Návrh dodavatele (Popis technického řešení)

Obsahem dokumentu je návrh technického řešení předmětu plnění. Návrh vychází z informací poskytnutých Objednatelem v rámci Zadávací dokumentace – tím je určena možná míra detailu návrhu, zejména v oblasti technických vazeb, ale i vazeb na procesy a organizace. Z těchto důvodů návrh představuje dokument zpracovaný dle nejlepšího vědomí a svědomí Dodavatele, který v případě realizace veřejné zakázky bude v souladu s požadavky Zadávací dokumentace na základě předimplementační analýzy zpracován (rozšířen) do finálního návrhu cílového stavu. Finální návrh cílového stavu bude po schválení Objednatelem sloužit jako závazný dokument pro vlastní realizaci.

1. Předmět plnění

(1) Předmětem plnění veřejné zakázky je dodávka a implementace technologií pro zvýšení kybernetické bezpečnosti informačních systémů (IS) a komunikačních systémů (KS) Objednatele 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 je být navrženo tak, aby náklady na provoz systému byly co nejmenší.

(2) 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 Dodavatelů-při vzdáleném i lokálním přístupu k IS. Součástí je pořízení software pro správu privilegovaných účtů a přístupů, dále implementace a související služby.	Soubor	1

Komodita	Zajišťovaná oblast	Stručný popis položky	Jednotka	Počet jednotek
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. 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.	Soubor	1
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

(3) Technologie (produkty) navržené pro naplnění cílů jednotlivých komodit

Komodita	Zajišťovaná oblast	Technologie
K.1	Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS	**WiFi 6 přístupové body Aruba AP-505 + Aruba Instant** **Síťové přepínače Aruba 6000** **Aruba Clearpass Policy Manager** **Next generation firewally Fortigate FG-40F**
K.2	Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS	**AC Identita – IDM (Identity management), resp. IAM (Identity and Access management) software** **Imprivata OneSign – pokročilá MFA** **Systém MONET ProID – komponenty Kartové centrum, ACEx, Správce karty** **Identifikační hybridní karty MONET ProID+Q** **Identifikační USB tokeny MONET ProID+Q** **Čtečky bezkontaktních a kontaktních identifikačních karet**
K.3	Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS	**AC PIMPAM – PIM (Privileged Identity Management) a PAM (Privileged Access Management) komplexní software**

Komodita	Zajišťovaná oblast	Technologie
K.4	Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů	**Logmanager – komplexní SEM (Security event management), resp. SIEM (Security Information and Event Management)**
K.5	Nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS	**GREYCORTEX Mendel All-in-one XS – NDR (Network Detection and Response) systém**
K.6	Nástroje pro zajišťování úrovně dostupnosti informací	**Originální serververové komponenty DELL pro upgrade HW serverů** **Disková police Synology s disky** **SDS software VMware vSAN Standard** **Server DELL PowerEdge T350** **Software Veeam Hardened Repository** **Tenký klient HP t640** **Monitory DELL P2422H se zvukovou lištou a S2722DZ** **Monitory Philips 172B9TN** **Počítače ASUS PN41** **Počítače DELL OptiPlex 5000**
K.7	Vozidlové komunikační jednotky	**Odolné tablety Panasonic Toughbook G2 s originálním příslušenstvím**
K.8	Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS	**Systém MONET ProID – komponenty Kartové centrum, CMS (Card management system) a QSeal**

2. Navržené parametry technického řešení

(1) Dodavatel při výstavbě, správě a provozu technologií striktně dodržuje hledisko technologické neutrálnosti, tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců.

(2) Dodavatele z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů využije stávající prostředky a technologie. Nebude implementovat duplicitní řešení např. další serverovou virtualizační platformu, adresářovou službu apod.

(3) Dodavatel prokáže, že všechny dodávky, které dodá Objednateli:

(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 Dodavatele doloží čestným prohlášením. Dodavatele respektuje právo Objednatele 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.

