	Podpora mobilních zařízení	Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno)		
	Správa referenčních objektů	Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systemizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát.		
	Referenční objekty	Systém umožní přidávání a správu dalších typů referenčních objektů, a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity		
	Zabezpečení referenčních objektů	Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů		
	Rozšiřující atributy	Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.		
	Přehledné zobrazení	Portál umožní grafické zobrazení a současné vyhledávání identit / uživatelských účtů ve stromové organizační struktuře a prohledávání organizační struktury včetně systematizovaných míst až do úrovně jednotlivých uživatelských účtů (identit).		
	Vyhledávání - diakritika	Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Parizek vyhledává i Pařízek apod.)		

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	Správa certifikátů	Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti.		
	Obrázky	Systém umožní k jednotlivým účtům (identitám) přikládat obrázky - fotografie.		
	Přesun identit	Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními.		
	Kopírování rolí	Systém umožní kopírovaní aplikačních rolí, pracovních pozic mezi jednotlivými systematizovanými místy.		
	Ochrana proti chybám	Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod).		
	Aktivní uživatelé	Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem		
	Slučování identit	Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.		
	Export údajů	Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu		
	Filtrování	Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.		
	Správa oprávnění	Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.)		
	Granularita oprávnění	Oprávnění přidělovaná uživatelům a správcům bude možné definovat a přidělovat pro jednotlivé části systému (identity, referenční objekty, notifikací, synchronizací, konfigurace systému, reporty, workflow, webové služby atd.). U jednotlivých částí bude možnost definovat akce, které může uživatel s přidělenými oprávnění v konkrétní části IDM provádět.		
	Oprávnění k atributům	Pro identity a referenčních objektů bude možná definovat oprávnění k jejich atributům včetně možností zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti nastavení/vyplnění atributu, pořadí zobrazení atributů.		
	Kontextový výběr	Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, pracovních pozic, systematizovaných míst dostupných pro identity z dané organizační jednotky.		
	Správa licencí	IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytvářeni víceúrovňových schvalovacích workflow.		
	Časová omezení	IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.		

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	Vícenásobné vazby	Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.		
	Přehled rolí	Možnost zobrazení přidělených rolí k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných na skupinu a delegovaných role.		
	Přehled dědičností	IDM umožní evidenci a přehledné souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda má nějakou roli od někoho delegovánu.		
	Skupiny	IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.		
	Zastupitelnost	IDM bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta, …) svoje role, nebo jejich část na jiné pověřené osoby, a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce.		
	Delegování oprávnění	Možnost delegování administrátorských práv.		
	Správa osobních údajů	IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací.		
	Osobní údaje	IDM bude obsahovat evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům.		
	Osobní údaje - automatizace	IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů.		
	Obnovení hesla	IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).		
	Žádosti	IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení.		
	Externí subjekty	IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin.		
	Kontextový výběr	Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.		
	Individualizace	IDM umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně.		
	Workflow	Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným - Možnost sledování stavu svých požadavků uživateli		

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
		- E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění - Podpora vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Správce IDM může pracovat se všemi úlohami - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů		
	Workflow - sledování	Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude ve obvyklém formátu pro zobrazní workflow např. aktivity diagram, BPMN nebo Archimate		
	Upozornění	IDM zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, pracovní pozice / funkce, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu.		
	Včasná upozornění	Upozornění na vypršení časových termínů musí být možno zasílat v předstihu. Velikost předstihu (např. 10 dnů) musí být možno konfigurovat pro každý typ upozornění samostatně.		
	Šablony upozornění	Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.		
	Kontext upozornění	Pro zasílání jednotlivých typů upozornění bude možno konfigurovat kontext, resp. podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Příklad: notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd.		
	Logování	Veškeré změny vyvolané požadavky uživatelů a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.		
	Důvěryhodnost logování	Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.		
	Provozní stav	Kumulovaný online přehled o aktuálním stavu hlavních částí systému a případných chybách - min. chyby běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu workflow.		
	Auditní report	IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených		

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
		na IDM, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.		
	Auditní report - výběr	Identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.		
	Reporty uživatelů	Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru.		
	Reporty - zasílání	Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel.		
	Reporty - historie	Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.		
	Reporty - porovnání	Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu.		
	Webové služby (WS)	IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.		
	Standardy WS	Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.		
	Bezpečnost WS	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.		
	Logování WS	Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu		
	Služby rozhraní WS	Rozhraní bude poskytovat minimálně následující služby: - Získání organizační struktury - Získání hierarchie systematizovaných míst - Získání seznamu identit - Získání nadřízené osoby pro daného zaměstnance - Získání seznamu funkcí / rolí - Získání seznamu uživatelů dané aplikace - Získání seznamu pracovních pozic / funkcí přiřazených dané aplikaci - Zápis seznamu funkcí do IDM - Zápis certifikátů do IDM - Zápis a změna identit		
	Synchronizace	Ruční i automatické spuštění synchronizací s propojenými systémy.		
	Synchronizace - simulace	Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.		
	Simulace - průběh	Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.		
	Synchronizace - režimy	Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace. - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě		

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
		pouze vybranou identitu. - Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému. - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala.		
	Synchronizace - správa	Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu.		
	Obecné konektory	Vestavěné obecné konektory pro správu identit v napojených systémech: - konektor pro spouštění CMD příkazů - konektor pro práci s CSV soubory - konektor pro práci s databází Microsoft SQL - konektor pro napojení na SOAP a REST webové služby - konektor pro napojení na LDAP server s podporou LDAP v3		
	Speciální konektory	IDM bude obsahovat konektor umožňující správu virtuálních aplikací. Požadavky na správu identit ve virtuálních aplikacích bude IDM předávat e-mailem správcům odpovídajících reálných aplikací. Správci potvrdí splnění požadavku zpět do IDM. Uvedeným systémem budou řízeny identity v aplikacích, které nelze nebo není ekonomicky efektivní integrovat s IDM pomocí obecných nebo aplikačních konektorů.		
	Aplikační konektory	IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. Nově dodávaným systémům a stávajícím systémům Microsoft bude IDM vytvářet a spravovat uživatelské účty a jejich oprávnění včetně provádění souvisejících operací potřebných pro automatizaci správy identit v daném systému (např. vytváření mailových schránek, úpravy metadat apod.): 1. Správa identit v systémech, které jsou součástí dodávky v rámci předmětu plnění: - nabízený nástroj řízení přístupu do sítě podle standardu IEEE 802.1X - nabízený nástroj pro správu a řízení oprávnění privilegovaných účtů - nabízený nástroj pro správu identifikačních prostředků 2. Správa identit ve stávajících systémech Microsoft: - Microsoft Active Directory - Microsoft Exchange Stávajícím systémům zadavatele bude IDM vytvářet a spravovat uživatelské účty. Dále bude spravovat oprávnění uživatelských účtů v systémech v rozsahu, který umožní a zajistí výrobce či uchazeč daného systému provozovaného u zadavatele. Zadavatel		

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
		zajistí potřebnou součinnost výrobce či uchazeče stávajícího systému. V případě, že napojení na stávající systém, nebude možné v předpokládaném rozsahu, bude tento systém do IDM integrován dle technických možností. Konkrétní rozsah napojení stávajících systémů bude stanoven v rámci předimplementační analýzy 3. Správa identit ve stávajících systémech zadavatele: - IS ZOS (výrobce Per4mance s.r.o.) - Elektronická karta pacienta (EKP) a Mobilní zadávání dat (MZD) (výrobce European Medical Distribution s.r.o) - Fleetware (výrobce RADIUM s.r.o.) - ReDAT (výrobce RETIA, a.s.) - NidlWare (výrobce Pavel Nídl) - AUTOPLAN (výrobce Krob Software s.r.o.) - ServiceDesk, Asset Management (výrobce Alvao s.r.o.)		
	Zdrojový systém	IDM bude napojeno na personální systém Avensio (Alfa software). Z personálního systému budou načítány údaje o organizační struktuře, pracovních místech a funkcích, osobách a tyto údaje budou pro IDM sloužit jako zdrojové		
	Záruka	Min. 60 měsíců včetně nároku na nové a opravné verze		
Ověřovací systém - dispečink	Obecné požadavky	Platforma pro zajištění služeb vícefaktorového a jednotného (SSO - single sign-on) ověřování		
	Klientské systémy	Podpora desktopových a serverových Windows OS (verze 7/2008 a vyšší) a Linuxu		
	Vysoká dostupnost	Vysoce dostupná architektura z minimálně 2 automaticky zastupitelných prvků (cluster apod.) s jednotnou správou celého řešení		
	Virtualizace	Podpora provozu ve virtuálním prostředí nabízené serverové virtualizace		
	Bezpečnost	Ověřování administrátorských účtů vůči Active Directory		
	Adresářové služby	Podpora běžných adresářových služeb - Active Directory, LDAP		
	Bezpečná komunikace	Komunikace mezi jednotlivými komponenty řešení (klient, server, adresářová služba apod.) je šifrována (SSL či kompatibilní)		
	Autentizace	Zajištění ověření uživatele pro přihlášení k pracovní stanici (PC nebo tenký klient) s využitím více faktorů		
	Autentizační metody	Podpora autentizačních předmětů (kontaktní čipové karty, bezkontaktní karty, USB a bezkontaktní tokeny), biometrických prvků (otisk prstu), kombinace jméno/heslo (s vazbou i bez vazby na Active Directory), PINu a jejich vzájemných kombinací.		
	Dynamické ověřování	Podpora konfigurace podmínek pro využití vícefaktorového ověřování - např. dvoufaktorové ověřování povinné jen při prvním přihlášení v daném dni (pro další přihlášení postačí jeden faktor) apod.		
	Virtualizované aplikace a desktopy	"Bezešvá" integrace přihlašovacího procesu bez nutnosti opakovaně zadávat přihlašovací údaje a potvrzovat připojovací dialogy s nejběžnějšími produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix XenApp/XenDesktop)		
	Tencí klienti	Podpora náhrady běžného uživatelského rozhraní tenkého klienta přihlašovací obrazovkou pro vícefaktorové ověřování		
	Scénáře	Podporované scénáře použití "Koncová stanice v roli kiosku", "Rychlé střídání uživatelů u koncové stanice", "Uživatel přecházející mezi koncovými stanicemi". Koncovou stanicí může být tenký klient i běžný počítač s OS Windows/Linux.		

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	Rychlé přihlášení	Podpora rychlého přihlášení, resp. přehlášení uživatele včetně přenesení otevřeného pracovního prostředí (viz. Scénáře) při použití bezkontaktních identifikačních prostředků.		
	Obecné požadavky	Podpora jednotného (SSO) automatického přihlášení uživatele do libovolných desktopových aplikací včetně jejich automatického spuštění pro přihlášení do operačního systému.		
	Podporované aplikace	Podpora SSO do různých typů aplikací - Windows aplikace, webové aplikace včetně Java aplikací, terminálové aplikace používající znakové rozhraní apod. Funkčnost nesmí vyžadovat úpravu aplikací.		
	Bezpečnost	Přihlašovací údaje do aplikací musí být dostupné jen příslušnému uživateli. Přihlašovací údaje musí být ukládány v ověřovací platformě a být centrálně dostupné na libovolném koncovém zařízení (počítač, tenký klient) v síti.		
	Profily	Intuitivní podpora vytváření a správu předpisů (profilů) pro jednotlivé aplikace (bez psaní kódu, používání řádkových příkazů apod.). Vytvořené předpisy (profily) aplikací musí být možné přidělovat uživatelům na základě členství v Active Directory skupinách.		
	Licence	Min. pro 30 uživatelů		
	Záruka	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze		
Ověřovací systém	Základní popis	Systém pro autentizaci uživatele identifikačním prostředkem vůči adresářové služeb včetně nástrojů pro správu osobního identifikačního prostředku		
	Rozhraní	Grafické rozhraní v českém jazyce		
	Obnova certifikátů	Automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů a vyvolání průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik		
	Autentizace	Autentizace uživatele ve operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem (Microsoft)		
	Správa	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK, ..)		
	Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti		
	Předávání veřejných doménových klíčů	Automatizované předávání veřejných klíčů doménových certifikátů do stávajícího systému Microsoft Active Directory		
	Licence	pro 250 uživatelů (včetně externích)		
	Záruka	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze		
Identifikační karty hybridní 300 ks	Základní popis	Hybridní identifikační karta s kontaktní částí SmartCard a bezkontaktní částí typu Mifare DESFire EV1 4K 13,56 MHz)		
	Veřejné certifikáty	Karta musí umožnit ukládání a používání vlastních doménových certifikátů a certifikátů veřejných certifikačních autorit – např. I. CA, Postsignum apod.		
	Identity	Karta musí umožnit ukládání více identit		
	Kvalifikovaný prostředek	Karta musí být možno využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku)		
	Softwarová podpora	Součástí dodávky bude software pro zpřístupnění jejich rozhraní v operačním systému včetně rozšířených funkcionalit, tzv. Middleware		
	Záruka	24 měsíců		

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
Identifikační tokeny 140 ks	Základní popis	Identifikační USB s čipovou částí (SmartCard)		
	Veřejné certifikáty	Token musí umožnit ukládání a používání vlastních certifikátů a certifikátů veřejných certifikačních autorit – např. I. CA, Postsignum apod.		
	Identity	Token musí umožnit ukládání více identit		
	Kvalifikovaný prostředek	Token musí být možno využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku)		
	Softwarová podpora	Součástí dodávky bude software pro zpřístupnění jejich rozhraní v operačním systému včetně rozšířených funkcionalit, tzv. Middleware		
	Záruka	24 měsíců		
Čtečky bezkontaktních karet 10 ks	Provedení	externí, připojitelná přes USB		
	Standardy	podpora obvyklých standardů 13,56 MHz - MIFARE (Classic, Ultralight, Ultralight C / Plus), DESFire, DESFire EV1, DESFire EV2, iCLASS. Čtení i zápis		
	Napájení	USB		
	Kompatibilita	Windows 7 a vyšší (32 a 64 bit), Linux, MacOS		
	Kompatibilita	s nabízenými tenkými klienty a Ověřovacím systémem - dispečink		
	Záruka	24 měsíců		
Čtečka hybridních karet 120 ks	Provedení	čtečka nabízených čipových (SmartCard) karet, připojitelná přes USB		
	Provedení	kvalitní provedení, výrobcem deklarovaná trvanlivost min. 100 000 zasunutí/vysunutí karty		
	Kompatibilita	Windows 7 a vyšší (32 a 64 bit), Linux, MacOS		
	Kompatibilita	s nabízenými počítači a Ověřovacím systémem		
	Záruka	24 měsíců		

(7) Požadavky na zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS

Komodita K.3 - Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém řízení a monitorování privilegovaných účtů	Základní popis	Proxy brána určená pro správu a monitoring privilegovaných přístupů		
	Záznam relací	Zaznamenávání uživatelských relací včetně vytváření logů		
	Logování relací	Nepozměnitelné podklady pro audit a analytické reporty uživatelského chování		
	Metadata	Ukládání metadat záznamů pro snadnou orientaci při prohlížení a vyhledávání (min. stisky kláves, kliknutí)		
	Architektura	Samostatná virtuální aplliance, bezagentové řešení (bez nutnosti instalace agentů na monitorované systémy)		
	Autentizace	LDAP, Microsoft Active Directory, Radius, TACACS+, Kerberos, X.509, OTP, Web SSO, podpora vícefaktorové autentizace (MFA)		
	Autorizace	Integrované pokročilé workflow pro autorizaci (povolené časy a trvání relace, white/black listy, rozpoznání činnosti v RDP relaci, parametry relace apod.)		
	Bezpečné přihlášení	Uživatel privilegovaného účtu se přihlašuje pouze k proxy. Přihlášení k cílovému systému zajišťuje proxy - uživatel nezná přístupové údaje k cílovému systému		

Komodita K.3 - Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS				
	Přístupové protokoly a aplikace	Proxy umožňuje zprostředkované (bez znalosti hesla cílového systému) přihlášení k cílovým systémům min. RDP, SSH, Microsoft SQL management, webová GUI		
	Notifikace	Zasílání notifikací o zahájení definované relace		
	Integrace	Integrace s nabízeným systémem pro správu identit (IDM), nabízeným systém pro správu logů a obecnými tiketovacími systémy třetích stran (žádost o schválení přístupu, přístup na základě existujícího tiketu)		
	Řízení v realném čase	Monitorování relací v raálném čase a jejich okamžité ukončení v případě potřeby		
	Vysoká dostupnost	Integrovaná podpora high-availability clusterů: Active/Passive nebo Active/Active		
	Rozšiřitelnost	Podpora modulů (plug-in) pro integraci s dalšími technologiemi / technologickými partnery		
	Rozhraní	Webové rozhraní pro přístup uživatelů I konfiguraci, bezpečná publikace do internetu (šifrovaná komunikace)		
	Zabezpečení přístupových údajů	Integrované bezpečné (šifrované) úložiště přístupových údajů k cílovým systémům		
	Aktivní bezpečnost	Upozornění a automatické ukončení podezřelé činnosti nebo neoprávněných pokusů o přístup		
	SIEM	Podpora odesílání záznamů a událostí do systému SIEM (Security Information and Event Management)		
	Logy	Nesmazatelnost logů po dobu minimálně 30 dní. Uložení auditních záznamů v zašifrované podobě s přístupem pouze oprávněných uživatelů		
	Bezpečnostní standardy	Podpora zajištění shody se standardy HIPAA, GDPR, PCI, SOX		
	Zálohování	Šifrování záloh, přístup k zálohovaným datům výhradně pomocí zabezpečených Disaster Recovery klíčů.		
	Licence	Licence pro monitorování a záznam min. 10 současně pracujících (privilegovaných) uživatelů, min. 100 cílových systémů.		
	Záruka	min. 60 měsíců včetně nároku na podporu výrobce a aktualizace systému včetně nových hlavních verzí		

(8) Požadavky na zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

Komodita K.4 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém pro správu logů	Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware		
	Architektura	Integrovaná aplliance (hw se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), samostatně funkční nezávisle na infrastruktuře zadavatele		
	Provedení	Určené pro montáž do stávajícího serverového datového rozvaděče 19", hloubka max 900 mm, včetně výsuvných kolejnic a ramene pro vedení kabelů.		
	Ovládání	Grafická webová konzole pro administrátory I operátory, umožňuje kompletní správu systému včetně úvodního nastavení.		

Komodita K.4 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
	Autentizace	Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze.		
	Uživatelské role	Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému.		
	Sběr dat (logů)	Bezagentový sběr logů s výjimkou systémů Windows		
	Windows agent	Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Event logů (včetně rozšířených) , šifrovaná komunikace, buffer pro případ ztráty komunikace, překlad kódů na text (např. Logon type 2 => "Interactive" apod.) a textový popis události shodný s Windows Event Viewerem		
	Protokoly	Příjem a zpracování logy, událostí a další strojově generovaných data minimálně protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně).		
	Formáty logů	Mini. RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog		
	Třídění logů	Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv.		
	Zpracování logů	Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy		
	Ochrana logů	Zamezení mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci.		
	Vizualizace logů	Grafická vizualizace logů, událostí a strojových dat (grafy událostí). Dynamická vizualizace - změnou volby (např. filtru) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Integrované podpora zobrazení TOP X událostí za zvolené časové období.		
	Pracovní plochy	Předpřipravené pohledy (dashboardy) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem. Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání		
	Zajištění logů	Ochrana proti ztrátě logů při přetížení systému. Ukládání nezpracovaných logů/událostí do vyrovnávací paměti o kapacitě min 25 GB, notifikace správce systému při riziku zaplnění vyrovnávací paměti		
	Doplňování logů	Integrovaná podpora doplňování logů dalšími údaji - např. umístění zařízení, typ zařízení, kritičnost zařízení apod. - k jednotlivým zdrojům dat, aplikacím, zařízením, IP rozsahů apod.		
	Archivace	Integrovaná archivace logů včetně zajištění integrity archivů, obnova		
	Rozpoznávání IP, MAC	Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce podle MAC adresy		
	Časová razítka	Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, slouží jako výchozí časový údaj pro systém		
	Vyhledávání	Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalosti (např. SQL dotazů apod.) napříč všemi typy data a zařízení.		
	Rychlé vyhledávání	Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování)		
	Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran		

Komodita K.4 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
	Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (např. SQL dotazů apod.). Průběžná aktualizace přednastavených reportů výrobcem.		
	Integrace	Integrované REST API rozhraní pro napojené systémy, musí umožnit autorizovaný přístup ke strukturované databázi logů.		
	Parsery	Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění - okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb		
	Konektory	Konektory (specifické parsery) pro stávající technologie - min. Active Directory, Vmware, Windows (vč. DNS, DHCP), Exchange, MS SQL, Fortinet, HPE/Aruba, Dell servery, Synology, Linux, Apache, nabízený Systém pro analýzu síťového provozu		
	Alerty, notifikace	Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Odesílání alertů min SMTP, Syslog, TCP.		
	Výkon	Min. 2000 EPS (events per second), krátkodobá (min. 10 min) přetižitelnost systému 200%		
	Kapacita	Využitelná diskové kapacita pro ukládání data min. 12 TB, disky musí být chráněny min. RAID 5		
	Řízení diskového systému	Hardwarový řadič RAID se zálohovanou vyrovnávací pamětí (zápis I čtení) o kapacitě min 2 GB		
	Úložiště logů	Logy musí být ukládány do databáze (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat.		
	Napájení	Systém musí mít redundantní napájení (min. 2 nezávislé zdroje)		
	LAN konektivita	Min. 2x LAN 1 Gb + 1x 1Gb nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent.		
	Aktualizace	Integrovaná aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade		
	Zálohování	Integrované zálohování a obnova konfigurace		
	Škálovatelnost	Systém lze propojit s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, výkonu (včetně vyhledávání) a dostupnosti. Navenek se propojené systémy chovají jako jeden.		
	Dokumentace	Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce		
	Záruka	Min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace		

(9) Požadavky na nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS

Komodita K.5 - Zavedení nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**

Komodita K.5 - Zavedení nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS				
Systém pro analýzu síťového provozu	Základní funkce	Monitorování síťové aktivity v reálném čase, identifikace potenciální kybernetické hrozby, bezpečnostního rizika a anomálního chování a tvorba upozornění o jejich výskytu v reálném časem		
	Architektura	Integrovaná aplliance (hw se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), provozovaný v prostředí zadavatele. Samostatně funkční nezávisle na infrastruktuře zadavatele či dalších (např. cloudových) službách.		
	Provedení	Určené pro montáž do stávajícího serverového datového rozvaděče 19", hloubka max 900 mm, včetně výsuvných kolejnic a ramene pro vedení kabelů.		
	Ovládání	Grafická webová konzole (HTTPS) pro administrátory I operátory, pro správu a používání systému. SSH pro CLI - automatizace, monitorování.		
	Viditelnost	Systém zajišťuje detailní viditelnost do síťové komunikace s "drill down" prokliky na veškerá uložená data.		
	Sběr dat	Systém bude získávat data na základě zrcadleného síťového provozu bez potřeby instalace agentů na zařízení v síti.		
	Zrcadlení komunikace	Podpora SPAN portů a síťových TAPů pro získávání dat zrcadlené komunikace		
	Pasivní sběr	Systém bude zcela pasivní vůči síťovém provozu, monitorovaný provoz přes systém nebude procházet a systém jej nebude nijak ovlivňovat.		
	Netflow protokoly	Systém umožní analyzovat síť na základě zpracování statistických protokolů typu NetFlow v5, NetFlow v9, IPFIX, NetStream a případně dalších ekvivalentních.		
	Záznam provozu	Zaznamenávání síťového provozu, minimálně základních parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6.		
	Integrace	Integrace s nabízeným Systémem pro správu, minimálně v úrovni syslog		
	Kontextuální informace	Získávání, vizualizace a integrace kontextuálních informací v jednotném grafickém rozhraní: - Hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS provozu a Active Directory - IP geolokace		
	Monitorování zařízení	Identifikace zařízení v síti (koncová zařízení, servery, IoT, síťové prvky), rozpoznání změn v síti a notifikace výskytu nového zařízení (obecně assetu)		
	Analýza	Integrovaný modul pro detailní analýzu sítě - vytváření dlouhodobých grafů a přehledů o komunikaci na síti s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (http, IMAP, SSH), SSL a DNS provozu, VoIP statistik, SMB/CIFS, DHCP a e-mail provozu.		
	Vizualizace, vyhledávání	Zobrazení provozu a jeho hloubková analýza - okamžité vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez speciálního dotazovacího jazyka a bez hlubokých znalostí konkrétních komunikačních protokolů		
	HTTP komunikace	Podpora pro příjem a analýzu HTTP provozu – včetně položek typu URL a hostname		
	Detekce anomálií	Integrované samostatné učení na základě matematických metod (např. strojové účení) pro analýzu síťové aktivity, vytváření a v automatická průběžná modifikace modelů chování na základě běžného chování jednotlivých zařízení a na nich provozovaných		

Komodita K.5 - Zavedení nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS				
		služeb. Schopnost identifikace nestandardního síťové chování na základě modelu chování daného zařízení a jeho služeb.		
	Detekce hrozeb	Schopnost detekce neznámých hrozeb, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Minimálně identifikace příznaků potenciálně škodlivého chování: - průzkumné aktivity v síti, - potenciální úniky dat, - detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, - detekce příznaků těžení kryptoměn, - útoky hrubou silou a enumerace dat		
	Behaviorální analýza	Detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů). Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti.		
	False-positive události	Integrovaná podpora identifikace neplatných událostí pomocí mechanismu false-positives, potlačení identifikovaných událostí při příštím výskytu		
	Autentizace	Podpora autentizace vůči LDAP, včetně podpory RBAC (přiřazení úrovně oprávnění na základě členství uživatele v konkrétní LDAP skupině).		
	Reporting	Tvorba dlouhodobých grafů a přehledů s různými typy pohledů dle kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDC, ICMP, ostatní) nebo protokolu (http, IMAP, SSH). Generování statistik a podrobných výpisů ve volitelných časových intervalech. Tvorba tzv Top N statistik podle různých kritérií (počet přenesených bytů, paketů, toků atd.) pro výpis nejaktivnějších či anomálně komunikující assety.		
	Automatizace reportingu	Vytváření automatizovaných manažerských reportů včetně možnosti exportu do PDF a CSV (nebo obdobného strojově čitelného) formátu. Automatické zasílání reportů emailem, předpřipravené reporty v českém a anglickém jazyce.		
	Alerty, notifikace	Notifikace na základě překročení prahových hodnot definovaných při implementaci či v průběhu provozu. Systém musí být schopen upozorňovat uživatele prostřednictvím e-mailu o: - všech identifikovaných událostech, - událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. Logování notifikací.		
	Výkon	min. 0,2 Gb/s trvalý síťový provoz, min. 200 Netflow/sec		
	Kapacita	úložná kapacita SSD s ochranou min. RAID 1 pro min. 30 denní historii při plném výkonu		
	Konektivita	Min. 1x LAN 1 Gb + 1x 1Gb nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent.		
	Záruka a podpora	Min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace		

(10) Požadavky na nástroje pro zajišťování úrovně dostupnosti informací

Komodita K.6 - Nástroje pro zajišťování úrovně dostupnosti informací				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Rozšíření stávajících serverů	RAM	18x modul 32 GB RAM 2Rx4 DDR4 RDIM 2666 MHz 6x modul 32 GB RAM 2Rx4 DDR4 RDIM 2933 MHz		
	HBA	3x HBA SAS 12Gb včetně kabeláže, kompatibilita s nabízenou diskovou virtualizací.		
	SSD	6x 960 GB SSD SATA Mixed Use 6Gbps 512e, 2.5" Hot-Plug 12x 3.84TB SSD SATA Read Intensive 6Gbps 512e, 2.5in" Hot-Plug 3x PCIe FH karta s integrovaným řadičem RAID1, každá osazen dvojicí M.2 240 GB SSD SATA, podpora bootování hypervizoru		
	Záruka	Nabízené komponenty převezmou záruku serverů a budou součástí konfigurace vedené v systému podpory výrobce		
Rozšíření NAS	Diskové police	Disková police pro rozšíření kapacity stávajících NAS (DS412+ nebo DS916+) určené pro ukládání záloh		
	HDD	Celková disková kapacita min. 40 TB RAW / 32 TB RAID5 sestavená z HDD SATA (256 MB cache), výrobcem určené pro NAS nebo servery		
	Záruka	36 měsíců		
Licence SDS	Provedení	Licence software vysoce dostupného virtualizovaného softwarově definovaného diskového úložiště pro stávají 3 virtualizační servery		
	Replikace	Software musí umožnit minimálně synchronní replikace dat (zrcadlení, RAID1) mezi uzly SDS (virtualizačními servery)		
	Vysoká dostupnost	Automatické překlenutí výpadku jednoho prvků systému – jednoho serveru či jeho komponenty (např. jednoho disku). Včetně podpory zotavení a obnovení		
	Podpora virtualizace	Software bude provozován na úrovni hypervizorů (bude do nich zaintegrován) nabízené serverové virtualizace		
	Jednotná správa	Správa SDS bude zaintegrována do nástroje pro správu serverové virtualizace pro jednotnou správu		
	Vyrovnávací paměť	Integrovaná podpora vyrovnávací paměti pro čtení i zápis s využitím flash médií (SSD, NVMe disků apod.)		
	Konzistence dat	Integrovaná kontrola dat kontrolními součty (checksum)		
	Škálovatelnost výkonu	Podpora přidání dalších uzlů SDS s rozprostřením stávajících dat za provozu a podpora RAID mezi uzly SDS. Podpora navyšování kapacity přidáním disků v rámci uzlu (licence není kapacitně omezena).		
	Škálovatelnost funkcí	Změnou typu licence lze aktivovat (bez potřeby instalace) pokročilé funkce – min. deduplikace, šifrování uložených dat apod.		
	Serverová virtualizace - integrace	Integrovaná podpora technologií stávající serverové virtualizace – replikace virtuálních strojů, podpora virtuálních distribuovaných přepínačů, správa politik úložišť		
	Řízení výkonu	Integrovaná podpora limitace IOPS (vstupně/výstupních operací za sekundu) virtuálních serverů		
	iSCSI	Integrovaná podpora publikace kapacity SDS prostřednictvím protokolu iSCSI (tzv. ISCI target)		
	Záruka	Podpora výrobce, včetně nároku na nové verze po dobu min 60 měsíců		

Komodita K.6 - Nástroje pro zajišťování úrovně dostupnosti informací				
Bezpečné úložiště	Provedení	umístitelné do racku, včetně montážního materiálu		
	CPU	Minimálně 1x procesor jádrový. Výkon serveru dle http://www.spec.org: SPECrate®2017_int_base min. 29 bodů SPECrate®2017_fp_base min. 38 bodů		
	RAM	32 GB, min. 3200 MT/s		
	Úložiště firmware	Min. 2x SSD 240 GB, read intensive, samostatný HW řadič RAID1		
	Úložiště data	Min. 7x 8 TB, NLSAS 12Gb, 7 200 ot/min		
	Rozšiřitelnost	Min. 1 volná pozice HDD pro rozšíření kapacity, aktivní, připojená k RAID/PCIe		
	RAID hardware	SAS 12Gb, RAID 1,5,6, zálohovaná zapisovací cache min. 8 GB		
	LAN	2x 1GbE RJ-45 s podporou virtualizace - VMware NetQueue, Microsoft VMQ. 10Gb porty s podporů NPAR (Network Partitioning) 1x 1Gb RJ-45 - samostatný port pro vzdálený management		
	USB	min. 2 USB konektory - min. 1x verze 3.0, min. min .1x na čelním panelu s podporou bootování		
	Management	Servisní modul s možnosti samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média. Vyhrazený LAN port, podpora http/s, ssh, SNMP, syslog. Okamžité a historické hodnoty teplot a napájení. Podpora vícefaktorového ověřování (autentizace)		
	Napájení	2x napájecí zdroj min. 600 W, redundance, min. Platinum specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80_Plus		
	Souborový systém	XFS		
	Protokoly	SMB/CIFS, SNMP, http/s a ssh (management)		
	Výkon	zápis min. 3 TB / hod		
	Ochrana dat	min RAID5, automatická relokací vadných datových bloků		
	Retence dat	programově nastavitelné retenční lhůty na uložený objekt (např. soubor), po dobu retence nelze objekt modifikovat		
	Redundance	redundantní rotační díly a napájecí zdroje		
	Ochrana proti přepisu dat	režim WORM (Write Once - Read many times Memory)		
	Kompatibilita	Kompatibilita se stávajícím zálohovacím systémem, podpora ukládání záloh, řízení jejich historie a řízení retenčních lhůt		
	Audit	Integrovaný logovací systém - systémové událostí, provádění příkazy, přihlášení/odhlášení, datové operace		
	Záruka	60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze software a firmware		
Dispečerské pracoviště 5x	**Terminál**			
	Provedení	Pasivní provedení bez rotačních dílů (HDD, ventilátor apod.), možnost umístění "nastojato" i "naležato"		
	Rozměry	max. 25 x 25 x 6 cm		
	Porty	min. 3x USB 3, z toho min 1x USB-C a audio (sluchátka, mikrofon) na čelním panelu min. 4x USB (min. 2x USB 3), audio (sluchátka, mikrofon) na zadním panelu min. 3x Display port min. 1.2, LAN RJ-45 1 Gb s podporou WoL		

Komodita K.6 - Nástroje pro zajišťování úrovně dostupnosti informací				
	Výkon	64 bit CPU, výkon min. 3800 bodů dle https://www.cpubenchmark.net HD grafický čip s podporou 4K/60 Hz současně na všech DP RAM min. 8 GB		
	Grafika	podpora vícemonitorového provozu, rozlišení min. 4K/UHD (3840 x 2160 @ 60Hz)		
	Kompatibilita	Microsoft RDP; Remote FX; Citrix ICA, Citrix HDX, VMware PCoIP		
	Bezpečnost	Plná podpora 802.1X		
	Operační systém	Windows 10 IoT Enterprise 64-bit a vyšší		
	VESA	Podpora standardu VESA pro montáž na monitor, zeď apod.		
	Spotřeba	do 10 W		
	Periferie	včetně klávesnice a myši		
	Záruka	36 měsíců včetně nároku na nové verze firmware		
	Monitor 3x			
	Provedení	24" (min. 23,8" viditelná plocha), tenký rámeček, matný - antireflexní povrch, design shodný s multimediálním monitorem		
	Panel	technologie IPS, podsvícení LED, odezva do 5 ms		
	Rozlišení	FullHD, min. 1920 x 1080		
	Porty - video	min. 1x Display Port 1.2, 1x HDMI 1.4, oba s podporu HDCP, včetně Display Port kabelu pro připojení k počítači		
	Porty - data	min. 5x USB 3 (1x IN, 4x OUT) včetně kabelu pro připojení k počítači, OUT porty snadno dostupné na hraně nebo čelním panelu monitoru		
	Ergonomie	Integrovaná technologie pro omezení vlivu modrého světla		
	Nastavení polohy	Výškově stavitelný, otočný kolem svislé osy, nastavitelný sklon, otočný na výšku (PIVOT)		
	Záruka	min. 36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace		
	Zvuková lišta 1x			
	Provedení	Originální zvuková lišta k nabízeným 24" monitorům s magnetickým upevněním, bez omezení polohovacích možností monitoru		
	Porty	USB pro napájení I zvuk		
	Výkon	min 3 W		
	Záruka	min 36 měsíců		
	Monitor dotykový 1x			
	Provedení	17" LCD dotykový monitor, ovládání prstem i předmětem		
	Dotyková vrstva	kapacitní nebo resistivní (min. 5 vodičová) nebo jiná srovnatelná technologie umožňující dotykové ovládání displeje		
	Rozlišení	min. 1280 x 1024		
	Odezva	max. 5 ms		
	Porty - video	min. 1x Display Port 1.2, 1x HDMI 1.4, včetně Display Port kabelu pro připojení k počítači		
	Porty - data	USB pro připojení dotykové vrstvy		
	Ergonomie	široký pozorovací úhel, min 150 stupňů vertikálně i horizontálně		
	Audio	2 integrované reproduktoru, audio jack		
	Kompatibilita	ovladače nebo integrovaná podpora Windows 7/8,10/11, Linux, Mac		
	Záruka	min. 36 měsíců poskytovaná výrobcem		

Komodita K.6 - Nástroje pro zajišťování úrovně dostupnosti informací				
	Řídící PC dotykového monitoru			
	Provedení	Pasivní provedení bez rotačních dílů (HDD, ventilátor apod.)		
	Rozměry	max. 20 x 20 x 6 cm		
	Porty	min. 2x USB 3, z toho min 1x USB-C a audio (sluchátka, mikrofon) na čelním panelu min. 2x USB 3, z toho min 1x USB-C na zadním panelu min. 1x Display port min. 1.2 a/nebo HDMI 1.4, LAN RJ-45 1 Gb s podporou WoL		
	Bezdrátová konektivita	Wi-Fi min 801.11an, Bluetooth 5		
	CPU	64 bit CPU, výkon min. 3000 bodů dle https://www.cpubenchmark.net		
	Grafika	podpora vícemonitorového provozu, rozlišení min. 4K/UHD (3840x2160/60Hz)		
	Paměť	min. 4 GB		
	Úložiště	min. 128 GB NVMe SSD		
	Bezpečnost	Plná podpora 802.1X		
	Operační systém	Windows 10Pro a vyšší		
	Spotřeba	do 15 W		
	Periferie	včetně klávesnice a myši		
	Záruka	36 měsíců včetně nároku na nové verze firmware		
Operátorské pracoviště výjezdového stanoviště 13x	**Monitor multimediální, videokonferenční**			
	Provedení	27", tenký rámeček, matný - antireflexní povrch		
	Panel	technologie IPS, podsvícení LED, odezva do 5 ms		
	Rozlišení	QHD, min. 2 560 × 1 440		
	Porty - video	min. 1x Display Port 1.2, 1x HDMI 1.4, včetně Display Port kabelu pro připojení k počítači		
	Porty - audio	Audio výstup jack		
	Porty - data	min. 3x USB 3 (1x IN, 2x OUT), včetně kabelu pro připojení k počítači, OUT porty snadno dostupné na boku nebo čelním panelu monitoru, IN port typu USB-C s přenosem obrazu a zvuku, napájením min. 65 W I při vypnutém monitoru		
	Reproduktory	min. 2 integrované reproduktory, výkon min. 2x 5 W		
	Mikrofony	min. 2 integrované mikrofony, tlumení ruchů, MUTE tlačítko		
	Kamera	Integrovaná kamera min. 2Mpix, podpora Microsoft Hello, fyzické zakrytí pro bezpečnost (krytka, zasunutí apod.)		
	Ergonomie	Integrovaná technologie pro omezení vlivu modrého světla		
	Nastavení polohy	Výškově stavitelný, otočný kolem svislé osy, nastavitelný sklon, otočný na výšku (PIVOT)		
	Záruka	min. 36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace		
	Stolní počítač			
	Provedení	Stolní provedení, možnost umístění nastojato i naležato		
	Rozměry	formát SFF nebo menší		
	Porty	min. 4x USB, z toho min 2x USB 3 a audio (sluchátka, mikrofon) na čelním panelu min. 2x USB, z toho min 2x USB 3 na zadním panelu min. 1x Display port min. 1.2 a HDMI 1.4 LAN RJ-45 1 Gb s podporou WoL		
	Bezdrátová konektivita	Wi-Fi min 801.11ac, Bluetooth 5		
	CPU	64 bit CPU, výkon min. 19 500 bodů dle https://www.cpubenchmark.net		

Komodita K.6 - Nástroje pro zajišťování úrovně dostupnosti informací				
	Grafika	podpora vícemonitorového provozu, rozlišení min. 4K/UHD (3840x2160/60Hz)		
	Paměť	min. 16 GB		
	Úložiště	min. 512 GB NVMe SSD		
	DVD, SD	integrovaná optická mechanika DVD, čtečka SD karet		
	Bezpečnost	Plná podpora 802.1X		
	Operační systém	Windows 10 Pro a vyšší		
	Periferie	včetně klávesnice a myši		
	Záruka	min. 36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace		
Řídící software operačního střediska	Základní funkce	Software pro automatizace krizového scénáře typu "červené tlačítko" - převodu provozu aplikací operačního střediska do záložního operačního střediska (fail-over)		
	Požadavky	Automatizace rekonfigurace síťových služeb včetně směrování, adresních prostorů a jmenných služeb, blokace internetu v případě útoku, rekonfigurace datových zdrojů (SQL, Oracle), aktivace souvisejících virtuálních serverů a souvisejících operací		
	Ovládání	Proces spuštění scénáře musí být možno aktivovat z libovolné pracovní stanice po ověření oprávnění uživatele k požadované operaci. Součástí řešení musí být I zpětný převod provozu do primárního operačního střediska (fail-back)		
	Provedení	Provoz v prostředí stávající virtualizační platformy Vmware		

(11) Požadavky na vozidlové komunikační jednotky

Komodita K.7 - Vozidlové komunikační jednotky				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Komunikační jednotka 40x	Provedení	odolný tablet pro umístění do vozidla		
	Displej	Min 10", rozlišení min. 1920 x 1080, antireflexní (čitelný na slunci), podpora dotykového ovládání, ovládání v rukavicích, jas min. 1 000 nitů (cd/m2),		
	CPU	výkon CPU dle https://www.cpubenchmark.net min. 6200 bodů, nízká spotřeba, TDP do 35W		
	Video	výkon video/grafického procesoru dle https://www.videocardbenchmark.net min. 850 bodů		
	RAM	min. 16 GB		
	úložiště	min. 512 GB NVMe SSD		
	Bezdrátové připojení	WiFi 6, 802.11ax, 2.4 + 5 GHz Bluetooth min. 5.0 WWAN (LTE,3G)		
	Porty	min 1x USB 3 min 1x USB 3 Type-C s podporou Power Delivery		
	Kamery	čelní min. 2 Mpix s bezpečnostní krytkou zadní min. 8 Mpix		

Komodita K.7 - Vozidlové komunikační jednotky				
	Bezpečnost	integrovaný čip TPM 2.0 integrovaná kontaktní nebo bezkontaktní čtečka čipových karet (SmartCard)		
	Reproduktory	integrovaný reproduktor nebo audio in/out		
	Senzory	GPS		
	Napájení	interní baterie, náhradní baterie, napájecí adaptér		
	Software	Zabezpečený (hardened) operační systém s podporou Windows aplikací, potlačeným uživatelským prostředím (uživatel má k dispozici pouze definovanou aplikaci) a autentizací pomocí SmardCard. (Re)instalační image součástí dodávky.		
	Hmotnost	do 2000 g bez příslušenství		
	Odolnost	Ochrana proti vniknutí IEC 6052913: IP-65 (prachotěsné, chráněné proti tlakové vodě) Pracovní teplota prostředí min v rozmezí -25 °C až +60 °C Odolnost proti pádu za provozu na tvrdou podložku min. z výšky 90 cm		
	Záruka	min. 60 měsíců poskytovaná výrobcem s podporou a hlášením závad v režimu 24x7 v českém jazyce a opravou následující pracovní den u zákazníka (on-site)		
Sada příslušenství	Přídavná klávesnice 40x	Odnímatelná klávesnice s touchpadem a držákem/stojánkem tabletu, krytí IP-65		
	Popruh 5x	Otočný popruh pro bezpečné upevnění tabletu na paži a možností práce na výšku i na šířku		
	Pero 40x	Pero určené pro dotykový displej tabletu, pro ovládání aplikací a podepisování		
	Dokovací stanice s klávesnicí 35x	Automobilová dokovací stanice pro pevné a bezpečné uchycení tabletu včetně příslušenství. Napájení tabletu. Snadné vkládání a vyjímání tabletu. Umožní pevné přichycení klávesnice.		
	Dokovací stanice bez klávesnice 5x	Automobilová dokovací stanice pro pevné a bezpečné uchycení tabletu včetně příslušenství. Napájení tabletu. Snadné vkládání a vyjímání tabletu.		
	Záruka	Min. 24 měsíců		

(12) Požadavky na správu identifikačních prostředků

Komodita K.8 - Správa identifikačních prostředků				
Správa identifikačních prostředků	Obecné požadavky	Systém pro evidenci a správu životního cyklu identifikačních prostředků		
	Prostředky	Podpora kontaktních, bezkontaktních i hybridních identifikačních prostředků		
	Evidence	Systém umožní evidovat minimálně - typ prostředku (kontaktní, bezkontaktní, hybridní, …) - druh prostředku (uživatelský, administrační, operátorský, …) - stav prostředku (používaný, k recyklaci, skartovaný, …) - historii prostředku (datum zavedení do evidence, vydání uživateli, recyklace, …) - držitele prostředku (aktuálního držitele i všechny předchozí držitele) - data uložená v prostředku (certifikáty a další data, včetně historie dat)		
	Integrace	Napojení na Active Directory (zdroj dat o uživatelích, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty)		
	Uživatelské rozhraní	Webové rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory		
	Certifikáty	Správa certifikátů (doménových i kvalifikovaných) ve webovém prostředí systému: - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření a tisk protokolu o vystavení		

		- odvolání certifikátu - vydávání "v zastoupení" - např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance		
	Certifikační autorita	Systém musí umožnit použití jakékoliv certifikačních autority od kvalifikovaných poskytovatelů certifikačních služeb (https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx).		
	Operace	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů		
	Potisk	Integrované prostředí pro generování podkladů pro potisk identifikačních karet externím uchazečem i na vlastní tiskárně		
	Rozhraní	Integrované aktivní aplikační rozhraní (API) pro bezpečné (autorizované) poskytování veřejných informací o uložených prostředcích, certifikátech a kvalifikovaných elektronických pečetí pro systémy třetích stran včetně dokumentace.		
	Elektronická pečeť	Systém umožní poskytování elektronických pečetí pomocí čipové karty s kvalifikovaným certifikátem prostřednictvím otevřené webové služby – aplikačního rozhraní (viz. Rozhraní). Řízení oprávnění uživatelů požadujících pečetění musí probíhat min. vůči Active Directory. Součástí dodávky není provedení integrace s napojenými systémy využívajících kvalifikované pečeti.		
	Licence	pro 350 uživatelů (včetně externích)		
	Záruka	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze		

3.11. Požadavky na architekturu technického řešení

(1) Architektura komodit musí být navržena tak, aby vhodně využívala a doplňovala stávající systémy ZZS KVK.