2.2. K1 – Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS

(1) Pro zvýšení bezpečnosti komunikační sítě Dodavatele implementuje:

(a) granulární a dynamickou 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. Využije 2 nezávislé vstupními body VPN centrály/LAN a zajistí jejich využití základnovými prvky pro automatického přepnutí komunikace (VPN) výjezdových základen na ZZOS v případě výpadku ZOS

(c) centrálně spravovanou WIFI na bázi Aruba Instant s aplikováním ověřování a segmentací a podporou aktuálního zabezpečení komunikace WPA3-Enterprise

(2) V rámci plnění 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.

(3) Dále bude implementován systém centrální správy VLAN, který 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.

(4) 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 bude 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.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) 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 dodávky).

2.3. K2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS

(1) Pro zvýšení úrovně zabezpečení v oblasti správy a ověřování identit uživatelů a správců Dodavatel implementuje:

(a) Nástroj 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) Dvoufaktorovou autentizaci 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 operačního střediska 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. Řešení bude připraveno na využívání jiných faktorů (např. biometrických) pro autentizaci.

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

(3) 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 Objednatele.

(4) Na IDM budou navázány hlavní informační systémy Objednatele – 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.

(5) 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.

(6) 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.

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

(8) 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.

2.4. K3 – Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS

Pro zvýšení úrovně zabezpečení v oblasti řízení přístupových oprávnění interních i externích správců Dodavatel implementuje nástroje pro správu a kontrolu privilegovaných uživatelů (tzv. PIM (privileged identity management) a PAM (privileged access management)).

(1) Nástroj bude integrován s Nástrojem pro automatickou správu identit.

(2) Nástroj bude implementován jako proxy, tzn. jako zprostředkovatel autentizace privilegovaného uživatele vůči chráněnému a monitorovanému systému.

(3) 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.

(4) Nabízené řešení bude 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.

(5) Součástí nástroje bude i 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 bude nahrávána ve video formátu a bude jednoznačně přiřazena konkrétní osobě. Nahrávky budou zabezpečeným způsobem přenášeny do centrálního úložiště, kde jsou dlouhodobě uchovávány a bude 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) Dodavatele vybuduje monitorovací server/applianci, 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 bude šifrována bez potřeby využití VPN apod.

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

Pro zvýšení úrovně zabezpečení v oblasti řízení přístupových oprávnění interních i externích správců Dodavatel implementuje Nástroj pro správu logů (tzv. log management),

(1) Zavedením nástroje 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.

(2) 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 zajistí integritu archivu.

(3) Systém bude implementován jako samostatná hardwarová appliance, aby byla zajištěna nezávislost nástroje na infrastruktuře ZZS KVK a tím schopnost zaznamenávání její činnosti i v nestandardních provozních stavech (přetížení, start, nestabilita apod.)

(4) Nabízené řešení je standardní Log/Event Management, které obsahuje prvky (dílčí služby) SIEM a lze jej napojit na služby SOC (Security operations center).

(5) 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 bude 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.

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

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

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

(9) 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.

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

(11) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – samostatntá appliance, která umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Ukládání všech informací bude prováděno do jedné databázetak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů.

(12) 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.

(13) Nástroj umožní 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.

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

(15) 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.

2.6. K5 – Nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS

Pro Zvýšení úrovně zabezpečení v oblasti detekci kybernetických bezpečnostních událostí vůči IS ZOS Dodavatel implementuje:

(1) Nástroj 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.

(2) Nástroj bude implementován jako samostatná hardwarová appliance, 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 bude monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a bude 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 budou být instalované v interním prostředí Objednatele („on premise“) bez použití externích komponent nebo cloudových služeb.

(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.

2.7. K6 – Nástroje pro zajišťování úrovně dostupnosti informací

Pro zvýšení úrovně dostupnosti informací Dodavatel implementuje:

(1) Rozšíření diskové a paměťové kapacity serverů. Do serverů budou 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.

(2) Nový systém diskové virtualizace VMware tak, aby byla zachována současná funkcionalita (především vysoká dostupnost a výkon) a kompatibilita se serverovou virtualizací

(3) Moderní koncová zařízení pro pracoviště operačního střediska. 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).