(2) Propojení mezi lokalitami (operační středisko – výjezdová stanoviště) bude provedeno prostřednictvím stávajících internetových přípojek a VPN na bázi SD-WAN s využitím nabízených VPN routerů.

3.12. Požadavky na rozhraní

(1) Veškeré nabízené aktivní síťové prvky musí disponovat rozhraním SNMP min v2 pro management a vzdálenou správu.

3.13. Požadavky na kompatibilitu s ostatními systémy

(1) Veškeré softwarové komponenty nabízeného řešení budou provozovány ve virtuálním prostředí VMware vSphere a musí být pro běh v tomto prostředí výrobcem podporovány.

3.14. Požadavky na typy klientů

(1) Webová rozhraní nabízených systémů a zařízení být funkční v obvyklých internetových prohlížečích – min. Edge, Chrome, Safari v aktuálních verzích bez potřeby instalace speciálních doplňků či plug-in modulů.

3.15. Požadavky na bezpečnost informací

(1) Veškeré nástroje pro správu musí umožňovat správu interních účtů (min. jméno a heslo) a/nebo napojení na LDAP/Active Directory.

(2) Veškeré nástroje pro správu musí umožňovat definici s minimálně 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa)

(3) Veškeré nástroje pro správu musí komunikovat se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní hardware) musí být použita šifrovaná komunikace (např. HTTPS).

(4) Bezpečnost vnější komunikace publikovaných webových rozhraní aplikací a systémů bude zajištěna použitím tzv. „hvězdičkového“ (wildcard) certifikátu veřejné certifikační autority, tj. takové autority, jejíž kořenový certifikát je součástí běžných operačních systémů a je automaticky obnovován v rámci běžných updatů operačních systémů. Účastník může využít stávající certifikát ZZS KVK nebo dodat jím preferovaný jako součást nabízeného řešení.

4. Implementační služby

4.1. Obecné požadavky

(1) Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Uchazeč je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou minimálně v následujícím rozsahu:

(a) Zajištění projektového vedení realizace předmětu plnění.

(b) Zpracování prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí zpracování prováděcí dokumentace je mj. provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.

(c) Dodávku nabízených prvků a kompletní implementaci řešení provedenou podle prováděcí dokumentace a splňující povinné parametry technického řešení,

(d) Provedení školení,

(e) Zajištění zkušebního provozu,

(f) Provedení akceptačních testů,

(g) Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu.

(h) Předání do ostrého provozu,

(2) Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

(3) Uchazeč je dále povinen zahrnout do nabídky i další související služby minimálně v dále uvedeném rozsahu. Pro každou uvedenou službu uvede uchazeč podrobný popis způsobu provedení služby při realizaci předmětu plnění zohledňující požadavky zadavatele na technické řešení, včetně zajištění požadavků dle kapitoly 3, požadavků na záruky dle kap. 5; zajištění požadavků na podporu provozu dle kapitoly 6; a to vše při zohlednění stávajícího stavu dle ZD, část 3b (popis současného stavu):

K.1 - Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS
a) Analýza stávajícího síťového prostředí a návrh nové architektury LAN, WiFi, VPN b) Zavedení segmentace a IEE802.1X c) Rekonstrukce VPN d) Vybudování centrálně řízené WiFi e) Návrh a provedení akceptačních testů
K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS

a) Analýza ICT prostředí se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí a zavedení vícefaktorové autentizace.

b) Vybudování systému správy identit (IDM)

c) Vybudování systému vícefaktorové autentizace s využitím kontaktních a bezkontaktních identifikačních prostředků (karet, tokenů). Instalace externích čteček na koncová zařízení ani distribuce identifikačních medií uživatelům není součástí plnění.

d) Metodické a odborné vedení pracovníků Zadavatele při jednání o způsobu poskytnutí a parametrech potřebných rozhraní na straně integrovaných systémů.

e) Návrh a provedení akceptačních testů, musí prokázat plnou funkčnost integrací v obvyklých scénářích použití

K.3 - Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS

a) Analýza ICT prostředí se zaměřením na vyhledání a inventarizace privilegovaných účtů

b) Vybudování systému pro správu a řízení privilegovaných účtů

c) Návrh a provedení akceptačních testů

K.4 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

a) Analýza a detailní identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat, korelovat a analyzovat. Bude obsahovat i návrh způsobu zpracování získaných informací a vhodných proaktivních i reaktivních akcí

b) Vybudování systému centrálního logování pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

c) Návrh a provedení akceptačních testů, musí zahrnovat i testy archivace a obnovy logů a ověření detekce jejich neoprávněně modifikace.

K.5 - Zavedení nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS

a) Analýza komunikačního systému a návrh způsobu sběru a obsahu síťových toků a logovaných událostí

b) Vybudování systému sběru a analýzy síťových toků a souvisejících bezpečnostních událostí.

c) Návrh a provedení akceptačních testů

K.6 - Nástroje pro zajišťování úrovně dostupnosti informací

a) Analýza současného způsobu ukládání a zálohování dat, návrh způsobu modernizace diskové virtualizace a zálohování bez významného omezení provozu operačního střediska (míra omezení navržená Účastníkem musí být schválena Zadavatelem před zahájením realizace)

b) Provedení modernizace diskové virtualizace včetně upgrade hardware serverů a kompletní migrace dat

c) Rekonstrukce zálohovacího systému se začleněním bezpečného úložiště

d) Instalace a zprovoznění koncových zařízení operačního střediska a výjezdových stanovišť

e) Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti, dále obnovení min. 1 virtuálního serveru ze zálohy z každého úložiště záloh (tj. min 3 obnovy)

f) Návrh scénářů přepnutí provozu IS ZOS do ZZOS a fungování v tzv. „ostrovním režimu“, jejich automatizace s využitím nabízeného systému pro přepnutí provozu
K.7 – Vozidlové komunikační jednotky
a) Úpravy operačního systému pro jednoúčelové používání zařízení, ověřování uživatelů nabízenými identifikačními prostředky. b) Kooperace s uchazeči provozovaných aplikací pro kompletní zprovoznění a ověření spolehlivé funkce (aplikační) pracovního uživatele. c) Návrh a příprava image pro obnovu zařízení d) Návrh a provedení akceptačních testů
K.8 – Správa identifikačních prostředků
a) Analýza a návrh životního cyklu identifikačních médií a souvisejících certifikátů, návrh politik a šablon b) Vybudování systému pro správu a řízení životního cyklu identifikačních prostředků včetně kompletní podnikové PKI (public key infrastructure) s dvouvrstvou strukturou certifikačních autorit integrované s Active Directory c) Návrh a provedení akceptačních testů, pro každý typ zařízení, které bude využit k přihlašování uživatelů nabízenými identifikačními prostředky, bude předvedena vzorová konfigurace (min. 1 vzorek) a plná funkcionalita řešení

(4) Uchazeč dle svého uvážení může doplnit v nabídce další služby, které jsou dle jeho názoru potřebné pro úspěšnou realizaci zakázky.

(5) Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office) používaných zadavatelem.

4.2. Požadavky na zpracování prováděcí dokumentace

(1) Uchazeč před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

(2) Jako podklad pro zpracování prováděcí dokumentace tedy uchazeč provede předimplementační analýzu, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění uchazeče, zejména pak s ohledem na uchazečem použité technické řešení, minimálně pro následující oblasti:

(a) Analýza a vyhodnocení stávajícího stavu, identifikace slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy.

(b) Způsob začlenění nabízených komodit do prostředí zadavatele.

(c) Síťová infrastruktura ve vztahu k plánovanému využití.

(d) Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.

(e) Analýza možností napojení zdrojových aplikačních systémů, resp. možností získávání jejich dat.

(f) Integrace nabízených softwarových systémů.

(g) Požadavky na rekonfiguraci stávajících systémů ve vztahu k plánovanému využití jejich dat.

(h) Dopady implementace na dostupnost a funkčnost stávajících služeb.

(i) Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).

(j) Integrace s virtualizační platformou VMware vSphere ve vysoce dostupném režimu a integrace s dohledovým systémem Zadavatele (provoz a správu systému zajišťuje externí partner) min. v rozsahu doporučení parametrů pro sledování.

(k) Požadované součinnosti Zadavatele.

(l) Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

(3) Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného uchazečem a musí obsahovat minimálně tyto části:

(a) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,

(b) Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů (vSphere, LAN, VPN atd.),

(c) Způsob zajištění dodávek a služeb, včetně harmonogramu zajištění HW dodávek

(d) Způsob zajištění koordinace realizace předmětu plnění s běžným provozem,

(e) Detailní návrh a popis postupu implementace předmětu plnění,

(f) Detailní popis zajištění bezpečnosti informací,

(g) Detailní harmonogram projektu včetně uvedení kritických milníků,

(h) Vazby na stávající systémy a jejich konfigurace,

(i) Návrh akceptačních kritérií a akceptačních testů,

(j) Detailní popis navrhovaných školení.

(k) Obsah a rozsah provozní dokumentace.

(4) Před zahájením projektu budou provedeny vstupní externí penetrační testy, výsledky budou uchazeči poskytnuty a relevantní opatření bude uchazeč povinen zapracovat do svého řešení tzn. i do prováděcí dokumentace. Realizace vstupních externích penetračních testů není součástí předmětu plnění.

(5) Prováděcí dokumentace bude ve lhůtě do 10 pracovních dní od předání zhotovitelem připomínkována objednatelem a připomínky budou ze strany zhotovitele vypořádány (tj. zapracovány, případně s jasným a konkrétním písemným zdůvodněním odmítnuty jako nevalidní). Ze strany objednatele nebude v rámci připomínkování v případě nepravdivých, nepřesných nebo věcně nejasných informací v této dokumentaci požadováno její opravování na správné znění, bude se pouze jednat o vyznačení výše uvedených nedokonalostí a bude na zhotoviteli jejich řádné zpracování.

(6) **Prováděcí dokumentace musí být před zahájením realizace dalších etap plnění výslovně schválena zadavatelem**.

(7) Na základě provedené implementace bude prováděcí dokumentace aktualizována na skutečně provedenou včetně detailní konfigurace, a to jak funkční, tak provedené nastavení včetně podložení provedenými analytickými podklady a dokumenty. Aktualizovaná prováděcí dokumentace bude součástí dokumentace předávané v rámci předávacího protokolu.

4.3. Harmonogram realizace

(1) Uchazeč zajistí projektové vedení po celou dobu realizace zakázky osobou odpovědnou za realizaci předmětu plnění, která bude hlavní kontaktní osobou a která bude přítomna při všech jednáních týkajících se projektu.

(2) Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy o

dílo, čísla značí počet kalendářních dnů. Údaj A značí datum předání díla, čísla značí počet kalendářních měsíců.

Poř. č.	Aktivita projektu	Nejpozdější termín pro dokončení aktivity
Etapa 1 - dodávky a implementace		
E1.1	Předimplementační analýza a zhotovení Prováděcí dokumentace	D+60
E1.2	Předání Prováděcí dokumentace Zadavateli, připomínkové řízení	D+60
E1.3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem	D+60
E1.4	Dodávky a implementace	D+180
E1.5	Školení uživatelů a administrátorů	D+180
E1.6	Zkušební provoz	D+180
E1.7	Akceptační testy	D+180
Etapa 2 - podpora provozu		
E2.1	Produkční provoz	A+min. 48 (měs)

(3) Uchazeč může dle svého uvážení výše uvedené maximální lhůty trvání v rámci Etapy 1 zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

(4) Maximální lhůty trvání nesmí uchazeč při tvorbě detailního harmonogramu prodloužit.

(5) Uchazeč uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy o dílo.

(6) Uchazeč uvede potřebnou součinnost zadavatele pro splnění harmonogramu plnění ve své nabídce.

4.4. Požadavky na školení

(1) Uchazeč zajistí školení pracovníků Zadavatele – administrátorů a uživatelů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.

(2) Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin a pracovníkům bude vystaveno osvědčení o školení s uvedením rozsahu školení. Budou provedena tato školení:

(a) Školení administrátorů – minimální rozsah školení je 20 hodin, předpokládá se účast max. 6 účastníků, školení bude probíhat v sídle Zadavatele.

(b) Školení uživatelů – minimální rozsah školení je 6 hodin, předpokládá se účast max. 10 účastníků, školení bude probíhat v sídle Zadavatele.

(3) Náklady na školení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

(4) S ohledem na pandemii COVID-19 musí být formát školení připraven jak pro prezenční výuku, tak pro možnost provedení školení elektronicky (vzdálenou formou) např. pomocí MS Teams nebo jiných elektronických prostředí pro výuku. Formát školení bude zvolen zadavatelem nejpozději týden před realizací školení, a to podle aktuálního stavu pandemie a dle doporučení relevantních orgánů (Ministerstvo zdravotnictví ČR, Hygienická stanice atp.).

4.5. Požadavky na provedení akceptačních testů a přechod do zkušebního (testovacího) provozu

(1) Uchazeč navrhne způsob a provedení akceptačních testů. Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně:

(a) Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.

(b) Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

(c) Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

(d) Prokázání registrace / aktivace podpory hardware a software výrobce, je-li podpora součástí dodávky a její aktivace potřebná

(e) Pro každou komoditu navrhne uchazeč vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a stabilita dodaného řešení.

(f) Výkonové testy prokazující shodu s požadovanými výkonnostními parametry a dále výrobcem deklarovanými či s ohledem na technologii objektivně očekávatelnými parametry:

(i) Propustnost a zpoždění (latence) u síťových komunikačních tras

(ii) Výkon u datových úložišť (IOPS, přenosová rychlost, latence)

(iii) Odezva uživatelských rozhraní aplikací a softwarových rozhraní

(2) O provedení akceptace a jejím výsledku musí být vyhotoven písemný akceptační protokol. Šablony akceptačních protokolů budou předány zadavatelem při zahájení projektu, pro zapracování uchazečem do prováděcí dokumentace.

(3) Uchazeč zajistí pro každou komoditu zkušební (testovací) provoz v délce minimálně 90 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení s dojezdem maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h. Dojezd do 2 hodin od nahlášení požadavku (v rámci pracovní doby) je zásadní pro udržení provozu kritických informačních systémů v potřebném rozsahu při plnění zákonných povinností zadavatele. V případě předávání díla po částech (viz bod (4)) je uchazeč povinen zajistit zkušební (testovací) provoz pro předávané části díla až do doby zahájení plného provozu díla jako celku, při dodržení minimální požadované lhůty pro zkušební provoz.

(4) Dílo lze předávat i po jednotlivých částech (komoditách, v členění dle tabulky uvedené v kapitole 1, bod (2)), při dodržení následujících podmínek – dílo je možné předávat po jednotlivých komoditách, přičemž podmínkou předání pro každou komoditu je provedení akceptačních testů alespoň v rozsahu bodu (1).

Etapa č. E1.4 – Dodávka a implementace	**Etapa č. E.1.6 – Zkušební provoz**	**Etapa č. E.1.7 – Zahájení plného provozu a poskytování technické podpory**
V případě hardware dodání kompletního zařízení, v případě software dodání licencí. Provedení akceptačních testů alespoň v rozsahu bodu (1)(a), (c)	Provedení akceptačních testů alespoň v rozsahu bodu (1)(b), (e)	Provedení akceptačních testů v rozsahu bodu (1)(d), (f)

(5) Po provedení akceptačních testů všech komodit, budou provedeny výstupní externí penetrační testy a uchazeč bude v rámci zkušebního provozu povinen vyřešit případné relevantní nedostatky dodaného řešení. Realizace výstupních externích penetračních testů není součástí předmětu plnění.

(6) Při předávání díla po částech bude po předání jednotlivých částí a dokončení díla jako celku následovat, akceptační řízení v plném rozsahu a předání celého díla. Jako podklad pro akceptaci celého díla budou sloužit akceptační protokoly s informacemi ohledně pokrytí požadavků akceptačních testů a zkušebního provozu z jednotlivých částí tzn. že již není nutné opakování akceptačních testů.

(7) Přechodem do plného provozu se rozumí okamžik akceptace díla v plném rozsahu včetně vypořádání všech vad a nedodělků.

4.6. Požadavky na dokumentaci

(1) Uchazeč zpracuje provozní dokumentaci, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.

(2) Provozní dokumentace bude vycházet z prováděcí dokumentace, která bude před předáním do provozu aktualizovaná dle skutečného stavu.

(3) Součástí provozní dokumentace bude popis úkonů doporučené údržby a specifikace intervalů jejích provádění a další dokumentaci v rozsahu stanoveném v prováděcí dokumentaci.

(4) Součástí předané dokumentace bude podrobná příručka pro správce i uživatele Systému pro správu identity (IDM) v českém jazyce. Součástí bude popis rozhraní IDM, kdy tato část dokumentace bude určena k přímému poskytnutí dalším uchazečům IT technologií do prostředí zadavatele za účelem napojení se na rozhraní IDM.

(5) Součástí předané dokumentace budou podrobné uživatelské postupy pro Wifi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 7 a 10, Android, iOS a macOS zohledňující nasazení systému řízení přístupů na bázi IEEE 802.1X.

(6) Uchazeč uvede do nabídky kompletní podmínky pro zajištění provozu dodaných prvků, včetně požadavků na aktualizace software (maintenance).

(7) Zhotovitel dále dodá uživatelskou dokumentaci, která bude obsahovat minimálně základní popis práce s dodaným řešením, dále bude popisovat funkcionality řešení, a to pro potřebu řádné orientace a práce uživatele. Dokumentace musí být zhotovena v českém jazyce. Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

(8) Zhotovitel dále dodá administrátorskou dokumentaci pro objednatele, která bude obsahovat popis správy a údržby dodaného řešení. Dokumentace musí být zhotovena v českém jazyce.

(9) Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

5. Požadavky na záruky

(1) Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně 24 měsíců od okamžiku předání do zkušebního provozu, není-li u konkrétního zařízení či komponenty uvedeno jinak jejím výrobcem.

(2) Uchazeč ve své nabídce uvede ceny záruky takto:

(a) Standardní záruka a standardní podpora běžně poskytovaná výrobcem technologie na území České republiky bude součástí pořizovací ceny zařízení, do přílohy **Část 6 ZD_Kalkulace nabídkové ceny_REACT**

(b) Cenu nadstandardních záruk a nadstandardních podpor (včetně aktualizací software/firmware apod.) požadovaných Zadavatelem (tj. rozdíl mezi Standardními zárukami a podporami a požadavky Zadavatele) Uchazeče uvede v položce "**Nadstandardní záruky a podpory výrobců"** přílohy **Část 6 ZD_Kalkulace**

nabídkové ceny_REACT a to dle charakteru zařízení do části hardware nebo software.

(3) Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

(4) Uchazeč ve své nabídce výslovně uvede všechny podmínky záruk

(5) Hlášení záručních závad, řízení a evidence průběhu jejich řešení bude probíhat stejným způsobem a s využitím stejného helpdeskového systému jako u podpory provozu (6).

6. Požadavky na podporu provozu

6.1. Obecná pravidla provozu

(1) Zadavatel požaduje detailní návrh podmínek podpory provozu, zajišťující plnohodnotný provoz předmětu plnění od doby předání do provozu. Uchazeč podle svého uvážení může provést úpravu parametrů, pokud takové úpravy nepovedou ke zhoršení podmínek zajištění podpory provozu.

(2) Pro hlášení servisních požadavků zajistí Duchazeč Zadavatelei přístup ke svému helpdeskovému systému s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí nabídky. Provozní doba helpdeskového systému musí být minimálně 8-17 hod. v pracovních dnech.

(3) Běžná pracovní doba zadavatele je období mezi 8:00 a 17:00 v pracovní dny.

(4) Pravidla vzdáleného přístupu budou vítěznému uchazeči předána při podpisu smlouvy.

(5) Neplánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 1 hodinu před zahájením poskytování služby nebo činnosti.

(6) Plánované zásahy do systému, které mohou ovlivnit uživatelské prostředí, jsou uživatelům oznámeny minimálně 24 hodin před zahájením poskytování služby nebo činnosti

6.2. Požadavky na podporu provozu

(1) Rozsah základní servisní podpory:

(a) Provádění aktualizací firmware a software dodaných produktů (nezahrnuje upgrade na nové hlavní verze software) v rozsahu 3 hod měsíčně. Četnost aktualizací řídí Uchazeč s ohledem na zajištění spolehlivého provozu systémů a jejich bezpečnost a kritičnost aktualizací.

(b) Helpdeskový systém s on-line přístupem (web, e-mail) pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení.

(2) Rozsah rozšířené servisní podpory:

(a) Řešení Incidentů - pokud se během řešení Incidentu ukáže, že se jedná o vadu, která spadá pod záruku systému, nebude se čas potřebný pro řešení incidentu Zadavateli účtovat.

(b) Řešení Incidentů může být zahájeno na základně požadavku Zadavatele, na základě Zadavatelem schváleného požadavku třetí strany nebo na základě schváleného podnětu uchazeče.

(c) Odborná podpora – vzdálené konzultace pro podporované služby/produkty

(3) Pro případ, že bude zadavatel požadovat služby rozšířené servisní podpory podle odst. (2), budou tyto služby vyúčtovány na konci měsíce v hodinové sazbě uvedené v Kalkulaci ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené servisní podpory pro účely přípravy nabídky je 1 hodina měsíčně.

6.3. Způsob poskytování servisní podpory

(1) Servisní podpora je poskytována zejména následujícím způsobem:

(a) Prostřednictvím pracovníka uchazeče Vzdálenou správou

(b) Prostřednictvím pracovníka uchazeče přímo na pracovišti Zadavatele

(c) Prostřednictvím pracovníka uchazeče formou vzdálené konzultace

(2) Uchazeč provede záznam o provedení servisní podpory, v záznamu uveden relevantní informace včetně doby poskytování servisní podpory a záznam zašle elektronicky zadavateli. Servisní služby, které jsou poskytovány vzdálenou formou, mohou být evidovány v elektronickém seznamu provedených úkonů.