(4) Nástroje pro automatické přepnutí provozu IS ZOS mezi ZOS a ZZOS a zpět. Nástroj zajistí rekonfiguraci dotčených systémů a síťových služeb (zejména DNS) tak, aby IS ZOS byl dostupný uživatelům v ZZOS a výjezdových základnách z prostředí ZZOS.

(5) Bezpečné datové úložiště pro zálohy. Půjde o 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). Data budou chráněna 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/záloh a odpovídajících retenčních lhůt. Data bude možné ukládat pomocí

běžných síťových protokolů, např. SMB/CIFS. 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.

(6) Nová koncová zařízení výjezdových stanovišť včetně migrace pracovních (služebních) uživatelských dat a zprovoznění vícefaktorové autentizace uživatelů dodanými identifikačními prostředky.

2.8. K7 – Vozidlové komunikační jednotky

Dodavatel v rámci komodity dodá vozidlové komunikační jednotky (déle jen jednotky) zásahových (převáženě sanitních) vozidel, které budou sloužit pro provoz aplikace MZD (Mobilní zadávání dat), EKP (Elektronická kniha pacienta) a IS ZOS. Jednotky 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.

(1) 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. Dodavatel poskytne technickou podpora montáže do vozidel. Samotná montáž zařízení do vozidel není předmětem plnění.

(2) Nabízené jednotky – speciální odolné tablety – jsou odolné proto nešetrnému zacházení včetně pádu na zem při zachování mobility a snadného ovládání.

(3) Technické provedení jednotek je nabízeno 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 umožňuje „ruční podepisování“ prstem či předmětem - dodaným perem Jednotky budou vybaveny operačním systémem, kompatibilním se stávajícími aplikacemi MZD, EKP a IS ZOS a nově dodávanými technologiemi.

2.9. K8 – Správa identifikačních prostředků

Pro správu identifikačních prostředků, které budou nositeli elektronických identit Dodavatel implementuje systém pro centrální správu životního cyklu těchto prostředků.

Systém umožní ((re)iniciace prostředku, jeho 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.

(1) Dodavatel doporučí vhodné certifikační služby pro implementaci, přičemž respektuje právo Objednatele 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) – v takovém případě Dodavatel akceptuje povinnost jednu stanovenou certifikační službu implementovat.

(2) 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.

(3) 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.

2.10. Specifické požadavky – povinné parametry řešení

(1) V dále uvedených tabulkách jsou uvedeny nabízené parametry dodávaného řešení.

(2) **Dodavatel plní všechny povinné parametry.**

(3) 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**	**Dodavatel popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Dodavatel uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém řízení přístupu do sítě podle standardu IEEE 802.1X **Aruba Clearpass Policy Manager + licence pro 500 konkurenčních zařízení**	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.	Pokročilý systém řízení přístupu do sítě (network access control) v povedení softwarové appliance založená na IEEE 802.1X. Podporuje autentizaci, autorizaci, účtování přístupů uživatelů i libovolných síťových zařízení. Obsahuje RADIUS server i databáze uživatelů a zařízení.	Aruba ClearPass.pdf
	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	Umožňuje nastavit síťový přístup uživatelů a zařízení podle politik pomocí přiřazení VLAN, ACL. Atributy pro definici politik IP, MAC, port, VLAN, Q in Q VLAN, hostname (PC name), uživatelské jméno Active Directory, operační systém	ClearPass-Wired.pdf
	Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN	Podporuje autentizaci a autorizaci pomocí IEEE802.1X pro různé typy sítí (včetně bezdrátových, Ethernet LAN a VPN) napříč různými výrobci	Aruba ClearPass.pdf
	Základní autentizační metody	Min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty	Podpora EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS), PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP- Public, EAP-PWD), TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP), MAC authentication, Online Certificate Status Protocol (OCSP), Admin/operator access security via CAC and TLS certificates	Aruba ClearPass.pdf
	Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází – Active Directory, LDAP, ODBC	Interná databáze využitelná napříč doménami, podpora Active Directory, LDAP, ODBC	Aruba ClearPass.pdf
	Nezávislá autentizace a autorizace	Úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, ale autorizace proti externí SQL databázi.	Podpora více nezávislých zdrojů pro autentizaci a autorizaci včetně Active Directory, SQL databáze a požadovaného scénáře.	Aruba ClearPass.pdf
	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).	Pro autentizaci a autorizaci jsou podporovány LDAP, MS AD, obecná SQL databáze (vč. MySQL, PostGRES, Oracle, ODBC), Kerberos, web autentizace (https). Systém podporuje Single-Sign-On SAML2 (standardní podpora Identity	Aruba ClearPass.pdf

Komodita K.1 – Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS				
			Providers (IdP) a Relying Party (RP)), Oauth2, Shibboleth i Okta	
	Kontexová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory.	Integrovaný context-based policy engine umožňuje autorizace na základě libovolných atributů z Active Directory a parametrů připojení, zařízení či uživatele včetně času, typu připojení, osobního profilu	Aruba ClearPass.pdf ClearPass-Wired.pdf
	Externí identity	Podpora autentizace externími identitami – min. Microsoft, Google.	Podpora externích (cloudových identit Microsoft Azure AD a Google Workspace (dříve G Suite).	Aruba ClearPass.pdf
	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	Uživatele lze autorizovat podle politik s využitím účtovaných informací z předchozích připojení, např. čas, objem přenesených dat. Včetně příkladového scénáře.	ClearPass-Wired.pdf
	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.	Plná podpora RADIUS CoA (Change of Authorization) podle RFC3576 pro změnu autorizačního stavu zařízení beze změny politiky.	Aruba ClearPass.pdf ClearPass User Guide.pdf
	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.	Podrobné zpracování syslog zpráv a automatizované reakce pomocí Ingress Enevt Engine. Podpora integrace firewallů Fortinet a izolace klientů.	ClearPass Ingress.pdf ClearPass Fortinet.pdf
	Zpracování syslog	Vestavěná podpora tvorby a úprav vlastních parserů, syslog zpráv pro napojení na další systémy třetích stran	Tvorba vlastních parserů syslog zpráv pro napojení na 3d party systémy	ClearPass Ingress.pdf ClearPass Exchange.pdf
	Bezpečnost	Podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)	Funce RADIUS Dynamic Authorization umožňuje okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)	ClearPass User Guide.pdf
	Správa	Vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení	Snadná správa systému integrovanými nástroji pro testování politik, diagnostiku chování systému i spravovaných zařízení	ClearPass User Guide.pdf
	Portál	Captive portál pro uživatele a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně. Integrovaná podpora úpravy vzhledu	Modifikovatelná captive portál pro rozšířenou autentizaci uživatelů s možností paralelního běhů více unikátních instancí, integrovaný nástroj pro úpravy.	Aruba ClearPass.pdf
	Rychlé přihlášení	Podpora přihlášení prostřednictvím QR kódu. Zapamatování úspěšně autentizovaných/registrovaných klientů a zjednodušení opakovaných přihlášení (např. jen potvrzení uvítací/informační) stránky.	Možnost přihlašování klientů pomocí QR kódu s možností zjednodušeného opakovaného přihlášení.	ClearPass QR.pdf
	Registrace	Podpora samoobslužné registrace s ověřením SMS, e-mailem apod.	Integrovaná samoobslužné registrace, ověření / distribuce údajů SMS, e-mail,	Aruba ClearPass.pdf