(3) Zadavatel je povinen zabezpečit uchazeči podmínky pro řádné plnění, zejména

(a) zajistit a udržovat podmínky pro Vzdálený přístup uchazeče,

(b) zajistit dostupnost nebo odpovídající zástup Odpovědné osoby Zadavatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby Zadavatele a zajištění efektivní součinnosti odborných pracovníků Zadavatele,

(c) zabezpečit přítomnost kvalifikované osoby, která poskytne pracovníku uchazeče veškeré informace či přístupy potřebné k podpoře předmětného systému, resp. informace o zařízeních a programovém vybavení souvisejícím s předmětným systémem,

(d) umožnit uchazeči v případě nutnosti a po předchozím oznámení odstavení technických prostředků z běžného provozu,

(e) zajistit součinnost třetí strany, jestliže je to pro provedení služby potřebné.

(4) uchazeč je v případě potřeby též z vlastní iniciativy oprávněn požádat Zadavatele o dodatečné údaje o Incidentu a o nezbytnou součinnost Zadavatele na řešení Incidentu, bez které nelze zahájit či pokračovat v řešení Incidentu.

(5) Zadavatel je povinen

(a) elektronicky potvrdit uchazeči provedení služby,

(b) zajistit zálohování dat i programů a výměnu zálohovacích médií dle zálohovacího plánu, jejich dostupnost v případě potřeba a jejich uložení na bezpečných místech tak, aby bylo nešlo k jejich ztrátě nebo poškození,

(c) poskytovat potřebné nebo vyžádané informace a podklady včetně dokumentace k předmětnému systému nebo zařízení a programovému vybavení, které s ním souvisí.

6.4. Postup při řešení incidentů

(1) Zadavatel bude incident oznamovat uchazeči bez zbytečného odkladu jedním ze způsobů a na kontaktních místech uvedených ve Smlouvě o zabezpečení provozu, kam budou mít zajištěny přístup pověřené osoby Zadavatele.

(2) Součástí nahlášení požadavku Zadavatelem musí být:

(a) popis Incidentu nebo Požadavku,

(b) jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh nezbytných pro replikaci incidentu,

(c) kontaktní osoba.

(3) Uchazečem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku.

(4) Uchazeč zahájí řešení incidentu do 5 pracovních hodin od nahlášení, za pracovní hodiny se považuje období mezi 8:00 a 17:00 v pracovní dny.

(5) Uchazeč neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.

(6) Uchazeč v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že uchazeč v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. uchazeč vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.

(7) Zjistí-li uchazeč v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele.

(8) Zjistí-li uchazeč v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je uchazeč povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy uchazečem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.

(9) Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok uchazeče na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.

(10) V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:

(a) v případě Incidentu specifikuje příčinu (pokud je známa),

(b) vyzve iniciátora k ověření funkčnosti služby.

(11) Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.

(12) Po vyřešení požadavku uchazeč požadavek uzavře v systému HelpDesk a informuje Zadavatele.

(13) Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.

6.5. Záruky na servisní služby

(1) Zadavatel požaduje záruku na veškeré servisní služby provedené v rámci podpory provozu v délce trvání minimálně 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele.

1. Hlavní činnost ZZS KVK

(1) Hlavní náplní činnosti ZZS KVK je zajišťování odborné přednemocniční neodkladné péče u stavů ohrožujících život obyvatel Karlovarského kraje. V současnosti je tato služba zajišťována posádkami systému rendez-vous RV a posádkami rychlé zdravotnické pomoci RZP – velké sanitní vozy s posádkou ve složení paramedik a řidič-záchranář.

(1) Veškerou činnost ZZS řídí Zdravotnické Operační Středisko (dále jen „ZOS“, které je umístěno v Karlových Varech. ZOS využívá pro potřeby řízení výkonu ZZS informační a komunikační technologie, případně prostřednictvím těchto technologií, poskytuje informace, řídí posádky ZZS.

(2) ZZS KVK plní úkoly k zajištění zvláštní zdravotní péče fyzickým osobám, které se náhle nebo nečekaně ocitly v ohrožení zdraví či života, tedy nepřetržitě zabezpečuje odbornou přednemocniční neodkladnou péči včetně přednemocniční péče o dárce a příjemce orgánů v souladu s příslušnými právními předpisy a pokyny zřizovatele a za plnění těchto úkolů odpovídá.

(3) V rámci svých činností ZZS KVK zajišťuje kvalifikovaný příjem, zpracování a vyhodnocení tísňových výzev k odborné zdravotnické první pomoci, určení nejvhodnějšího způsobu poskytování přednemocniční neodkladné péče, výjezd výjezdových skupin (VS) k pacientům vyžadujícím PNP na místě a jejich následný transport do zdravotnických zařízení (urgentní příjem).

(4) Poskytování služeb ZZS KVK je zajišťováno s využitím IS ZZS KVK a souvisejících technologií. Systém a související technologie a jejich garantovaný provoz jsou podmínkou nutnou pro poskytování služeb ZZS KVK. Popis IS ZZS KVK a souvisejících technologií je uveden dále v tomto dokumentu.

2. Popis dokumentace

(1) K provozování a řízení rozvoje ICT je využívána a udržována základní Provozní dokumentace.

(2) Provozní dokumentace popisuje základní nastavení technologií, hardwarových a softwarových systémů, s výjimkou sítě je tvořena uživatelskými manuály jednotlivých zařízení či programů.

(3) Citlivé údaje (přístupové účty apod.) jsou uloženy odděleně od Provozních dokumentací.

(4) Dodavatel je povinen zajistit nezbytné doplnění Provozní dokumentace reflektující provedené změny. Relevantní části dokumentace budou dodavateli zpřístupněny až po podpisu Smlouvy o dílo k této zakázce.

3. Popis způsobu řešení incidentů

(1) Zadavatel pro řešení incidentů a podporu uživatelů nevyužívá vlastní systém Helpdesk.

(2) Zadavatel zajišťuje podporu 1. úrovně a většinu běžných problémů jsou schopni vyřešit interní pracovníci Zadavatele.

(3) Incidenty a požadavky, které nevyřeší interní specialisté, jsou zadávány do helpdeskových systémů dodavatele systému, který vykazuje incident nebo na který směřuje požadavek

uživatele. Hlášení incidentů a požadavků je prováděno telefonicky, emailem nebo přímo zadáním ticketu/požadavku do helpdeskového systému dodavatele.

4. Popis servisních oken

(1) Zadavatel nemá pevně definovaná pravidelná servisní okna pro údržbu ICT technologií. Aplikace aktualizací a oprav virtuálních serverů se provádějí dle potřeby a s přihlédnutím k minimalizaci omezení uživatelů.

5. Místo plnění

(1) Lokality, ve kterých bude předmět plnění realizován je uveden v této kapitole. Zadavatel má ze svého statutu povinnost zajistit odbornou přednemocniční neodkladnou péči a tu poskytovat v zákonem požadovaných limitech – z toho plyne i rozmístění a počet výjezdových základen, které jsou zároveň předmětem procesu kontinuální optimalizace. Dodavatel ve své nabídce musí zohlednit skutečnost, že počet i konkrétní umístění výjezdových základen se v průběhu zajištění předmětu plnění může změnit.

(2) Mimo budovu operačního střediska ZZS KVK, kde je umístěno primární datové centrum, působí na jednotlivých výjezdových základnách (dále jen VS) na území Karlovarského kraje. ZZS KVK má v rámci Karlovarského kraje celkem 13 výjezdových základen:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Karlovarského kraje, p.o.	Karlovy Vary - Dvory, Závodní 390/98C	Primární datové centrum ZZS KVK – umístění technologií, návaznost na technologie umístěné v tomto DC a případná dodávka částí technologie. Poskytování servisních služeb pro Systém a technologie umístěné do této lokality. Sídlo ZZS KVK – místo předávání poskytovaných služeb.
Území Karlovarského kraje	Území Karlovarského kraje	Poskytování servisních služeb k SW a technologiím ve vozidlech a SW využívaného ze strany výjezdových skupin v terénu a související služby dle definice služeb.
Policie ČR – Krajské ředitelství Karlovarského kraje	Karlovy Vary – Dvory, Závodní 386/100	V této lokalitě je umístěna technologie systému PEGAS. Bude se týkat části technologie pro zajištění integrace radiového systému Pegas (CC-API). Nezbytná součinnost pro Poskytovatele bude zajištěna Objednatelem.

Přehled výjezdových základen k 1. 7. 2020:

Číslo výjezdové základny	Výjezdové základny (VZ)	Adresa
Oblast Cheb		
1	Cheb	**Cheb**, K Nemocnici 1110/17
2	Mariánské Lázně	**Mariánské Lázně**, U Nemocnice 464/1
3	Aš	**Aš**, Okružní 2545
4	Luby	**Luby,** Malé náměstí 35, 351 37

Číslo výjezdové základny	Výjezdové základny (VZ)	Adresa
Oblast Karlovy Vary		
5	Karlovy Vary	**Karlovy Vary**, Závodní 390/98C
6	Ostrov	**Ostrov**, Jáchymovská 1491
7	Nejdek	**Nejdek**, Karlovarská 1347
8	Toužim	**Toužim**, Sídliště 526
9	Žlutice	**Žlutice**, Karlovarská 530
10	Teplá	**Teplá,** Pivovarská 333, 364 61
Oblast Sokolov		
11	Sokolov	**Sokolov**, Slovenská 1596
12	Horní Slavkov	**Horní Slavkov**, Větrná 1015
13	Kraslice	**Kraslice**, Husova 127

(3) Kromě primárního datového centra v lokalitě Karlovy Vary je součástí plnění i zařízení umístěné v lokalitě Sokolov, kde je záložní datové centrum.

5.1. Uživatelé a vybavení

(1) V následující tabulce jsou uvedeny orientační počty současných uživatelů (jedná se o počet registrovaných, nikoliv současně připojených uživatelů):

Skupina	Počet	Doplňující informace
Členové výjezdových skupin	270	Jedná se o maximální počet členů posádek v rámci směnného provozu pro systémy EKP, MZD, NAV.
Operátoři ZOS	19	Jedná se o maximální počet operátorů v rámci směnného provozu pro systémy IS ZOS, GIS, integraci telefonie a radiofonie.
Uživatelé EKJ	10	Jedná se o maximální počet uživatelů přistupujících přes GUI do AVL nad rámec uživatelů IS ZOS.
Uživatelé pojišťovny	6	Jedná se o maximální počet uživatelů přistupujících přes GUI do pojišťovny.
Uživatelé nahrávání	25	Jedná se o maximální počet uživatelů přistupujících přes GUI do systému nahrávání nad rámec IS ZOS.
Vozidel	100 / 50	Maximální počet vozidel současně provozovaných v AVL a NAV je 100. Maximální počet skutečně provozovaných vozidel je 45. Neprovozovaná vozidla budou v systému deaktivována, nicméně musí být zachována jejich historie.
Správci	7	Správci technologie a informačních systémů.

6. Stávající stav informačních a komunikačních technologií

(1) Dále je stručně uveden přehled jednotlivých systémů a technologií, které zadavatel používá pro zajištění činnosti, **jejichž činnost nesmí být v průběhu předmětu plnění omezena** a na které se případně dodavatel bude napojovat např. s identitním systémem (systémy a technologie jsou detailně popsány v dalších kapitolách dokumentu):

IS, SW, subsystém	Výchozí stav
Informační systém zdravotnického operačního střediska (IS ZOS)	IS ZOS je systém pro operační řízení dispečinku Zdravotnické záchranné služby (ZZS). Poskytuje funkcionalitu pro všechny činnosti ZOS ZZS počínaje náběrem tísňové výzvy (calltaking) přes operační řízení po vyhodnocení činnosti ZOS. Základní moduly implementované na ZZS: 1. Dispečink 2. Základna 3. Správa směn 4. Evidence směn 5. Svolávání 6. Statistiky 7. Kontrolní pracoviště 8. Administrace 9. Správa stanic Stávající IS ZOS je produkt SOS jehož výrobcem je společnost PER4MANCE s.r.o.
Geografický informační systém (GIS)	Geografický informační systém (GIS) zajišťuje: 1. Zobrazení mapových podkladů a základní práce s mapou na všech pracovištích. 2. Zobrazování poloh a stavů vozidel ZZS ze systému sledování vozidel (AVL). 3. Zobrazování poloh událostí a SaP dalších složek IZS v rámci integrace na NIS IZS. 4. Lokalizace pro IS ZOS, vyhledávání v mapě a další geografické služby. Stávající GIS je produkt, jehož výrobcem je společnost T-mapy s.r.o.
Informační systém pro sledování vozidel (AVL)	Informační systém pro sledování vozidel (AVL) zajišťuje: 1. Sledování polohy a stavu vozidel ZZS. 2. Předávání těchto stavů, vč. doprovodných údajů z vozidel do IS ZOS a EKP. 3. Předávání dat pro zobrazení polohy a stavů vozidel v mapě. 4. Zasílání výzvy do vozidel. Stávající Informační systém pro sledování vozidel (AVL) je produkt Fleetware jehož výrobcem je společnost RADIUM s.r.o.
Navigační software pro posádky vozidel	Jedná se o zásahový SW pro výjezdová vozidla ve vozidlech sloužící pro navigaci posádek a další služby pro posádky ve vozidlech. Jedná se o produkt, jehož dodavatelem je společnost RADIUM s.r.o.

IS, SW, subsystém	Výchozí stav
Elektronická karta pacienta (EKP) a Mobilní zadávání dat (MZD)	Elektronická karta pacienta (EKP) slouží pro zaznamenávání všech relevantních údajů o výjezdech a pacientech v rámci těchto výjezdů. Data jsou na vstupu čerpána z IS ZOS a následně během nebo po ukončení výjezdu z MZD (Mobilní zadávání dat), kontrolována a následně zpracována do formy pro vykazování pojišťovnám. Mobilní zadávání dat (MZD) o pacientech slouží pro zadávání dat o pacientech v rámci výjezdu ZZS v terénu prostřednictvím mobilních zařízení (tabletů) a následně jejich předávání do centrálního systému EKP pro následné zpracování. Systémy poskytují následující funkce: 1. Přebírání dat o výjezdu z IS ZOS (součástí integrace). 2. Posílání dat do mobilních zařízení posádek v terénu. 3. Funkčnost pro vyplnění posádkami v terénu. 4. Předání z MZD zpět do EKP. 5. Přebírání dat ze systému sledování vozidel. 6. Následné úpravy, dopracování, kontrola dat na výjezdových základnách. 7. Předávání do IS Pojišťovna. Stávající EKP/MZD jsou produkty společnosti European Medical Distribution s.r.o. Součástí této části je uzel ISAC, který zajišťuje: 1. Vyhledání životních údajů pacienta (alergie, rizikové faktory, medikace, diagnózy a návštěvy) 2. Zobrazení náhledu na dokument klinického případu 3. Odeslání výjezdové zprávy ZZS Stávající ISAC je produkt, jehož výrobcem je firma I.CZ.
Pojišťovna	Pojišťovna přebírá data ze systému EKP a slouží pro vyúčtování poskytnuté zdravotnické péče zdravotním pojišťovnám. Stávající Pojišťovna je produktem společnosti European Medical Distribution s.r.o.
Elektronická kniha jízd (EKJ)	Stávající systém elektronické knihy jízd je od společnosti RADIUM s.r.o. Popis současné implementace systému je uveden dále v této kapitole. Stávající Elektronická kniha jízd (EKJ) je produkt Fleetware jehož výrobcem je společnost RADIUM s.r.o.
Integrace se systémem Pegas (CC-API)	CC-API slouží jako integrační rozhraní pro napojení informačních systémů a aplikačního SW k radiové síti PEGAS/TETRA a TETRAPOL. CC-API je produktem společnosti AIRBUS a výhradním dodavatelem technologie PEGAS/TETRA a TETRAPOL je společnost Pramacom Prague spol. s r.o.
Integrace	Integrace telefonie a radiofonie zajišťuje propojení IS ZOS s telefonií

IS, SW, subsystém	Výchozí stav
radiofonie a telefonie	(telefonní ústředna), obsluhou radiové sítě Pegas/Matra MV ČR, záznamovým zařízením a poskytuje obsluze jednotný, a hlavně jednoduchý systém obsluhy pomocí dotykové obrazovky na pracovišti operátora. Základní funkcionality a integrace jsou: 1. Zajištění integrace a obsluhy telefonní komunikace prostřednictvím telefonní ústředny. 2. Zajištění integrace a obsluhy radiofonní komunikace prostřednictvím radiové sítě Pegas/Matra. 3. Integrace s IS ZOS – volání, návaznost hovorů na výzvy a události. 4. Záznamové zařízení (REDAT) – nahrávání radiofonní komunikace. 5. Poskytnuté aplikace na dotykové obrazovce obsluhy. Stávající Integrace radiofonie a telefonie je produktem společnosti Komcentra s.r.o.
Telefonní ústředna	Telefonní ústředna slouží pro příjem tísňové výzvy na lince 155 a komunikaci ZOS ZZS. Telefonní ústředna je postavena na řešení Alcatel-Lucent OmniPCX Enterprise Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu. Objednatel nepřipouští změny integračních rozhraní subsystému při zahájení poskytování služeb. Popis současné implementace systému: **Karlovy Vary** - Tel. Ústředna Alcatel-Lucent OmniPCX Enterprise s SW R.11.0 verzí a s propojením do ostatních Pbx přes VOIP. **Sokolov** - Tel. Ústředna Alcatel – Lucent OmniPCX Office s aktuální SW verzí R.7.1. **Cheb** - Tel. Ústředna Alcatel-Lucent OmniPCX Office s aktuální SW verzí R.9.2. **Aš** - Tel. Ústředna Alcatel-Lucent OmniPCX Office s aktuální SW verzí R.9.2. **Nejdek** - Tel. Ústředna Alcatel-Lucent OmniPCX Office s aktuální SW verzí R.9.2. **Žlutice** - Tel. Ústředna Alcatel-Lucent OmniPCX Office s aktuální SW verzí R.9.2. **Ostrov** - Tel. Ústředna Alcatel-Lucent OmniPCX Office s aktuální SW verzí R.9.2. **Horní Slavkov** - Tel. Ústředna Alcatel-Lucent OmniPCX Office s aktuální SW verzí R.9.2. **Mariánské Lázně** - Tel. Ústředna Alcatel-Lucent OmniPCX Office s aktuální SW verzí R.9.2.

IS, SW, subsystém	Výchozí stav
Systém nahrávání	Záznamový systém (REDAT), jeho aplikační část SW ReDat Aplikační server (RAS) slouží pro záznam telefonních hovorů na tísňové lince, záznam všech hovorů na ZOS, a to jak telefonních, tak radiofonních. Stávající systém nahrávání je produktem společnosti RETIA, a.s.
Infrastruktura	Plně virtualizovaná a vysoce dostupná serverová a disková platforma poskytuje ve režimu 24x7 (nonstop) výpočetní zdroje a úložné kapacity aplikačním i sdílených systémů systémům ZZS. Virtualizační platforma je provozována na technologiích VMware vSphere a HPE StoreVirtual. Interní síťová komunikace je zajišťována síťovými prvky HPE. Perimetrovou ochranu zabezpečuje cluster next-gen firewallů Fortinet, který slouží i pro zakončení VPN výjezdových základen vybavených VPN routery Cisco. Pro doručování aplikací pracovníkům operačního střediska je využívána technologie VDI VMware View/Horizon. Koncová zařízení jsou typu tenký klient (terminal) výrobce HPE. Pro sdílení klíčových informací v operačním středisku je k dispozici telestěna sestavená ze 4 velkoplošných displejů. Dále je operační středisko vybaveno sdíleným multifiknčním zařízením (tiskárna-skener-fax). Kritické systémy (virtuální server) jsou replikovány do záložní lokality (Sokolov) a společně s definovanými postupy obnovy provozu při nedostupnosti primárního operačního střediska tvoří tzv. DR (disaster recovery) lokalitu. Replikace je součástí zálohovacího systému Veeam, zálohy jsou ukládány na dvojici nezávislých síťových úložišť NAS. Veškeré systémy jsou provozně ověřeny na kompatibilitu s aplikačními systémy a specialisté Objednatele jsou vyškoleni na jejich používání.

8. Popis datových rozhraní

(1) Zadavatel zajistil potřebnou součinnost dodavatelů informačních systémů používaných zadavatelem a na které se dodavatel musí napojit v rámci systému pro správu identit (IDM), aby mohl získat potřebná data a řídit v těchto systémech uživatele a jejich oprávnění – **realizace napojení na tyto systémy za účelem propojení uvedených informačních systémů s IDM je součástí předmětu plnění**.

(2) Zadavatel zároveň provedl průzkum trhu ohledně technických možností napojení IDM na stávající systémy včetně předpokládaných nákladů na připojení na tyto informační systémy. **Zadavatel upozorňuje na to, že se jedná o předpokládané podmínky stanovené na základě jednání s dodavateli ohledně možností připojení na zdroje dat a zároveň v rozsahu informací používaných v části 3a Technická specifikace. Zadavatel výslovně doporučuje dodavatelům, aby si konkrétní podmínky pro napojení na IDM prověřili ve vztahu k dodavateli nabízeným technologiím samostatně u výrobce daného systému. Dodavatel je povinen ve své nabídce všechny uvedené skutečnosti zohlednit**.

(3) Přehled stávajících systémů a možností datových rozhraní pro napojení, včetně předkládaných nákladů na implementaci datového rozhraní:

Stávající systémy	**Funkcionalita č.1:** **Ověřování (autentizace) uživatelů aplikace vůči Microsoft Active Directory.**	**Funkcionalita č.2:** **Řízení oprávnění uživatelů v aplikaci na základě členství uživatelů ve skupinách Active Directory.**	**Funkcionalita č.3:** **Automatické přihlášení a ověření uživatele přihlášeného do operačního systému Windows (tzv. SSO - Single-Sign-On) do aplikace, alternativně ověření přihlášeného uživatele Windows přistupujícího do aplikace vůči čipové kartě nebo tokenu prostřednictvím rozhraní standardu PKCS #11**	**Funkcionalita č.4:** **API nebo jiný způsob správy uživatelů vaší aplikace a jejich oprávnění (pokud aplikace nepodporuje funkcionalitu uvedenou v přechozích sloupcích)**	**Funkcionalita č.5:** **Logování činnosti uživatelů a správců a poskytnutí těchto logů systému centrální správy logů**
IS ZOS (výrobce Per4mance	Ano, nutné konfigurační změny a impementace	Ano, nutné konfigurační změny a impementace	Ano, nutné	Není relevantní (aplikace podporuje	Ano, nutné konfigurační změny

s.r.o.) https://www.per4mance.cz/cs/comp/contact.php	funkcionality AD, předpokládané náklady na zpřístupnění funkce jsou 300 000 Kč bez DPH	funkcionality AD, předpokládané náklady na zpřístupnění funkce jsou 200 000 Kč bez DPH	konfigurační změny	funkcionalitu uvedenou v přechozích sloupcích)	a implementace rozšířeného logovacího systému, předpokládané náklady na zpřístupnění funkce jsou 200 000 Kč bez DPH
Elektronická karta pacienta (EKP) a Mobilní zadávání dat (MZD), Pojišťovna, MedText (výrobce European Medical Distribution s.r.o) https://emd-company.eu/en/contact/	Ano, nutné konfigurační změny a implementace a konfigurace EMD AD konektoru, předpokládané náklady na zpřístupnění kompletní funkcionality jsou 400 000 Kč bez DPH	Ano, nutné konfigurační změny, práva na základě skupin v AD lze nastavovat, je nutná implementace a konfigurace EMD AD konektoru, předpokládané náklady na zpřístupnění kompletní funkcionality jsou 89 000 Kč bez DPH	Ne, SSO přes windows systém nepodporuje. Ověření přes komerční certifikát PKCS11 je momenálně implementované pro ICA a eIdentity a jejich příslušné chipy Starcos (Middleware SecureStore) a Gemalto (Middleware SAC – SafeNet Auth. Client). Implementace a konfigurace závisí na daném hardwaru a verzi middleware, potřebného pro komunikaci s chipem, předpokládané náklady na zpřístupnění kompletní funkcionality jsou 479 000 Kč bez DPH	Není relevantní (aplikace podporuje funkcionalitu uvedenou v přechozích sloupcích)	Ano, nutné konfigurační změny, předpokládané náklady na zpřístupnění kompletní funkcionality jsou 79 000 Kč bez DPH
Fleetware (výrobce RADIUM	Ano, nutné konfigurační	Ano, nutné konfigurační	SSO je při funkční AD	Ano, REST API,	Ano, nutné

s.r.o.) https://www.fleetware.promo/	změny, aplikace podporuje autentizaci uživatelů vůči Microsoft Active Directory (dále AD), ověřování je založeno na LDAP (Lightweight Directory Access Protocol).	změny, v rámci AD autentizace aplikace zařazuje uživatele do (maximálně jedné) role odpovídající jeho AD skupině. V konfiguraci aplikace je určeno, jaké AD skupiny řídí uživatelskou roli. Uživatelské role musejí být založeny v aplikaci a obsahovat požadovaná oprávnění. Synchronizace - zařazování uživatelů do rolí dle AD skupin - je zajištěna pravidelně spouštěným procesem (frekvenci lze nastavit).	autentizaci podporováno, funguje na protokolu Kerberos. V případě, kdy např. díky nesprávnému nastavení prohlížeče není SSO dostupné, zobrazí aplikace standardní přihlašovací dialog.	Aplikace disponuje REST API, pomocí kterého lze spravovat uživatele a oprávnění ve stejném rozsahu, který je dostupný z UI.	konfigurační změny, Aplikace disponuje Audit logem, kde jsou logovány vybrané uživatelské akce ve struktuře kdo / kdy / co vykonal - např. akce prováděné v Knize jízd, založení/aktualizace/ smazání jednotlivých entit, e-mailové notifikace generované aplikací. V případě požadavku je možné logování rozšířit a začít logovat danou operaci, která v současnosti v Audit logu zachycena není (uživatelská úprava = placený vývoj nad rámec předpokládaných nákladů). Data z tohoto logu jsou dostupná na REST API, v requestu lze specifikovat období. Pozn.: Kromě výše uvedeného Audit

					logu aplikace loguje jednotlivé API požadavky, k těmto logům lze přistupovat např. pomocí nástroje Grafana. Tato úroveň logování je určena pro dodavatele/servisní účely, nicméně v závažných případech lze takto dostupné informace analyzovat a následně poskytnout. Předpokládané náklady na úpravy funkcionalit 1 až 5 – 70 000 Kč bez DPH
ReDAT (výrobce RETIA, a.s.) https://retia.cz/kontakty/	Ano, nutné konfigurační změny, předpokládané náklady jsou 18 000 Kč bez DPH.	Není v aplikaci dostupné	Ano, nutné konfigurační změny (nelze se přihlásit pod stejným odkazem přes LDAP a SSO), předpokládané náklady jsou 18 000 Kč bez DPH. Záznamový systém ReDAT ve svém základním rozhraní podporuje Automatické	Ne Aktuálně dodaný a používaný Záznamový systém ReDAT (ReDAT eXperience) na ZZS KVK podporuje možnosti autentizace a automatické přihlášení uvedené v požadavku č. 1 a 3. Požadavek č. 2 je	Ano, nutné konfigurační změny Aktuálně dodaný a používaný Záznamový systém ReDAT (ReDAT eXperience) na ZZS KVK umožňuje interní vytváření a správu uživatelských a systémových logů uvnitř systému v tzv.

			přihlášení a ověření uživatele přihlášeného do operačního systému Windows (tzv. SSO - Single-Sign-On). S využitím alternativních způsobů, tj. vůči čipové kartě či tokenu na rozhraní PKCS #11 neuvažujeme.	plněn částečně (pouze na úrovni přístupu do aplikace). Z tohoto důvodu nevidíme důvod, proč pro toto využívat jiné rozhraní či způsoby správy uživatelů. V rámci Záznamového systému ReDAT nedoporučujeme využití pro správu uživatelů jiný způsob, než je podporován.	aplikaci AUDIT. Který v základní verzi umožňuje pouze jednorázový export logů do CSV soboru. Požadavek na určité automatické poskytování uživatelských a systémových logů systému centrální správy logů u nás představuje dovývoj. Ten může realizován různými způsoby, např.: job, který se spustí jednou za den (řízeno WatchDogem) a automaticky vyexportuje v csv formátu logy za uplynulých 24h. Tyto logy budou ukládány na dané místo v adresářové struktuře ReDAT eXperience, odkud si je můžete stahovat a pracovat s nimi dle potřeby. Tato varianta je

					předpokládána ve výši 39 900 Kč bez DPH (vývoj + pro nezbytné úpravy včetně nasazení a jeho konfigurace). Výše popsanou funkci považujeme za základní variantu. Pokud by byly požadovány nějaké další funkcionality, muselo by být specifikováno jaké a na základě toho bychom posoudili proveditelnost a pracnost.
NidlWare (výrobce Ing. Pavel Nídl) https://www.nidl.cz/cz/kontakt	Prostředí instalovaných ekonomických aplikací je Microsoft Access. Pro přístup k aplikacím se uživatelé přihlašují ověřením vůči Microsoft Active Directory na svůj „virtuální počítač“ (ad 1 a 3) s nastavením svého členství ve skupinách Active Directory (ad 2). Toto přihlášení je aplikacemi akceptováno a	Viz text funkcionalita č. 1	Viz předchozí text funkcionalita č. 1	Viz předchozí text funkcionalita č. 1	Viz předchozí text funkcionalita č. 1

	interní autentizace aplikací je proto vypnuta (ad 4). Kromě logování, které provádí MS Access do centrální správy logů, zapisují aplikace vybrané činnosti přihlášených uživatelů do interních databází (ad 5).				
AUTOPLAN (Krob Software s.r.o.) https://www.autoplan.cz/cz/kategorie/kontakty.aspx	Funkcionalita aktuálně není podporovaná. Aplikace používá autentizaci dle vlastní evidence uživatelů. Ti mohou být napojeni na AD uživatele, napojení ale slouží pouze pro SSO (viz funkcionalita č. 3). Autentizaci stávajících uživatelů Autoplanu vůči AD lze doplnit. Náklady 2000 Kč bez DPH, realizace do 2 měsíců od objednání. Nasazení formou standardní aktualizace, žádné další speciální požadavky. Omezení na jednu (aktuální) doménu.	Jsou poskytovány nástroje na synchronizaci organizační struktury zaměstnanců a částečně i evidence uživatelů s AD, požadovaná funkcionalita ale není podporována. Je možné připravit šablonové řešení "rolí" (sad obecných práv) na základě členství uživatelů ve skupinách AD (s automatickými periodickými synchronizacemi dle AD). Náklady 5000 Kč bez DPH, realizace do 3 měsíců od objednání. Nasazení formou	Standardní součást stávající verze aplikace.	API tuto funkcionalitu neposkytuje (navíc není součástí standardní verze aplikace). Doplnění pouze formou zakázkové úpravy, přesné podmínky by bylo nutné dojednat. Vhodnější by ale bylo realizovat přímo úpravy 1) a 2).	V rámci aplikace protokolujeme veškeré aktivity relevantní z pohledu GDPR a ochrany osobních údajů a tyto protokoly jsou přístupné oprávněným uživatelům. Export protokolů aktuálně nepodporujeme. Bylo by možné doplnit modul pro automatický přírůstkový export protokolů ve formě dat strukturovaných v několika polích (datum/čas, uživatel, provedená operace, ...) prostřednictvím souborů, volání API

		standardní aktualizace, žádné další speciální požadavky. Omezení na jednu (aktuální) doménu.			nebo zápisů do externí databáze. Náklady 3000 Kč bez DPH, realizace do 3 měsíců od objednání (po dohodě technických parametrů). Nasazení formou standardní aktualizace, žádné další speciální požadavky.
IS (Pavel Uher) info@puher.cz	Ano. Funkce je dostupná formou upgrade aplikace. Předpokládané náklady na upgrade jsou 2000 Kč bez DPH.	Ano. Funkce je dostupná formou upgrade aplikace. Předpokládané náklady na upgrade jsou 5000 Kč bez DPH.	Ano. Funkce je dostupná formou upgrade aplikace. Předpokládané náklady na upgrade jsou 2000 Kč bez DPH.	Není relevantní (aplikace podporuje funkcionalitu uvedenou v přechozích sloupcích)	Ano, aplikace automaticky loguje veškeré změny, které provedli uživateli i správci. Požadavek je realizovatelný, bude potřeba implementovat napojení na API rozhraní třetí strany, pomocí kterého se budou uploadovat logy do systému centrální správy logů. Vzhledem k tomu, že API rozhraní třetí strany není zatím specifikováno, lze

					stanovit pouze odhadované náklady na implementaci. Tyto náklady jsou 5000 Kč bez DPH
Avensio (Alfa Software s.r.o.) Mzdy https://www.alfasoftware.cz/kontakt/	Není dostupná, v případě požadavku je možné provést realizaci ověřování uživatele v Active Directory s tím, že se pouze ověří jméno a heslo a ostatní nastavení i tak zůstávají v aplikaci. Předpokládané náklady na úpravu jsou 57 600 bez DPH	Ne	Ne	Ne	Ano, logování změn je součástí aplikace, logují se přihlášení a zadávané změny na datech, přístup k logovaným datům je z rozhraní aplikace formou exportu CSV
ServiceDesk, Asset Management (Alvao s.r.o.) https://www.alvao.com/cs/kontakt	Ano, již implementováno.	Ano, již implementováno. Pravidelný import uživatelů utilitou ImportAD.exe	Ano, již implementováno. Nastaveno integrované ověřování do webového portálu a AM console.	K dispozici je API, viz https://doc.alvao.com/cs/10.4/alvao_asset_management/implementation/customization/alvao_api.aspx Cena za poskytnutí součinnosti při implementaci rozhraní API – dle skutečnosti v sazbě 12.000 Kč/člověkoden konzultantské práce a 16.000 Kč/člověkoden	Ano, logování změn je součástí aplikacePřihlášení/odhlášení do/z systému Přidání/úprava/odebrání uživatelů/skupin Změna členství ve skupinách Změna nastavení SLA a oprávnění na službách V rámci Asset Management má každá konfigurační

				programátorské práce	položka svůj deník, do kterého se zapisují veškeré změny provedené s daným objektem V rámci Service Desku je u každého požadavku dostupný „Podrobný deník“, ve kterém lze nalézt všechny aktivity, které byly s požadavkem provedeny.
O2 FirstResponder (O2 Czech Republic a.s.) https://www.o2.cz/firmy-a-organizace/o2-sos	Ano, funkcionalita je již součástí systému, programová úprava není třeba (aplikační server musí být součástí domény, musí být zavedeni uživatelé z AD)	Ano, je nutná příprava synchronizační služby, která bude synchronizovat data uživatelů do O2 SOS dle skupin. Úprava API O2 SOS pro metody synchronizace uživatelů. Služba musí běžet v kontextu AD, pod AD uživatelem a mít přístup na API O2 SOS	Ano, SSO je součástí systému, čipová karta nebo token není aktuálně možný	Ano, je nutná úprava stávajícího API o kompletní set metod na správu uživatelů	Ano, je nutné provést doplnění auditní stopy. Úprava stávajícího API o možnost stažení auditní stopy. Přidání reportu pro auditní stopu Nutno upřesnit rozsah auditních dat, může mít dopad do velikosti DB (tj. doby retence dat).. Předpokládané náklady na úpravy funkcionalit 1 až 5 – 140 000 Kč bez

					DPH

(4) Dodavatel není povinen využít výše zmíněné možnosti napojení na informační systémy a může použít i jiné vhodné metody pro připojení na datové zdroje.

9. Informační systém zdravotnického operačního střediska (IS ZOS)

(1) Informační systém zdravotnického operačního střediska (IS ZOS) je realizován SW SOS s moduly Dispečer, Evidence výjezdových skupin, Plánování směn a Administrace a integrovaných spolupracujících modulů GIS, Sledování vozidel (AVL), Elektronická kniha jízd (EKJ), EKP, MZD a Pojišťovna.

9.1. Detailní popis řešení IS ZOS

(1) Subsystém IS ZOS funkčně pokrývá procesy pro podporu činnosti Krajského zdravotnického operačního střediska ZZS KVK a výjezdových skupin na výjezdových skupin na základnách ZZS KVK. V následujících kapitolách jsou popsány tyto oblasti:

(a) uživatelé systému IS ZOS,

(b) řešené procesní a funkční oblasti,

(c) integrace se systémy, technologiemi a datovými zdroji.

9.2. Uživatelé IS ZOS

(1) Uživateli IS ZOS jsou pracovníci Krajského zdravotnického operačního střediska ZZS, představitelé vedení ZZS a pracovníci posádek VS. Pracovníkům jsou přiřazeny role podle jejich úkolů a rozsahu oprávnění při práci se systémem. Role obsahují omezení/povolení přístupu na aplikační části a data.

(2) Hlavní uživatelské role jsou:

(a) operátor (call-taker / dispečer) – call-taker přijímá tísňové výzvy, provádí identifikaci a lokalizaci volání. Přijaté výzvy zpracovává dispečer, který událostem přiděluje příslušné prostředky ZZS a řídí výjezdové skupiny.

(b) vedoucí dispečer – dohlíží na práci call-takerů a dispečerů, provádí dílčí administrační úkony v systému (např. doplnění číselníku)

(c) supervizor (správce) – provádí složitější administrační úkony v systému, provádí údržbu mapových podkladů a jejich synchronizaci

(3) Mimo hlavní uvedené role jsou v systému IS ZOS i jiné role pro další speciální činnosti.

(4) Uživatelé pracují se systémem prostřednictvím grafického uživatelského rozhraní.

(5) Každý uživatel má svůj vlastní účet a k němu přidělené heslo.

(6) Uživatelem navigačního tabletu je posádka vozidla (řidič), který prostřednictvím vozidlové jednotky dostává informaci o místě zásahu a zároveň jeho prostřednictvím zadává a mění informace o stavu výjezdu (status).

9.3. Procesní a funkční oblasti

(1) K základním funkčním oblastem řešení IS ZOS patří:

(a) Příjem tísňové výzvy – zahrnuje příjem tísňové výzvy hlasové, pomocí SMS zprávy či datovou větou ze systému NIS IZS. Součástí procesu je identifikace a lokalizace volajícího a klasifikace událostí.

(b) Operační řízení – pokrývá procesy a funkcionalitu pro podporu práce dispečerů pomocí událostně orientovaného GUI, podporuje správu součinností s ostatními složkami IZS a jinými subjekty. Je provázáno na vizualizace situací pomocí systému GIS, správu výjezdových skupin a prostředků.

(c) Komunikace s výjezdovými skupinami – zahrnuje scénáře hlasové i datové komunikace s výjezdovými skupinami integrací na komunikační technologie (telefony, radiová síť) a integraci na podpůrné systémy (systém komunikace s vozidlovými jednotkami).

(d) Monitorování posádek a prostředků – zahrnuje sběr informací o stavu posádek a prostředků ze systému pro sledování vozidel na podporu operačního řízení.

(e) Sekundární transporty – řešení podporuje zadávání a správu požadavků na sekundární transporty a plánování prostředků na ně.

(f) Integrace technologií a dalších systémů – pokrývá procesy technických a technologických rozhraní na technologie a integrační API na další systémy - interní systémy ZZS či externí.

(g) Zobrazování historických dat – všechny minulé události s jejich historií řešení jsou zachovány pro zpětné kontroly a zjišťování. Prohlížení historických dat v IS ZOS je možné přes přehled události, i přes dotazy na historii řešení konkrétního místa události nebo historii telefonátů z daného telefonu.

(h) Sestavy, statistiky – zahrnuje funkcionalitu pro vytváření potřebných tiskových sestav, přehledů a statistik jak pro tiskovou prezentaci, tak pro načtení k dalšímu zpracování v externím software (data na import do MS EXCEL).

(i) Správa systému a mapových podkladů – pokrývá procesy konfigurace parametrů systému, správu číselníkových položek, správu uživatelů a jejich rolí (oprávnění), zálohování systému, aktualizace a doplňování mapových podkladů.

9.4. Integrované systémy a technologie

(1) Řešení IS ZOS je integrováno na řadu technologických systémů sloužících pro přímou podporu komunikace Krajského zdravotnického operačního střediska s výjezdovými skupinami či místem události.

(2) Obsahem integrace pro jednotlivé systémy jsou:

(a) Systém nahrávání (ReDat) – provázání s hlasovými záznamy, podkladová data pro identifikaci a lokalizaci

(b) Telefonní ústředna – identifikace a lokalizace hovorů

(c) RUIAN – hlavní registr adres pro IS ZOS

(d) Systém pro sledování vozidel (AVL) – odesílání výzev k výjezdu včetně doplňkových informací, příjem statusů posádek

(e) Integrace telefonie a radiofonie – systém inteligentního ovládání telekomunikací pracoviště

(f) NIS IZS – předávání informací o výjezdu mezi složkami IZS

(3) IS ZOS si vyměňuje data s interními systémy ZZS pro podporu činnosti výjezdových skupin (sledování vozidel/výjezdových skupin, EKP, MZD).

(4) IS ZOS komunikuje s dalšími externími systémy:

(a) Info35/AML – využívání služby lokalizace podle telefonního čísla

(b) NSPTV NIS – předávání informací o výjezdu v rámci národního systému příjmu tísňových výzev

9.5. Technologické řešení IS ZOS

(1) Jádrem informačního systému ZOS jsou moduly informačního systému S.O.S., což je informační systém operačního střediska záchranné služby. K tomuto jádru jsou napojeny spolupracující moduly dalších subsystémů, které dohromady v komplexním řešení uspokojují požadavky ZZS KVK.

(2) Informační systém S.O.S. je postaven na databázové architektuře klient-server, klientem je aplikace vytvořená v prostředí Oracle Developer (Forms & Reports), na straně serveru je využíván databázový systém Oracle.

(3) U systému S.O.S je uplatněno:

(a) objektový model aplikace – systém S.O.S. důsledně odlišuje entity Událost, Výjezd a Pacient a umožňuje práci s relacemi mezi těmito entitami v korespondenci s realitou řešených událostí. Uživatelské GUI je koncipováno tak, aby se tyto vazby mezi uvedenými entitami prezentovaly dispečerům maximálně přehledným způsobem.

(b) integrace s GIS – modul Dispečer systému S.O.S. je plně integrován se systémy GIS.

(c) Integrace s vozidlovými jednotkami – modul Dispečer systému S.O.S. je již provozován v integraci s navigačním systémem a systémem pro sledování vozidel (AVL).

(4) Architektura pro provoz aplikace – databázová architektura a prostředí (databázový systém Oracle na serveru, Oracle Forms & Reports na klientech), kterou využívá informační systém S.O.S.

(5) Využití webových služeb – pro integraci s dalšími systémy a technologiemi zákazníka je využita především datová výměna uskutečňovaná pomocí webových služeb. Na straně subsystému ZOS je komunikace webovými službami zajištěna pomocí těchto prostředků:

(a) klientský přístup k webovým službám třetích stran je zajištěn přímým voláním webových služeb z databázového serveru subsystému ZOS (s využitím možností poskytovaných databázovým systémem)

(b) poskytování webových služeb subsystému ZOS je realizováno prostřednictvím standardních prostředků databázového systému Oracle (Database Native Web Services)

9.6. Administrace

(1) Administrace subsystému ZOS je prováděna následujícími prostředky:

(a) pomocí speciálního administrátorského modulu subsystému ZOS (správa uživatelů a základních číselníků)

(b) pomocí speciálních administrátorských formulářů přímo v dispečerském systému (nastavení způsobu práce dispečerského systému)

(2) K administraci subsystému ZOS je obecně oprávněn uživatel s rolí „supervizor“, k méně závažným konfiguračním záležitostem jsou oprávněni i uživatelé s rolí „vedoucí dispečer“ (například nastavení aktuální nabídky sledovaných skupin událostí, přepínání rolí pracoviště call-taker/dispečer).

(3) Administrace se týká především následujících oblastí:

(a) správa uživatelů a jejich oprávnění

(b) správa číselníku vozů, správa číselníku výjezdových stanovišť

(c) správa konfiguračních schémat

(d) konfigurace sledovaných skupin událostí a dalších konfiguračních atributů událostí

(e) konfigurace vizuálních atributů ovlivňujících GUI systému

(f) správa parametrů stanic

(4) Při běžném provozu má oprávněná osoba (vedoucí dispečer nebo supervizor) možnost zasahovat do následujících nastavení:

(a) přepínání role call-taker / dispečer pro jednotlivá pracoviště

(b) Nastavení zvukových upozornění dispečinku

9.7. Detailní popis modulu Základna

(1) V následujících kapitolách je popisován modul SOS Základna. Jeho nasazení na PC výjezdových stanovišť umožňuje přihlašování a odhlašování posádek do Směn bez nutnosti zatěžovat touto činností operátory KZOS.

(2) Na výjezdových základnách jsou posádkami výjezdových skupin přihlašovány (a odhlašovány) výjezdové skupiny do služby na základě evidence VS spravované modulem Evidence výjezdových skupin.

(3) Při nástupu do služby se výjezdová skupina z aplikace přihlásí do služby (dá se k dispozici dispečerům), při ukončování směny je výjezdová skupina odhlašována. Systém umožňuje pracovníkům výjezdových základen měnit složení posádek VS během směny tak, aby odpovídalo skutečnému aktuálnímu stavu výjezdových skupin (změna složení posádky, výměna vozu).

(4) Automatické odhlášení předchozí VS při přihlášení nové VS je možné. Ruční odhlášení VS (např. nenásleduje-li další směna) je rovněž možné (obojí závisí na konfiguraci modulu Základna).

(5) Uživatelé modulu Základna – uživateli modulu Základna jsou uživatelé zaregistrovaní v systému SOS (posádky a pracovníci na základnách ZZS KVK) s přístupovými právy typu Základna.

(6) Modul Základna je jedním z řady modulů informačního systému zdravotnické záchranné služby S.O.S. a podobně jako ostatní moduly pracuje s daty v centrální databázi systému.

(7) Modul Základna poskytuje funkcionalitu běžně využívanou ZZS KVK:

(a) Přihlášení posádek a VS do služby / odhlášení

(b) Změna ve VS (složení posádky nebo změna vozidla)

(c) Zobrazení dostupných VS na základně

(d) Zobrazení událostí obsluhovaných VS ze základny

(8) Mimo toto může modul poskytovat i další funkcionalitu:

(a) Zobrazení a potvrzení výzvy k výjezdu

(b) Tisk výjezdového lístku

(9) Modul Základna má integrované technologické rozhraní pro:

(10) Přeříkávání hlasových výzev

(a) Signalizaci dostupnosti základny do dispečinku ZOS

(b) Tisk výjezdového lístku na tiskárně základnového PC při obdržení výzvy

(11) Na každém základnovém PC může běžet nepřetržitě aplikace Základna – zajišťuje přijímání výzev k výjezdu.

(12) Tento běh základny nevyžaduje přihlášení konkrétního uživatele – může fungovat i po odhlášení uživatele, který modul Základna po svém přihlášení spustil.

(13) Pokud dojde k odpojení PC od sítě nebo k vypnutí modulu Základna, je na problém graficky upozorněn dispečink KZOS červeným podbarvením základny ve stripech Výjezdových skupin.

(14) Hlavní podmínkou provozu je existující konektivita do sítě, přes kterou je prováděno přihlášení do systému a následně přihlášení/střídání/odhlášení směn, možný i příjem výzev k výjezdu a potvrzování těchto výzev. Dále musí být správně nastaveny konfigurační parametry PC pro SOS zajišťující unikátní identifikace základny pro IS ZOS (SOS).

(15) Modul Základna může být spuštěn na daném základnovém PC i bez přihlášení konkrétního uživatele.

(16) Hlavní podmínkou provozu je existující konektivita do sítě, přes kterou je prováděno přihlášení do systému a následně přihlášení/střídání/odhlášení směn, možný i příjem výzev k výjezdu a potvrzování těchto výzev. Dále musí být správně nastaveny konfigurační parametry PC pro SOS zajišťující unikátní identifikace základny pro IS ZOS (SOS).

(17) Nastavení pro funkcionalitu modulu Základna je prováděno správcem ve formulářích pro správou číselníků SOS pro oblast Základna a přidělováním přístupových práv uživatelů pro přihlašování a odhlašování posádek.

(18) Mimo to lze konfigurovat parametry základnové stanice:

(a) Režim Prohlížení/ Příjem výzvy

(b) Volitelný Tisk na tiskárnu

(c) Příslušnost k okresu

(d) Zobrazení prostředků z jiné základny

(e) Povolení možnosti přihlašovat nové posádky, odhlašovat posádky, střídat posádky.

10. Geografický informační systém (GIS)

10.1. Uživatelé GIS

(1) Uživatelé aplikace GIS jsou primárně pracovníci dispečinku, kteří aktivně využívají propojení GIS a IS ZOS. Uživatelé se přihlašují v IS ZOS a jejich role je nastavena v GIS. GIS využívá možnosti měnit roli uživateli (uživatel = pracoviště) dle přihlášení v IS ZOS. Na roli jsou nastavena uživatelská práva.

(2) Dalšími uživateli jsou uživatelé AVL v rámci ZZS mimo IS ZOS.

10.2. Procesní a funkční oblasti

(1) Veškerá funkčnost GIS probíhá odděleně ve třech úrovních/vrstvách:

(a) první vrstvu tvoří mapové podklady a mapová data.

(b) druhá vrstva slouží pro zobrazení vozidel, jejich polohy a vstupů.

(c) třetí vrstva je určena pro lokalizaci zájmových, adresních a jiných důležitých míst v mapě

(2) Proces integrace se SOS (IS ZOS) je řešen rovněž v několika rovinách:

(a) aktuálně řešené události jsou do mapy načítány skrz přímé připojení GIS do geograficky lokalizované DB SOS (IS ZOS) prostřednictvím databázového pohledu

(b) pro výměnu povelů a dat mezi subsystémy IS ZOS a GIS je využita technologie DB pipe

(c) pro předávání dat z fleetové části systému AVL do IS ZOS je využito připojení komunikační služby aplikačního serveru AVL do DB IS ZOS

(3) GIS klient obsahuje funkci vyhledávání v databázi adres a v databázi zájmových bodů. Fulltextové vyhledávání místa události je řešeno primárně v dispečerské aplikaci IS ZOS, ale je možné i v rámci GIS aplikace.

10.3. Uživatelské rozhraní

(1) Po spuštění aplikace GIS jsou defaultně zobrazeny panely Vozidla, Události, Textové zprávy, Detail vozidla a Přehledová mapa. Všechny panely lze otevírat a zavírat pomocí tlačítek v hlavním menu.

(2) Pokud na jedné stanici otevřete dva a více GIS klientů, se SOS komunikuje vždy pouze první otevřený. Další instance se přihlašují pod uživatelem „GisViewer“, který se SOS nekomunikuje a má právo pouze na sledování situace. Pokud zavřete klienta, který komunikuje se SOS, pro jeho opětovné otevření musíte nejdříve pozavírat všechny instance, které sledují situaci (uživatel „GisViewer“).

(3) Ovládací prvky

(a) Spodní lišta neustále zobrazuje souřadnice kurzoru myši v mapě, po zastavení kurzoru myši je následně zobrazen také popis lokality.

(b) Ve spodní liště je dále zobrazeno upozornění na nevyřešené úkoly, pracoviště, kde je GIS spuštěn (v nastavení uživatelů je totožné s uživatelem), připojená DB a aktuální čas.

(c) Mapou je možné posouvat pomocí myši, kliknutím a podržením levého tlačítka myši nad mapou a následným pohybem. Pro změnu měřítka mapy také slouží posuvník v horní části aplikace.

(4) Panel Najít dle souřadnic

(a) Aplikace umožňuje vyhledat místo zadáním souřadnic. Panel pro hledání souřadnic se spouští kliknutím na ikonu „Najít dle souřadnic“.

(b) Souřadnice lze zadávat ve formátu WGS-84 ve stupních, minutách a vteřinách, nebo ve formátu S-JTSK. V panelu probíhá přepočítávání mezi zvolenými formáty. Pro vyhledání místa na mapě je nutné zadat zeměpisnou šířku a délku.

(5) Přehledová mapa

(a) Panel s přehledovou mapou je standardně zobrazen v pravé části aplikace. Tento panel je možné zavírat. Za pomocí tlačítka „Přehledová mapa“ na nástrojové liště je možné panel otevřít.

(b) Přehledová mapa usnadňuje orientaci v hlavním mapovém okně. Poskytuje širší náhled na aktuálně zvolené území. Červený obdélník vyznačuje zobrazený výřez hlavní mapy. Posunem výřezu v hlavním mapovém okně se automaticky přesouvá i tento obdélník v přehledové mapě, ale platí to také naopak. Je tedy možné myší posouvat obdélník v přehledové mapě a tím pádem měnit výřez zobrazený v hlavní mapě. Obdélník lze přesouvat dvěma způsoby. Levým tlačítek myši ho uchopíte a posunete na požadované místo nebo chvíli podržíte levé tlačítko myši na místě, kam si přejete obdélník posunout.

(6) Panel Vozidla

(a) Panel vozidel poskytuje přehled o vozidlech. Informuje o tom, zda je vozidlo ve službě. Je zde také zobrazen typ výjezdové skupiny a stav. V neposlední řadě je zde i informace o aktuální poloze a události, ke které je výjezdová skupina přiřazena.

(b) V horní části panelu je zobrazen počet vozidel, v závorce je pak uvedeno, kolik vozidel je aktuálně viditelných v mapě. Je-li aktivní filtr, je pomocí lomítka uvedeno, kolik vozidel je vyfiltrováno z celkového počtu vozidel v panelu.

(c) Seznam vozidel je koncipován jako tabulkový seznam, který umožňuje řazení a filtraci dle zobrazených položek ve sloupcích. Data ze seznamu vozidel je možné exportovat do dalších aplikací (Excel, Word, Poznámkový blok).

(d) Volby určují, které objekty mají být zobrazeny, případně které objekty mají být použity pro zvolení optimálního měřítka mapy tak, aby byly viditelné.

(7) Panel událostí

(a) Panel událostí poskytuje přehledné zobrazení informací o všech evidovaných událostech. V seznamu se nachází informace o čísle, naléhavosti, stavu, klasifikaci a lokalitě události. Dále se zde zobrazují čísla přiřazených posádek k dané události.

(b) V horní části panelu je zobrazen počet událostí, v závorce je pak uvedeno, kolik událostí je aktuálně viditelných v mapě. Je-li aktivní filtr, je pomocí lomítka uvedeno, kolik událostí je vyfiltrováno z celkového počtu v panelu.

(c) Seznam událostí je koncipován jako tabulkový seznam, který umožňuje řazení a filtraci dle zobrazených položek ve sloupcích. Data ze seznamu událostí je možné exportovat do dalších aplikací (Excel, Word, Poznámkový blok).

(d) Ikony v horní části panelu určují, jaké události ze seznamu mají být viditelné na mapě.

(8) Panel Viditelné objekty v mapě

(a) Spouští se z panelu vozidel kliknutím na ikonu „Viditelné objekty v mapě“. Jsou zde vypsána všechna vozidla a události, která jsou aktuálně viditelná v mapě. V tomto panelu také funguje otevření kontextového menu přes pravé tlačítko myši, pro práci s jednotlivými vozidly a událostmi, stejně jako na ikonkách v mapě.

(9) Nejbližší vozidla

(a) Funkce zobrazuje nejbližší vozidla ke zvolenému místu včetně doby dojezdu. Ikona „Nejbližší vozidla“ se nachází na panelu vozidel. Po jejím stisknutí určíte pravým tlačítkem myši na mapě bod, ke kterému chcete nalézt nejbližší vozidla. V seznamu vozidel a na mapě se vyfiltrují nejbližší vozidla. Černým křížkem je na mapě označen určený bod. Zároveň se otevře panel Nejbližší vozidla, kde jsou vypsány doby dojezdu u jednotlivých vozidel.

(10) Hledání adres

(a) Panel pro vyhledání adres se spouští kliknutím na ikonu „Hledat místa“. V poli Kraj se určuje, v jakém kraji má vyhledávání adresy proběhnout, defaultně je nastaven „K Karlovarský kraj“.

(b) Ve vyhledávacím poli funguje tzv. fulltextové vyhledávání. Zadáte název nebo část hledané adresy a potvrdíte enterem. V seznamu se zobrazí všechny odpovídající záznamy. Do vyhledávacího pole je nutné zadat minimálně dva znaky.

(c) Pokud zaškrtnete pole „Pouze obce a části obcí“, vyhledávání je omezeno pouze na názvy obcí a jejich částí.

(d) Dvojklikem na adresu se mapa vycentruje nad dané místo a zobrazí se modrá navigační vlajka.

(11) Uživatelské oblasti

(a) Pomocí definice uživatelských oblastí je možné generovat vlastní textové a grafické informace o průjezdu vozidel známými oblastmi.

(b) Panel pro uživatelské oblasti se spouští kliknutím na ikonu „Uživatelské oblasti“. Zde je možné vytvářet různé typy oblastí. Každou oblast je dále možné přiřadit k určité kategorii oblastí a vytvářet tak přehlednou strukturu oblastí s podobnými vlastnostmi.

(12) Panel vyhledávání v POI

(a) Nejprve je nutné vybrat kategorii, ve které má probíhat hledání. Pro upřesnění je možné zvolit také podkategorii. Podle zvolené kategorie se určuje typ vyhledávání a to buď fulltextové, nebo intervalové (standardně je nastaveno fulltextové vyhledávání).

(b) Intervalové vyhledávání je nastaveno ve vlastnostech kategorie podle stanovených pravidel tam, kde je možno interval definovat.

(c) Fulltextové vyhledávání funguje v kategoriích, jejichž POI nejsou. Pokud zaškrtnete pole „Celá slova“, vyhledávání funguje pouze po celých slovech v názvech POI.

(13) Panel Detail POI - po vyhledání POI dojde také k otevření panelu „Detail POI“ na pravé straně aplikace. Tento panel obsahuje veškeré informace o vybraném POI. Panel zobrazuje vždy aktuálně označený POI ze seznamu vyhledaných POI.

(14) Panel POI - kategorie - ve stromovém zobrazení jsou vypsány všechny kategorie a podkategorie POI nacházející se v databázi. Zaškrtnutím kategorie (případně podkategorie) dojde k zobrazení všech POI, které tam náleží, do mapy.

(15) Témata - v tématech se nastavuje posloupnost mapových podkladů při zoomování. Téma je možné zvolit, stejně jako mapový podklad, vpravo od posuvníku na horní nástrojové liště. Uživatel má buď vybrán konkrétní mapový podklad, nebo téma. Dostupné mapové podklady jsou uvedeny v seznamu dle abecedy, témata jsou oddělena čárou. K jednotlivým mapovým vrstvám lze nadefinovat datové vrstvy (POI a uživatelské oblasti).

10.4. Integrované systémy a technologie

(1) Řešení je založené na osvědčené technologii OpenLayers, která je vyvíjena striktně dle standardů OGC (Open Geospatial Consortium) a je jádrem mnoha GIS systémů a mapových aplikací po celém světě.

(2) Integrace - systém je úzce integrovaný se SOS (IS ZOS) a nevyžaduje po obsluze suplovat přenášení dat mezi oběma systémy zbytečnými manuálními zásahy.

(3) Nad mapovým podkladem probíhá, v jednotlivých vrstvách:

(a) zobrazení polohy a stavu vozidel

(b) poloha a stav řešených událostí

(c) zobrazení lokalizovaných míst v mapě prostřednictvím nástroje hledání či jiným způsobem prostřednictvím ZOS

10.5. Technologické řešení GIS

(1) Systém je koncipován jako systém pro podporu rozhodování a rozšiřuje pracovníkům dispečinku možnosti dispečerské aplikace SOS (IS ZOS) o práci s mapovým podkladem. Taktéž zajišťuje vizualizaci geograficky orientovaných dat a zobrazení fleetových a telematických informací z vozidel ZZS.

(2) Aplikace GIS jsou jak desktopové aplikace kompatibilní se standardy OGC, tak webové aplikace.

(3) Co se týče fleetových a telematických dat, je systém vystavěn nad robustním DB strojem MS SQL server 2008 R2/2012.

(4) Vizualizace vozidel, resp. výjezdních skupin je nativní částí systému AVL a nevyžaduje interface na jiný subsystém.

10.6. Administrace

(1) Pro konfiguraci GIS je primárně určena konzole serveru aplikace, většina nastavení je možná v rámci klienta dle nastavení práv.

(2) Instalace všech komponent systému je řešena instalačním programem se standardním průvodcem. Aktualizace je řešena automatickou kontrolou aktuálnosti verze při startu aplikace a následným stažením aktualizačního balíčku z umístění ve sdílené složce v síti LAN. Uživatel je v průběhu aktualizace přehledně informován o probíhající aktualizaci.

11. Informační systém pro sledování vozidel (AVL)

(1) Pro sledování vozidel je určena aplikace Fleetware, jejíž uživatelé jsou primárně pracovníci, kteří spravují vozidla (nastavují vlastnosti vozidel, sledují spotřebu PHM, schvalují jízdy) a nastavují práva uživatelům Fleetware a modulu Kniha jízd. Každý uživatel Fleetware má své vlastní jméno a heslo, uživatelům je možno nastavit stejné oprávnění pomocí zařazení do role.

11.1. Uživatelské rozhraní

(1) Klient je rozdělen na jednotlivé pohledy, které umožňují různé druhy práce uživatele.

(2) On-line pohled klienta umožňuje zobrazování stavu vozového parku v reálném čase (tzv. real-time tracking).

(3) Off-line pohled slouží k detailnímu prohlížení jízd a jejich trajektorií pomocí přehrávače jízd ve kterém je možné jak plynulé přehrávání, tak také krokování či zrychlené posuvy vpřed a vzad. Samozřejmostí je časová osa s detailním průběhem rychlosti vozidla.

(4) Aplikace také umožňuje a obsahuje bohatou škálu tiskových výstupů jejichž organizace je vyřešena pomocí přehledných průvodců.

11.2. Technologické řešení

(1) Software systému Fleetware je založen na technologii Klient – Server a databázovém systému MS SQL. Díky těmto technologiím aplikace umožňuje stabilní provoz v náročném prostředí dispečinku ZZS.

11.3. Administrace

(1) Pro konfiguraci Fleetware je primárně určena konzole serveru aplikace, většina nastavení je možná v rámci klienta Fleetware dle nastavení práv.

(2) Instalace všech komponent systému Fleetware je řešena instalačním programem se standardním průvodcem. Aktualizace je řešena automatickou kontrolou aktuálnosti verze při startu aplikace a následným stažením aktualizačního balíčku z umístění ve sdílené složce v síti LAN. Uživatel je v průběhu aktualizace přehledně informován o probíhající aktualizaci.

12. Navigační software pro posádky vozidel

(1) ZZS KVK používá pro příjem výzev posádkou vozidel a jejich následného navigování na místo zásahu včetně evidence statusů posádky specializovaný navigační software CarPC, výrobce Fleetware s.r.o. Navigační software je provozován na tabletech Samsung a průmyslový tablet 7145 s operačním systémem Android. Serverová část využívá databázový server s DB SQL.

12.1. Základní funkcionality

(1) Příjem a potvrzení výzev k výjezdu posádkou vozidla

(2) Zadávání statusů posádky na navigačním tabletu na záložce Statusy

(a) Pro potvrzení statusu musí uživatel na daném statusu podržet prst cca 3 sekundy (ochrana proti náhodnému stisknutí statusu). Po stisknutí uslyší uživatel krátký oznamovací tón odeslání statusu na server. Po potvrzení přijetí stavu vozidla na serveru se odeslaný status podbarví a také nový stav zahlásí.

(b) Software podporuje změnu stavu vozidla i z externího zdroje (např. změnu způsobenou na dispečinku).

(c) Software umožňuje odeslání předdefinovaných statusů.

(3) Přijímání a zobrazování textových zpráv ze ZOS

(4) zobrazení dalších posádek na stejném zásahu

(5) Doručení cíle od dispečerky se zobrazením cíle v mapě nebo volitelně automatické spuštění navigace.

12.2. Uživatelé

(1) Uživateli navigačního SW jsou všechny posádky RLP/RZP.

12.3. Integrované systémy a technologie

(1) Klientská aplikace instalovaná na vozidlových tabletech obousměrně datově komunikuje přes fleetware komunikační server a rozhraní v něm implementované se systémem IS ZOS. Největší část vyměňovaných dat jsou informace o výjezdech (příjem výzvy posádkou vozidla, příjem cíle zásahu), status posádky (na výjezdu, na příjmu atd.), textové doplňující informace ze ZOS.

(2) Pro příjem výzvy s místem požadovaného zásahu, její aktualizaci, zasílám statusů posádky, příjem textových zpráv ze ZOS do navigačního tabletu je potřeba datová konektivita s komunikačním serverem (zajišťuje ZZS samostatně).

13. Mobilní zadávání dat (MZD)

(1) Mobilní zadávání dat (MZD) slouží pro podporu zadávání dat o výjezdech a pacientech, získaných v rámci výjezdu k řešeným událostem včetně integrace na další subsystémy celého IS ZZS KVK. Tento informační systém jako součást komplexního řešení IS ZZS KVK a zajišťuje mobilní zadávání dat lékaři a záchranáři v terénu (mobilní klient na tabletech – MZD).

(2) Účelem subsystému pro mobilní zadávání dat o pacientech je odstranění nutnosti ručního přepisování dat, nečitelnosti parere, zajištění kompletní administrativy již v rámci výjezdu, kvalita a úplnost zadávaných dat (aplikací kontrolních mechanismů).

(3) Obecné vlastnosti MZD jsou:

(a) uživatelsky jednoduchá obsluha, jednotné uživatelské rozhraní.

(b) ergonomické zobrazení – vhodná velikost a barevné provedení uživatelského interface.

(c) omezení důsledků lidské chyby – dodržení časových posloupností a zákonitostí vyplňování pro vyloučení nepravděpodobných nebo nemožných operací.

(d) oddělený způsob (rozsahu) zadávaných dat pro lékaře a pro záchranáře včetně datového setu.

(e) propojení se systémem operačního řízení (IS ZOS) a předávání dat tak, by docházelo k maximálnímu vytěžení dat mezi systémy v rámci IS ZOS.

(f) tisk parere – z důvodu dokladování a archivace je tento kompletní záznam tištěn a dlouhodobě uložen, tj. nejedná se o plnohodnotnou elektronizaci celého procesu.

(g) zabezpečení systému prostředky pro zabránění neoprávněného čtení a manipulaci s daty

(h) lokální ukládání dat na pevný disk mobilního zařízení (tabletu) nebo paměťové médium je chráněno proti neoprávněnému přístupu k datům pacienta.

13.1. Základní funkcionality

(1) Převzetí a potvrzení výzvy – výzva vzniká v IS ZOS zadáním dispečera a MZD tuto výzvu včetně základních atributů přebírá a zobrazuje posádce.

(2) Vyplnění a tisk a záznamu o výjezdu – z uživatelského pohledu MZD zabezpečuje podporu pro vyplnění záznamu o výjezdu na mobilním zařízení a na stacionárním PC na výjezdové základně Výstupem je vytištěný papírový formulář a centrálně uložená data v IS pro další využití.

(3) Vytváření Protokolu o ohledání zemřelého.

(4) Uložení a poskytování dat o výjezdu – všechna zadaná data zůstávají k dispozici k pozdějšímu nahlížení (ne editaci) a k exportu do systému EKP (elektronická karta pacienta), který zajišťuje jejich další zpracování a tvorbu pokladů například dávek pro pojišťovny. Stacionární zadávání dat zajišťuje úpravu dat v rozsahu tak, aby nebylo možné rozporovat předanou a vytištěnou kartu pacienta. V systému EKP je prováděno další zpracování a vyhodnocování dat o výjezdech včetně exportu.

(5) Integrace s monitorem/defibrilátorem LifePak. Integrace s monitorem/defibrilátorem tak, aby bylo možné zobrazit/načíst křivku EKG do mobilního prostředku (tabletu) a přiřadit takovou informaci do karty o výjezdu.

(6) Hlavní vstup dat do systému je výzva převzatá z IS ZOS a ruční vstup pomocí mobilních klientských stanic.

(7) Aplikace zajišťuje sledování stavů dokladu dle úrovně vyplnění a dalšího zpracování (Editace, uzavřen, kontrolován, vykázán, nepřijatý, opravený, mimo dávky, storno, předaný, faktura, přímá platba) a označení dokladů u kterých probíhá dohledání potřebných údajů a nevyúčtovatelných dokladů.

(8) Reporty a statistiky – v rozsahu současných statistik IS ZZS.

(9) Exporty hlavních datových souborů (hlášení, výjezdy, pacienti) do Excelu.

13.2. Detailní funkcionality

(1) Kompatibilní datový model se systémem stacionárního sběru dat – EKP Mobilní zadávání dat umožňuje plnohodnotný vstup dat kompatibilních s EKP.

(2) Standardizace pořízené zdravotní dokumentace – aplikace informuje uživatele o validitě zadaných dat, zda splňují stanovené minimum požadovaných informací, které odpovídají definovaným kritériím závažnosti postižení pacienta (např. NACA skóre). Aplikace nesmí umožnit zadání nesmyslných dat (kontrola rozsahu, posloupnosti apod.) s výrazným upozorněním na chybně zadaná data.

(3) Zajištění tisku zadaných dat v terénu v podobě tzv. parere prostřednictvím mobilní tiskárny přímo propojené s počítačem v rámci zástavby případně s využitím bezdrátové Bluetooth technologie.

(4) Zajištění tisku na mobilní tiskárně ve vozidle.

(5) Ergonomické uživatelské rozhraní s podporou Tablet PC funkčností – snadné zadání informací, maximální podpora Tablet PC funkcionality v uživatelském rozhraní. UI aplikace přizpůsobené workflow výjezdové skupiny (RLP, RZP).

(a) Ovládání pomocí dotykového displeje a klávesnice

(b) Dostatečná velikost fontů

(c) Logický postup zadávání dat

(d) Grafické rozhraní odpovídá logickému postupu vyplňování

(e) Důraz na ergonomii zadávání ve ztížených podmínkách

(6) Komunikace klienta s aplikačním serverem po zabezpečeném kanálu.

(7) Aplikace umožňuje zadání informací v terénu nezávisle na dostupnosti připojení s centrálním systémem. V případě výpadku připojení je možnost zadat informace o výjezdu a pořídit výjezdovou kartu.

(8) Aplikace obdrží nejpozději do 3 min od přijetí výzvy posádkou vybrané informace o výzvě ze systému IS ZOS (podmínkou je dostupný mobilní internet).

(9) V případě uzavření záznamu o výjezdu ze strany uživatele je centrální systém aktualizován nejpozději do 3 min. (podmínkou je dostupný mobilní internet)

(10) Správa číselníků mobilních terminálů – aplikace umožňuje za provozu synchronizaci číselníku v terénu se serverovými verzemi. Pokud je k dispozici mobilní internet, pak po změně serverové verze číselníků se změny promítnou nejpozději do 12 hod do všech používaných mobilních terminál (podmínkou je, že budou v online módu).

(11) Automatické aktualizace – aplikační SW mobilních terminálů umožňuje aktualizaci sebe sama.

(12) Aplikace umožňuje vzdálené smazání veškerých citlivých dat. (podmínkou je dostupný mobilní internet)

(13) Mobilní terminál společně s aplikací by měl být uzavřený jednoúčelový systém.

(14) Dohled a správa mobilního klientského aplikačního SW – systém umožňuje vzdálený přístup do log souborů MZD a tyto logy vzdáleně importovat na server pro další vyhodnocení.

(15) Velké zobrazení, intuitivní funkce, zajištění vstupu kdekoliv v průběhu zapisování, rychlé zkopírování známých dat z jiných databází (např. IS ZOS) automaticky, porovnání s databází (zda již stejného pacienta neobsahuje), fulltextové vyhledávání. Instalace SW pro mobilní zadávání dat do nového tabletu bude vlastními silami a prostředky ZZS KVK.

(16) Přístup jen pod přiděleným jménem a heslem

(17) Zabezpečení provozní správy a konfiguračního řízení – aktualizace SW jednotně a pravidelně na všech pracovištích, zajištění průkazného systému aktualizace a údržby SW.

(18) Z MZD lze tisknout „Záznam o výjezdu“, „List o prohlídce zemřelého“ (část A i B) a průvodní list k pitvě.

(19) Seznam uživatelů a práva uživatelů jsou automaticky synchronizovány každé ráno v 5:00 ze systému IS ZOS. Tento seznam lze editovat v administrátorské konzoli, včetně oprávnění.

(20) Práci na tabletu pomocí dotykového pera nebo dotyku.

13.3. Integrované systémy a technologie

(1) Systémy EKP a MZD obousměrně datově komunikují se systémem IS ZOS. Největší část vyměňovaných dat jsou informace o výjezdech, pacientech a uživatelích. Častěji se měnící číselníky (léky, materiály atd.) se automaticky synchronizují každé ráno v 5:00 ze systému IS ZOS. Lze se dotazovat na interní historii pacienta. Tato historie se bere z databáze již proběhlých výjezdů, které jsou zaznamenány v EKP.

(2) Na všech tabletech nainstalován softwarový interface umožňující přenos dat z přístroje LIFEPAK na tablet a následný import těchto dat do aplikace MZD.

(3) Pro příjem výzvy, její aktualizaci a její následné uzavření je potřeba datová konektivita s aplikačním serverem (zajišťuje objednatel). V průběhu práce lze na tabletu pracovat v režimu off-line. Pokud uživatel výzvu uzavře a tablet nebude mít k dispozici konektivitu, data se uloží na HDD a data odešle ve chvíli, kdy konektivitu naváže. Datové SIM karty pro připojená tabletů v terénu zajišťuje objednatel.

(4) Systém lze administrovat pomocí rozhraní přístupného pomocí webového prohlížeče. Toto rozhraní umožňuje editaci všech číselníků, zobrazuje aktuální stav připojení jednotlivých klientů a jejich historii, historii výzev atd.

14. Elektronická karta pacienta (EKP)

Elektronická karta pacienta (dále jen „EKP“) je označení ZZS pro subsystém IS pro zadávání dat na výjezdových základnách.

14.1. Základní funkcionality

(1) Systém zajišťuje příjem výzev k výjezdu na výjezdové základně.

(2) Systém zajišťuje editace dat výjezdů a pacientů potřebných pro účtování a pro statistické výstupy.

(3) Systém zjišťuje zadání dat o pacientovi ve stejném rozsahu jako v mobilním klientu, vyjma dat z externích zařízení a vyjma grafických zadání.

(4) Systém vede evidence výkonů a podaných léků a zvlášť účtovaného materiálu.

(5) Zadávání dat je funkčně podobné s MZD, vyjma napojení na externí zařízení a import dat z těchto zařízení (monitor/defibrilátor).

(6) Uživatelské rozhraní ve formě tenkého klienta na výjezdových základnách.

(7) Aplikace zajišťuje sledování stavů dokladu dle úrovně vyplnění a dalšího zpracování (Editace, uzavřen, kontrolován, vykázán, nepřijatý, opravený, mimo dávky, storno, předaný, faktura, přímá platba) a označení dokladů u kterých probíhá dohledání potřebných údajů a neúčtovatelných dokladů.

(8) Reporty a statistiky systému jsou v rozsahu současných statistik SOS.

(9) Hlavní datové soubory (hlášení, výjezdy, pacienti) lze exportovat do Excelu.

14.2. Detailní funkcionality

(1) Standardizace pořízené zdravotní dokumentace – aplikace informuje uživatele o validitě zadaných dat, zda splňují stanovené minimum požadovaných informací, které odpovídají definovaným kritériím závažnosti postižení pacienta (např. NACA skóre). Aplikace nesmí umožnit zadání nesmyslných dat (kontrola rozsahu, posloupnosti apod.) s výrazným upozorněním na chybně zadaná data.

(2) Zajistit tisk Záznamu o výjezdu ZZS – tisk zadaných dat do formátu PDF.

(3) Ergonomické uživatelské rozhraní – snadné zadání informací, maximální podpora funkcionality v uživatelském rozhraní.

- (a) Logický postup zadávání dat
- (b) Grafické rozhraní odpovídá logickému postupu vyplňování RLP i RZP
- (c) Důraz na ergonomii zadávání dat

(4) Příjem výzev z IS ZOS – aplikace obdrží nejpozději do 3 min od přijetí výzvy posádkou vybrané informace o výzvě z IS ZOS.

(5) Příjem informací o výjezdu z mobilních terminálů do centrálního systému – v případě uzavření záznamu o výjezdu ze strany uživatele je centrální systém aktualizován nejpozději do 3 min. při funkčnosti spojení s aplikačním serverem

(6) Snadná obsluha a ergonomie.

(7) Velké zobrazení, intuitivní funkce, možnost vstupu kdekoliv v průběhu zapisování, rychlé zkopírování známých dat z jiných databází (např. IS ZOS) automaticky, porovnání s databází (zda již stejného pacienta neobsahuje), fulltextové vyhledávání.

(8) Přístup jen pro oprávněné uživatele pomocí jména a hesla.

(9) Řešení obsahuje nástroj na verifikaci poskytnutých dokladů pacienta tak, aby mohlo proběhnout následné vyúčtování.

(10) Seznam uživatelů a práva uživatelů jsou automaticky synchronizovány každé ráno v 5:00 ze systému IS ZOS. Tento seznam lze editovat v administrátorské konzoli, včetně oprávnění.

(11) Data jsou zadávána vyplňováním textových polí, rolovacích menu, výběrem z číselníků, nebo výběrových položek.

(12) Datový set EKP je stejný jako datový set MZD. Všechny položky z MZD jsou obsažené i v EKP. EKP je pouze uzpůsobeno pro práci na PC za pomoci klávesnice a myši.

(13) Formuláře – z EKP lze tisknout „Záznam o výjezdu“, „List o prohlídce zemřelého“ (část A i B) a „Průvodní list k pitvě“.

14.3. Integrované systémy a technologie

(1) Systémy EKP a MZD obousměrně datově komunikují se systémem IS ZOS. Největší část vyměňovaných dat jsou informace o výjezdech, pacientech a uživatelích. Častěji se měnící číselníky (léky, materiály atd.) se automaticky synchronizují každé ráno v 5:00 ze systému IS ZOS. Lze se dotazovat na interní historii pacienta. Tato historie se bere z databáze již proběhlých výjezdů, které jsou zaznamenány v EKP.

(2) Pro provoz EKP je nezbytně nutná existující konektivita do sítě, přes kterou se lze spojit s aplikační a databázovým serverem.

(3) Systém lze administrovat pomocí rozhraní přístupného pomocí webového prohlížeče. Toto rozhraní umožňuje editaci všech číselníků, zobrazuje aktuální stav připojení jednotlivých klientů a jejich historii, historii výzev atd.

15. Pojišťovna

(1) Modul Pojišťovna (POJ) implementuje následující funkcionality:

(a) Provádění kontroly úplnosti dokladů pacientů před jejich vyúčtováním – nástroj pro provedení automatické hromadné kontroly dokladů za zadané období, výsledkem kontroly je označení úspěšně zkontrolovaných dokladů pro jejich následné předávání pojišťovnám.

(b) Systém podporuje datové předávání dokladů pojišťovnám v souladu se standardy VZP.

(c) Systém podporuje údržbu potřebných číselníků VZP, importy číselníků.

(d) Do systému je integrováno B2B rozhraní VZP – vybrané služby uvedené dále v textu.

15.1. Základní funkcionality

(1) Kontrola dokladů – nástroj pro provedení automatické hromadné kontroly dokladů za zadané období, výsledkem kontroly je označení úspěšně zkontrolovaných dokladů pro jejich následné předávání pojišťovnám.

(2) Pro zamezení zbytečně chybnému předávání dat zajistí systém provést předběžnou kontrolu příslušnosti pacientů jednotlivým zdravotním pojišťovnám pomocí portálu VZP.

(3) Nástroj pro kontrolu příslušnosti pacientů k jednotlivým zdravotním pojišťovnám pomocí portálu VZP.

(4) Systém zajišťuje interní komunikaci mezi kontrolním pracovištěm a pracovišti na výjezdových základnách, pomocí níž budou řešeny problematické doklady (dotazy a výzvy k doplnění dat ze strany kontrolního pracoviště, následné doplnění dat a zpětné odpovědi do kontrolního pracoviště).

(5) Pro vlastní předávání dat pojišťovnám systém splňuje všechny potřebné standardy VZP. Data pacientů jsou pojišťovnám předávány v dávkách dokladů, které systém generuje. Aplikace následně funkcionalitou opravuje chybné doklady a vytváří opravné dávky – pokud je doklad pojišťovnou odmítnut, uživatel označí doklad jako nepřijatý a po následné opravě tohoto dokladu zařadí doklad pro následné generování opravných dávek. Aplikace zajišťuje sledování stavů dokladu dle úrovně vyplnění a dalšího zpracování (Editace, uzavřen, kontrolován, vykázán, nepřijatý, opravený, mimo dávky, storno, předaný, faktura, přímá platba) a označení dokladů u kterých probíhá dohledání potřebných údajů a neúčtovatelných dokladů.

(6) Aplikace automaticky vytváří průvodní listy k dávkám v souladu se standardy VZP.

(7) Pro správné účtování je systém vybaven aktuálními číselníky pojišťoven, pro zpětné účtování má k dispozici i historické informace o stavu těchto číselníků. Kromě přímé údržby číselníků je systém vybaven importem číselníků VZP, především číselníků léků a zdravotnického materiálu.

(8) Kromě hromadného účtování dokladů pojišťovnám je systém vybaven i zajištěním jednotlivého účtování dokladů, a to formou vytváření podkladů pro faktury jednotlivým pacientům.

(9) Dále systém zajišťuje registraci cizinců EU u pojišťovny a sledování stavu registrace a vyúčtování dokladů takovýchto pacientů. Upozorňuje na další výkony k pacientovi v procesu registrace.

15.2. Detailní funkcionality

(1) Kontrola dokladů – nástroj pro provedení automatické hromadné kontroly dokladů za zadané období, výsledkem kontroly je označení úspěšně zkontrolovaných dokladů pro jejich následné předávání pojišťovnám.

(2) Kontrola pomocí portálu VZP – nástroj pro kontrolu příslušnosti pacientů k jednotlivým zdravotním pojišťovnám pomocí portálu VZP.

(3) Modul pojišťovna umožňuje generovat dávky dokladů o pacientech (a to jak dávky původní, tak dávky opravné) a předávat je pojišťovnám.

(4) Systém splňuje všechny potřebné standardy a metodiky VZP

(5) Aplikace umožňuje opravovat chybné doklady a vytvářet opravné dávky – pokud je doklad pojišťovnou odmítnut, uživatel označí doklad jako nepřijatý a po následné opravě tohoto dokladu zařadí doklad pro následné generování opravných dávek.

(6) Systém umožňuje konfiguraci členění dávek pro pojišťovnu takovým způsobem, aby dávky odpovídaly podle potřeby okresům, výjezdovým stanovištím, typům výjezdů nebo kombinacím uvedeného.

(7) Korektní zpracování dokladů z výjezdů „rendez-vous“ systému.

(8) Pokud je k výjezdu přiřazeno více pacientů, je možné rozúčtování (rozdělení výkonů mezi pacienty).

(9) Subsystém automaticky generuje průvodní listy k dávkám v souladu se standardy VZP.

(10) Subsystém umožňuje přegenerování existující připravené dávky po provedení potřebných změn obsahu souvisejících číselníků.

(11) Subsystém umožňuje libovolné sdružování dávek do "disket" pro následné předání zdravotním pojišťovnám.

(12) Subsystém umožňuje automatického vytváření "disket" z dávek, které ještě nebyly zařazeny na diskety, a to podle volitelných kritérií (období, druh pojištění atd.).

(13) Subsystém umožňuje vytvoření statistického rozpisu obsahu diskety podle definovaných nákladových středisek.

(14) Pokud je doklad pojišťovnou odmítnut, uživatel označí doklad jako nepřijatý a po následné opravě tohoto dokladu zařadí doklad pro následné generování opravných dávek (nebo v případě potřeby pro generování původních dávek). Pokud je doklad pojišťovnou odmítnut, uživatel označí doklad jako nepřijatý a po následné opravě tohoto dokladu zařadí doklad pro následné generování opravných dávek (nebo v případě potřeby pro generování původních dávek).

(15) Správa číselníků pro účtování – subsystém umožňuje konfiguraci ohodnocení nasmlouvaných léků a materiálu s udržovaným historickým vývojem pro správné vykazování dokladů z určitého data, včetně možnosti individuální konfigurace pro jednotlivé pojišťovny.

(16) Konfigurace léků a materiálu – subsystém umožňuje konfiguraci ohodnocení nasmlouvaných léků a materiálu s udržovaným historickým vývojem pro správné vykazování dokladů z určitého data, včetně možnosti individuální konfigurace pro jednotlivé pojišťovny

(17) Konfigurace výkonů – subsystém umožňuje konfiguraci ohodnocení nasmlouvaných výkonů s udržovaným historickým vývojem pro správné vykazování dokladů z určitého data, včetně možnosti individuální konfigurace pro jednotlivé pojišťovny.

(18) Výše uvedené konfigurace mají možnost individuální konfigurace pro jednotlivé pojišťovny.

(19) IS podporuje import číselníků VZP, především číselník léků a zdravotnického materiálu.

(20) Integrace B2B rozhraní VZP – Stav pojištění – Systém umožňuje získat informaci, zda je pojištěnec se zadaným číslem pojištěnce pojištěn a u které pojišťovny.

(21) Integrace B2B rozhraní VZP – Průběh pojištění – systém umožňuje získat informaci, zda je pojištěnec se zadaným číslem pojištěnce pojištěn, u které pojišťovny a jaký má druh pojištění.

(22) Ověření platnosti průkazu pojištěnce (EHIC) – systém automaticky ověřuje platnost průkazu (EHIC) pro dané číslo průkazu a k danému datu.

(23) Systém vede evidence registrací cizinců EU.

(24) Systém rozúčtovává výkony na účetní střediska.

(25) Výstupy ze systému jsou statistiky a přehledy.

(26) Přístup uživatelů do modulu Pojišťovna je na základě práv, která lze nastavit v administrátorském rozhraní přístupného pomocí webového prohlížeče.

(27) Datový set modulu pojišťovna vychází z EKP a je rozšířen o položky nutné k účtování výjezdů vůči zdravotní pojišťovně.

15.3. Integrované systémy a technologie

(1) Modul pojišťovna je nainstalovaný na PC uživatele v podobě tlustého klienta. Data, se kterými modul pracuje, jsou uložena na databázovém serveru. Pro komunikaci s portálem VZP obsahuje modul Pojišťovna B2B rozhraní.

(2) Systém lze administrovat pomocí rozhraní přístupného pomocí webového prohlížeče. Toto rozhraní umožňuje krom jiného i editaci číselníků potřebných pro modul pojišťovna.

16. Elektronická kniha jízd (EKJ)

Modul Kniha jízd poskytuje přehled o jízdách vozidel ZZS KVK.

Převážná většina informací je čerpána automaticky z dat ze Systému pro sledování vozidel (AVL), jedná se o data generovaná automaticky (např. počátek a konec jízdy, ujeté km) nebo ručně zadané informace (např. zadané údaje o tankování PHM). Uživatelské rozhraní

(1) Výběr vozidla a období - při výběru vozidel je možné používat fulltextové vyhledávání podle RZ nebo jména vozidla.

(2) Pro zobrazení dat se volí začátek a konec období. Délka vybraného období však může mít maximálně 33 dnů.

(3) Pohled na jízdy – je určen pro práci se zaznamenanými jízdami. Jednotlivé jízdy je možné editovat a korigovat jejich ujetou vzdálenost zadáním tachometrů.

(4) Pohled na jízdy obsahuje:

(a) Seznam uskutečněných jízd s výběrem vozidla a období

(b) Mapový podklad pro zobrazení pohybu vozidel

(c) Panel Detail pro zobrazení podrobných informací o jízdě

(d) Panel Stavy tachometru pro zobrazení odchylky měření GPS zařízení a tachometru vozidla a pro úpravy stavů tachometru

(5) Úpravy jízd je možné provádět v seznamu jízd po označení vybrané jízdy, ve kterém můžete měnit účel jízdy, řidiče a nákladové středisko. U jednotlivé editace je možné měnit i ujetou vzdálenost dle GPS (úprava ujeté vzdálenosti dle GPS je určena pouze pro výjimečné situace).

16.2. Integrované systémy a technologie

(1) Modul kniha jízd spolupracuje s dalšími moduly IS ZOS:

(a) IS ZOS – přebírání čísel akcí, statusů vozidel, přihlášení řidičů do směny

(b) Fleetware – přebírání dat o jízdách

16.3. Integrované systémy a technologie

(1) Kniha jízd je webová aplikace, která pracuje se stejnou databází jako systém pro Sledování vozidel, tím je zajištěno přebírání dat z tohoto subsystému.

(2) Podmínkou provozu mimo obecných požadavků IS na provoz (funkční HW a databáze) je nastavení všech potřebných parametrů a využití dat spolupracujících modulů pro automatizaci plnění dat do Knihy jízd.

(3) Pro provoz v modulu Kniha jízd musí mít uživatel přidělena příslušní přístupová práva. Konfigurace modulu Kniha jízd je primárně spojena s konfigurací systému pro Sledování vozidel.

17. Integrace se systémem Pegas (CC-API)

(1) Funkční propojení operačního střediska ZZS KVK se sítí PEGAS s využitím standardizovaných integračních rozhraní pro operační řízení podle zveřejněných specifikací výrobce systému PEGAS, zejména TETRAPOL Publicly Available Specifications.

(2) Pro zajištění integrace včetně možnosti využívat níže uvedené funkce, a to prostřednictvím terminálů je používáno integrační rozhraní CC-API, které zprostředkovává komunikaci ZOS s technologiemi a prostředky, umístěnými přímo v síti Pegas. Tyto technologie jsou umístěny to v lokalitě Policie České republiky a jsou v její správě. Samotné integrační rozhraní CC-API je provozováno na serveru umístěném v datovém centru ZZS KVK.

(3) Zajištění plnohodnotných komunikací ve všech provozních módech systému PEGAS vč. Hovorových skupin TKG.

17.1. Integrace radiofonie a telefonie

(1) Systém a technologie pro integraci radiofonie a telefonie představuje důležitou součást celého komplexního IS ZOS. Umožnuje operátorům ovládat (přijímat, přepojovat, spojovat) hlasovou komunikaci jak v oblasti telefonie, tak v oblasti radiofonie.

(2) Mezi základní funkcionality systému v oblasti integrace s radiovou sítí Pegas patří:

(a) Řízení adresace paketů digitálního audia do hlavních a příposlechových kanálů v hovorových soupravách.

(b) Zajištění krátkodobého záznamu audia formou uložení paketů na HDD.

(c) Možnost volby mezi hlasitou a tichou hovorovou soupravou.

(d) Možnost otevřeného i šifrovaného přenosu se zajištěním ztrátové komprese.

(e) Používání jediného mikrofonu resp. jedné hovorové soupravy v kombinaci hlasitá/náhlavní pro všechny komunikační prvky (linkové i radiové terminály Pegas, telefon).

(f) Integrace na subsystém pro operační řízení (IS ZOS).

(g) Funkce klíčování.

(h) Zajištění připojení audiosignálů do propojovacího pole.

(i) Poskytování výstupů pro nahrávání.

(j) Zajištění zobrazení registračního stavu.

(k) Zobrazování seznamu operačních skupin.

(l) Zobrazení indikace stavu terminálu.

(m) Zajištění sestavení odchozího individuálního hovoru nebo vytáčené konference.

(n) Zajištění přijetí příchozího individuálního hovoru vč. zobrazení adresy RFSI volajícího.

(o) Zajištění předání probíhajícího individuálního volání na jiný terminál.

(p) Zajištění tichého volání s prověrkou oprávnění operátora.

(q) Zajištění ukončení individuálního hovoru operátorem nebo protistranou.

(r) Zajištění zobrazení seznamu standardních otevřených kanálů, krizových otevřených kanálů a otevřených kanálů typu broadcast.

(s) Zobrazení adresy RFSI terminálu hovořícího v otevřeném kanálu.

(t) Zajištění zřízení otevřeného kanálu, vstup, opuštění a uzavření otevřeného kanálu.

(u) Zajištění zřízení otevřeného kanálu typu broadcast, vstup, opuštění otevřeného kanálu typu broadcast.

(v) Zajištění uzavření otevřeného kanálu typu broadcast ručně nebo automaticky.

(w) Zajištění varování o nově otevřeném krizovém kanále.

(x) Zajištění vstupu do krizového otevřeného kanálu ručně nebo automaticky.

(y) Zajištění opuštění a uzavření krizového otevřeného kanálu.

(z) Zajištění přijetí statusu a adresovatelné odeslání statusu.

(aa) Zajištění přijetí SMS a adresovatelné odeslání SMS.

(bb) Zajištění skupinového odeslání SMS předem definované skupině.

(cc) V případě TKG – hovorových skupin zajištění veškerých dostupných funkcionalit systému PEGAS, tj. např. zřízení, vstup, opuštění, uzavření, zobrazení adresy, sloučení kanálů TKG.

(3) Mezi základní funkcionality systému v oblasti integrace telefonie patří:

(a) zajištění efektivní integrace telefonních systémů (pobočkové ústředny a stávajících IP telefonů) do systému integrace komunikací a IS ZOS.

(b) Usnadnění operátorovi ovládání komunikačních systémů přímo z rozhraní aplikace IS ZOS

(c) Usnadnění operátorovi ovládání komunikačních systémů dotykové obrazovky prostřednictvím rozhraní pro ovládání všech typů komunikací včetně radiových systémů

(d) připojení každého pracoviště operátora ZOS jednou telefonní linkou v režimu multiline

(e) indikace aktuálního stavu každé linky zabarvením příslušného pole na dotykové obrazovce dispečera

(f) sestavení odchozího hovoru ze seznamu nebo ad hoc

(g) přijetí příchozího hovoru se zobrazením telefonního čísla volajícího

(h) zavěšení hovoru operátorem nebo protistranou

(i) převzetí vyzvánějícího hovoru z jiné linky

(j) přidržení hovoru

(k) přepínání mezi aktivním a přidrženým hovorem

(l) třístranná konference

(m) vstup do hovoru

(n) vedení podrobných protokolů o činnosti

(o) zajištění příposlechu

(p) krátkodobý záznam

(q) databáze volajících s možností vložení poznámky k telefonnímu číslu operátorem ZOS, zobrazení informací z databáze o volajícím čísle v případě příchozího hovoru již při vyzvánění

(r) zobrazení historie příchozích hovorů s možností filtrace příchozích hovorů z linek tísňového volání atd.

17.2. Integrované systémy a technologie

(1) Integrace telefonie se skládá z pobočkové ústředny Alcatel, z šesti dispečerských terminálů, majáčků pro signalizaci obsazenosti linky daného dispečera připojeného k terminálu a ze záložních telefonů.

(2) Do integrace se síti Pegas je zahrnuto 7 LCT modulů. Klíčovým komponentem integrace se sítí Pegas je radiová brána GW TETRAPOL. S radiovou sítí Pegas je brána připojena přes rozhraní linkového terminálu LCT. Audiosignál a signály klíčování se převádí do IP prostředí, LCT pak ovládá pomocí CC-API rozhraní, které běží na CC-API serveru. Do ethernetové sítě je CC-API sever připojen pomocí dvou síťových adaptérů.

(3) Samotná komunikace dispečera se PEGAS sítí probíhá přes dispečerský terminál.

(4) V rámci řešení integrace radiofonie a telefonie do ovládání pomocí dotykové obrazovky terminálu a jsou využívány vazby na systémy/technologie:

(a) Telefonní ústředna

(b) Nahrávací systém

(c) IS ZOS

(d) CC-API

18. Telefonní ústředna

(1) Telefonní ústředna je postavena na řešení Alcatel-Lucent OmniPCX Enteprise. Jedná se o hybridní komunikační systém určený pro jednotnou komunikaci (Unified Communication) s podporou až pro 500 000 uživatelů. Podporuje standardy jako např. SIP signalizaci (uživatel i trunk), IP H.323, Wi-Fi, DECT, stejně jako klasické TDM – analogové a digitální rozhraní se širokým spektrem různých signalizací.

(2) Je založena na otevřených standardech software a hardware a běží na operačním systému SUSE LINUX. Pro integraci se systémy má standardizované rozhraní CSTA. PBX je instalána do 19“ RACKU s vlastním řízením v HA režimu.

(3) Telefonní ústředna pro operační řízení zajišťuje plnohodnotné propojení s objektovou ústřednou (pomocí SIP trunku) a propojení na telefonii v rámci NSPTV a VTS (veřejnou telefonní síť).

18.1. Základní funkcionality

(1) Podpora standardu Microsoft TAPI včetně licencí

(2) Hlasový průvodce v českém jazyce

(3) WEB management konzole

(4) podpora analogových telefonů (dveří hláska, faxy, spojení na letiště)

(5) podpora digitálních telefonů (spolehlivý provoz dispečinku)

(6) podpora IP telefonů (připojených nejen v LAN, ale i přes internet) – jen hlavní ústředna

(7) podpora připojení do veřejné/privátní telefonní sítě pomocí BRI (ISDN2) / PRI (ISDN30)

(8) podpora připojení do veřejné/privátní telefonní sítě pomocí analogových vnějších linek s přenosem CLIP (příčky do KNL, příp. GSM brány)

(9) podpora připojení do veřejné/privátní telefonní sítě IP telefonie protokolem SIP

(10) 30 x hlasových kanálů pro VOIP rozhraní

(11) licence pro integraci dispečerských pracovišť (8 pracovišť) CTI (JTAPI nebo CSTA)

(12) podpora SIP podle RFC 3261 a navazujících standardů

(13) propojení s objektovou telefonní ústřednou o kapacitě min. 10 souběžných hovorů, včetně signalizace, 10 x hlasové kanály H.323 s protokolem ABC-F

(14) standardní funkcionalitou je pak:

- (a) převzetí vyzvánějícího hovoru z jiné linky
- (b) přidržení hovoru
- (c) přepínání mezi aktivním a přidrženým hovorem
- (d) přepojení hovoru
- (e) rozhraní pro integraci telefonní ústředny v rámci integrace telefonie

18.2. Porty

(1) porty pro připojení 8 digitálních telefonů s víceřádkovým displejem, konektorem náhlavní soupravy, s minimálně 80 konfigurovatelnými tlačítky

(2) dalších 16 portů pro digitální telefony

(3) 8 portů pro analogové telefony

(4) licence pro 20 IP telefonů – pro externí pracoviště

(5) 4 porty ISDN2 pro připojení do veřejné telefonní sítě

(6) 2 porty ISDN 30B+D pro připojení k JTS a KU KVK

18.3. Provoz a vysoká dostupnost

(1) zdvojení základního prvku řešení – při výpadku automatický přechod dotčených prvků řešení na zálohu bez nutnosti zásahu administrátora.

(2) po odstranění závady automatický přechod dotčených prvků řešení do původního stavu (např. na primární řídící server nebo hlasovou přípojku)

18.4. Vyrozumívací systém AMDS

(1) Vyrozumnění posádek ZZS KV o výjezdu.

19. Systém nahrávání

Systém nahrávání zajišťuje nahrávání radiofonní a radiokomunikační komunikace.

19.1. Funkce a konfigurace

(1) Vstupní kanály:

(a) 32 analogových vstupů

(b) digitální interface, pasivní připojení, 2 porty, podpora sterea

(c) ethernet karta pro záznam VoIP

(d) SW aplikační server

(e) SW + HW voice procesor

(2) Rozsah záznamu

(a) záznam digitálních pobočkových linek, které používají dispečeři s identifikací volajícího a volaného

(b) záznam IP telefonů s identifikací volajícího a volaného

(c) záznam analogové telefonní linky pro vstup do objektu (dveřní hláska)

(d) záznam digitálních radiostanic s identifikací volajícího a volaného

(e) záznam z analogového režimu radiové sítě Motorola

(f) stereo záznam s rozdělením směrů volaný a volající

(g) záznam nepřevzatých hovorů vč. Identifikace volajícího

(3) Ukládání dat na dva paralelní HDD

(4) Ukládání ve formátu, který odpovídá obecnému standardu a který umožňuje konverzi do jiných formátů pro zajištění dostupnosti záznamu po celou dobu požadované archivace.

(5) Uživatelské funkce a integrace

(a) práce s hovory

(b) přístup přes web rozhraní

(c) integrace záznamového zařízení s IS ZOS

(d) integrace záznamového zařízení s integrací telefonie a radiofonie

(e) identifikace polohy volajícího z GSM telefonu

(f) přehrávání záznamů

(g) přeskakování ticha v záznamu

(h) svázání souvisejících záznamu volání při přepojování, konferencích a konzultačních hovorech

(i) integrace se stávajícími záznamovými zařízeními a aplikačním serverem

(j) grafické zobrazování výskytu klíčových slov

(k) zajištění hlasové analýzy

(l) automatické vyhledávání klíčových slov, emocí, pořadí klíčových slov, dialog flow

(m) přístup prostřednictvím hierarchických přístupových práv, uživatelských profilů,

(n) monitoring stavu dispečerů a živý příposlech telefonické komunikace vedoucím ZOS

(o) integrace se systémem BI ZZS KVK – zajištění přenosu dat potřebných pro vytváření statistik a přehledů

(p) komplexní dohled nad systémy ReDat ZZS KVK – monitoring funkce jednotlivých produktů a komponent, vytížení systému a záznamových vstupů, e-mail reporting.

(q) nahrávání telefonního provozu příjmu tísňové výzvy NSPTV

(6) Plně funkční nahrávání telefonního provozu příjmu tísňové výzvy z NSPTV, od okamžiku převzetí hovoru ZZS KVK, do ukončení převzetí tísňové výzvy dispečerem ZZS KVK, nebo do předání hovoru operátorovi jiné složky či operátorovi jiného ZOS ZZS.

(7) Architektura spočívá v neredundantním řešení, které se skládá z HW loggeru ReDat3, a na virtuálním stroji nainstalovaných ReDat eXperience a serveru pro hlasové analýzy. Pro ukládání nahrávek slouží složky D:\Archiv.

(8) Celkové schéma zapojení zařízení je následující:

(a) 3x neintegrované RCT – APCM + Moxa

(b) LCT a integrované RCT – přes IP (act. H323)

(c) UDRM – pobočky Mitel, ISDN2

(d) PCM – 1x ISDN 30

(e) IP Cisco – záložní telefony na SIPu

(f) IP záznam dotykových terminálů přes act. h.323

(9) Z důvodu hlasových analýz jsou všechny záznamy v nekomprimovaném formátu.

(10) Integrace na IS ZOS: Služba replikace odesílá UDP eventy do IS ZOS, na jejich základě spáruje systém nahrávky s polohou mobilních telefonů. Záznamy jsou párovány s IS ZOS přes integrační modul API.

(11) Integrace na integraci telefonie a radiofonie: UDP eventy z obou ReDat eXperience jsou zasílány na systém integrace telefonie a radiofonie.

20. GPS jednotky

(1) Sledování vozidel je závislé na přenosu dat mezi vozidlovou jednotkou a serverem GIS. Pro tuto komunikaci jsou nezbytné SIM karty s pevnou IP adresou, aktivované v prostředí privátního APN. SIM karty nejsou součástí řešení a ZZS KVK si pro tento účel zajistila vlastní SIM. Data jsou ukládána na Fleetware serveru na ZZS.

(2) Data z vozidel jsou přenášena pomocí GSM-GPRS komunikace, skrz síťovou infrastrukturu operátora na tzv. CGU komunikační modem, který je umístěný v síti ZZS KVK a zajišťuje správné směrování paketů v proprietárním komunikačním protokolu systému Fleetware.

(3) Příchozí data jsou zpracovávána a ukládána na serveru Fleetware umístěném v LAN ZZS. Současně s uložením dat do DB MS SQL 2012 standard jsou také paralelně, adresně na jednotlivé klienty, rozesílány aktualizační pakety online poloh.

21. Stávající infrastruktura

21.1. Datové sítě

LAN infrastruktura lokality Karlovy Vary

(1) Základem LAN infrastruktury lokality Karlovy Vary jsou dva vysoce dostupné stohy přepínačů HPE, z nich jeden tvoří jádro sítě a zajišťuje vzájemou komunikaci serverů rychlostí 10 Gb a druhý tvoří distribuční vrstvu LAN pro napojení dalších technologií a koncových zařízení rychlostí 1 Gb. Celkově je v LAN provozováno 6 síťových přepínačů HPE 1950 a HP5120 bez podpory PoE.

LAN infrastruktura záložního operačního střediska

(2) LAN infrastrukturu záložního operačního střediska tvoří síťový přepínač HPE 1950. LAN je, obdobně jako hlavní operační středisko, připojena ke komunikační infrastruktuře Karlovarského kraje a samostatnou linkou k Internetu. Záložní operační středisko je vybaveno firewallem Fortigate FG-60E a umožňuje zakončovat VPN ZZS.

Komunikační infrastruktura Karlovarského kraje

(3) Karlovarský kraj vlastní a provozuje komunikační infrastrukturu (dále jen KI) typu WAN na bázi optických tras. Infrastuktura propojuje významné veřejnoprávní subjekty (krajský úřad, obce s rozšířenou působností) a jimi zřizované organizace v karlovarském kraji. KI je také napojena na Internet a resortní sítě (PČR, KIVS apod.) a umožňuje tak napojeným subjektům přistupovat ke službám těchto sítí (Internet, CMS, ISZR apod.) LAN infrastruktura ZZS je s KI propojena a využívá ji pro přístup k Internetu (ISP O2), připojení některých základnových stanic (Ostrov), VPN komunikaci a napojení na další externí sítě.

KI a externí sítě

(4) LAN ZZS je propojena s KI a tím i zprostředkovaně k dalším externím sítím.

Internet

(5) Připojení prostřednictvím KI k ISP O2 Czech Republic je využíváno jak pro primární připojení do sítě Internet, tak i pro VPN přístup a realizaci VPN sítě ZZS. Sekundární (záložní) internotavé konektivita je zajišťována společností Wolfnet.

(6) Jako firewall a VPN koncentrátor je využit vysoce dostupný cluster firewall FortiGate FG-60F, který je plně pod správou ZZS.

VPN ZZS

(7) Výjezdová základny jsou k centrálním systémům ZZS připojeny prostřednictvím VPN. Jako transportní trasy jsou používány běžné internetové přípojky (typicky xDSL). Hraničním zařízením výjezdových základen je router Cisco řady 800, které uzavírají VPN vůči koncentrátoru v centrále ZZS, ale nepodporují technologi SD-WAN a automatické řízení provozu ukončovacími body VPN (operační středisko a záložní operační středisko) .

PČR – síť PEGAS

(8) Samostatné propojení L2 (jedna VLAN) do serverovny KŘ PČR je ukončeno v centrálním switchi. Na straně KŘ PČR je umístěn Switch ZZS, do kterého je připojena veškerá technologie pro provoz radiové sítě PEGAS (LCT, Gateway atd.)

Síť ITS – NIS IZS

(9) Síť ITS – NIS IZS slouží pro přístup do sítě NIS IZS a k aplikacím a jejich serverům (IPL, GIS) tzv. „střechového“ projektu.

(10) Síť provozuje MV ČR a Nakit. V rámci serverovny v lokalitě Karlovy Vary je ITS ukončena v zařízeních Juniper Karlovaského kraje. Tato zařízení jsou připojena do redundantního switche a prostřednictvím samostatného portu je síť přivedena do firewallu ZZS, kde je zajištěno oddělení sítě ITS od sítě OŘ.

INFO35 – AML

(11) Samostatné propojení ke službě INFO35 a AML, které zajišťuje O2 Czech Republic, je realizováno samostatným koncovým zařízením O2 připojeným do centrálního firewallu. Prostřednictvím firewallu přistupují jednotlivé technologie ke službě Info35.

Vzdálený přístup

(12) Pro vzdálený přístup pro účely servisu je k dispozici VPN na firewallech Fortigate. Pro případ výpadku firewallů je k dispozici nezávislé VPN připojení prostřednictvím routeru Mikrotik.

21.2. Virtualizační platforma

Servery a disková úložiště

(1) Virtualizační platforma operačního střediska v lokalitě Karlovy je tvořena třemi servery Dell R740 virtualizovanými technologií VMware vSphere Essentials Plus 6.7, které tvoří vysoce dostupný cluster. Interní disky serverů jsou virtualizovány technologií HPE StoreVirtual VSA a společně tvoří vysoce dostupné diskové úložiště publikované hypervizorům ESXi.

(2) Meziserverovou síťovou komunikaci rychlostí 10 Gb zajišťuje IRF stoh (vysoce dostupný cluster) přepínačů HPE 1950. Síťové propoje jsou redundantní.

(3) Vlastní instalace je realizována v jednom RACKu.

(4) Napájení veškerých technologií operačního střediska je zálohováno centrální UPS, jejíž správa není předmětem této VZ.

(5) Virtualizační platformu záložního operačního střediska tvoří jeden server Dell R640 virtualizovaný technologií VMware vSphere Essentials 6.7. Jako diskové úložiště slouží interní disky serveru. Napájení je zálohováno samostatnou UPS FSP/Fortron 2000VA.

Zálohování a replikace

(6) Zálohování všech virtuálních serverů je řízeno software Veeam Backup & Replication Essentials Enterprise. Zálohy jsou ukládány na dvě nezávislé NAS Synology DS916+ (kapacita 9TB) a DS412+ (kapacita 6 TB) umístěné v lokalitě Karlovy Vary.

(7) Software Veeam dále provádí replikaci klíčových virtuálních serverů do záložního operačního střediska a řídí procesy fail-over a fail-back.

Operační systémy a databáze

(8) Hlavními databázovými systémy jsou Microsoft SQL Server Standard a ORACLE database standard edition. Tyto systémy jsou sdíleny aplikacemi a systémy operačního střediska a jejich výkon a dostupnost jsou tak kritické pro zajištění bezproblémového běhu dispečerských systémů s rychlými odezvami prostředí.

Neprodukční systémy

(9) Součástí operačního střediska jsou historicky používané technogie, které již nejsou využívány v produkčním provozu a jsou určeny k odpojení od ostatních systémů (LAN, monitoring apod.), demontáži a vyřazení. Tyto technologie jsou uvedeny v tabulce v kapitole Technologie operační střediska.

Technologie operační střediska

(10) Následující tabulka shrnuje technologie operačního střediska:

Technologie	Množství
Operační systém Windows server 2003 - 2019	dle systémů
Win RDS 2012 DvcCAL (terminál mapy)	15
SQL Server Standard 2012	2
ORACLE Database Standard 2 CPU	1
VMware Horizon View	20
Microsoft VDA	20
HPE SV VSA 2014 10TB E-LTU	3
Veeam Backup Essentials Enterprise socket	4
VMware vSphere Essentials	1
VMware vSphere Essentials Plus	1
PowerEdge R740 Server	3
PowerEdge R640 Server	1
UPS FSP/Fortron UPS 2000 VA rack 2U, online	1
HPE 1950 Switch	3
HP A5120-SI Switch	4
Synology DS412+ Disc Station, 4x HDD 2 TB	1
Synology DS916+ DiskStation, 4x HDD 3TB	1
t610 PLUS WES7P 16SF/4GR QH TC	5
NM10, mini PC Crypto	5
17" LCD NEC V-Touch 1721 5R - 5-žilový,DVI,RS-232	5
DELL Profesional P2412H + 5x SoundBar	15
Řídící SW telestěny KINETIC	1
NM10, mini PC Crypto, RACK	1
LG M4224F-LCD monitor 42	4
Xerox WorkCentre 7125V_S	1
Cisco 886VA Secure Router with VDSL2/ADSL2+ over ISDN (VPN)	11
Fortinet FortiGate 60F, UTM	2
Mikrotik RB750r2	1
Datový rozvaděč CONTEG 42"	1
HP StoreVirtual 4330 450GB SAS Storage	1
HP DL360p Gen8 server	3
HP P4300 G2 7.2 TB SAS Storage	2
HP StoreVirtual 4330 450GB SAS Storage	1

21.3. Koncová zařízení a sdílené systémy

Doručování aplikací a pracoviště operátorů

(1) Aplikace jsou na koncová zařízení uživatelů (zejména, ale nejen operátorů) doručovány prostřednictvím virtualizační technolgie VMware Horizon View. Koncová zařízení jsou tencí klienti (terminály) HP TC610 Plus. Každý terminál obsluhuje 3 monitory Dell Professional P2412H, jeden z monitorů je vždy vybaven zvukovou lištou (soundbarem). Pro obsluhu

hlasových komunikačních systémů je každé operátorské pracoviště vybaveno samostatným mini PC s 17“ dotykovým monitorem NEC V-Touch 1721.

Sdílené systémy operačního střediska

(2) Operátoři mají v operačním středisku k dispozici sdílené multifukční zařízení Xerox WorkCentre 7125V a telestěnu tvořenou čtyřmi monitory LG M4224F, které jsou řízeny samostatným PC umístěným v serverovém racku.

Vybavení sanitních vozidel

(3) Pro provoz aplikace MZD jsou sanitní vozy vybaveny odolnými tablety Panasonic FZG1 se speciálně upraveným operačním systém na bázi Windows 7, který již není podporován. Tablety jsou umístěny ve vozidlových držácích a jsou vybaveny komunikačními rozhraními WiFi, Bluetooth a GSM 3G a standarním rozhraním USB 2.0. Nedisponují žádným bezpečnostním prvkem (čtečka karet, čtečka otisků prstů apod.).

Vybavení výjezdových základen

(4) Základny jsou jednotně vybaveny stolním kancelářským počítačem Dell s operačním systémem Windows 7 a kancelářským balíkem Office 2013. Počítač je připojen do VPN ZZS a jejím prostřednictvím komunikuje s IS ZOS, popřípadě do Internetu. Součástí sestavy je monitor 24“ Dell a laserová tiskárna Xerox A4.