Komodita K.1 – Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS				
			tištěná vizitka. Podpora externích identit, např. Facebook, Twitter	
	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.	Interní databáze (nativní součást systému) je šifrována AE2-256 a jsou v ní uloženy veškeré (interní) identitní údaje	ClearPass AES256.pdf
	Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení např. tiskárny, modality, technologické prvky, IoT.	Integrovaná podpora autentizace a autorizece libovolných i speciálních / nepočítačových síťových zařízení min. s využitím MAC	Aruba ClearPass.pdf ClearPass User Guide.pdf
	Vysoká dostupnost	Integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru min. 2 appliance. Druhá appliance není součástí dodávky.	Systém podporuje vysokou dostupnost a (High Availability) a rozkládání zátěže (load balancing) ze 2 uzlů (cluster) doplnění další appliance (není součástí nabídky)	ClearPass User Guide.pdf
	Licence	Licence pro min. 500 konkurenčních koncových zařízení ověřovaných pomocí 802.1X bez omezení počtu uživatelů.	Licence pro 500 konkurenčních koncových zařízení ověřovaných pomocí 802.1X bez omezení počtu uživatelů.	Součást nabídkové ceny
	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.	Integrované RESTful API pro autentizaci/autorizaci/účtování. Příjem syslog událostí, prohledávání a automatické reakce. Vlastí parsery syslog.	Aruba ClearPass.pdf ClearPass User Guide.pdf ClearPass Ingress.pdf ClearPass Exchange.pdf
	Kompatibilita	Appliance určena pro provoz v prostředí stávající serverové virtualizace	Podpora VMware vSphere Hypervisor (ESXi),	Aruba ClearPass.pdf
	Záruka	Záruka min. 60 měsíců v místě instalace, včetně podpory výrobce a nároku na nové verze software včetně aktualizací.	Záruka 60 měsíců v místě instalace, včetně podpory výrobce a nároku na nové verze software včetně aktualizací.	Součást nabídkové ceny
WiFi přístupový bod (AP) 23x **23x Aruba AP-505 + montážní držák AP-MNT-D**	Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na stěnu nebo strop	WiFi 6 přístupový bod (AP) včetně držáku pro montáž na stěnu nebo strop	Aruba AP505.pdf
	Frekvence	činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly s podporou standardu OFDMA	2 nezávislé radiové moduly pro současnou činnost v 2.4 a 5 GHz, podpora standardu OFDMA	Aruba AP505.pdf
	Anténní systém	interní systém pro min. 2x 2 MIMO, optimalizovaný pro montáž na strop	Integrované dvoupásmové antény s podporou 2x2 MIMO, optimalizace pro podstropní montáž	Aruba AP505.pdf
	Přenosové rychlosti	SU-MIMO 5GHz min 1200Mbps, SU-MIMO 2.4 GHz min. 550Mbps	SU-MIMO 5GHz 1.2 Gbps SU-MIMO 2.4 GHz 570 Mbps	Aruba AP505.pdf
	Standardy	podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN	Plná podpora podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN	Aruba AP505.pdf Aruba Instant.pdf
	Řízení klientů	automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma)	Technologie band steering	Aruba Instant.pdf
	Rušení	průběžná detekce non-WiFi rušení a spektrální analýza	Technologie Spectrum Monitor a Adaptive radio management (ARM)	Aruba Instant.pdf

Komodita K.1 – Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS				
	Multi SSID	podpora vysílání min. 8 SSID (WiFi sítí) současně, podpora přiřazení každého SSID samostatné VLAN	Až 16 SSID současně, každé SSID lze přiřadit do samostatné VLAN	Aruba AP505.pdf Aruba Instant.pdf
	Zatížení	min. 250 přiřazených (asociovaných) klientů na radiový modul	Až 256 přiřazených klientů na každý radiový modul	Aruba AP505.pdf
	Porty	min. 1x 1Gb, PoE s podporou standardů 802.3at a 802.3af	1x port 1 GbE PoE s podporou IEEE 802.3at a 802.3af Podpora IEEE 802.3az	Aruba AP505.pdf
	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	Technologie WMM Traffic Management	Aruba Instant.pdf
	Řízení kvality služeb	automatické řízení kvality služeb (QoS) pro hlas a video	Technologie WMM Traffic Management	Aruba Instant.pdf
	Současná obsluha více klientů	Popdora MU-MIMO (Multi-User MIMO) – multi-user multiple input/multiple output	Podpora MU-MIMO a OFDMA	Aruba AP505 specs.pdf
	Bezpečnost	Detekce cizích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu	Plná detekce cizích (rouge) AP	Aruba Instant.pdf
		Integrovaný bezpečnostní modul TPM pro uložení citlivých údajů (přihlašovací údaje, šifrovací klíče apod.)	Integrovaný TMP bezpečnostní modul. Aruba Instant – pokročilý 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.	Aruba Instant.pdf
	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)	Integrovaná podpora WPA3 a standardu 802.15.4 (Zigbee) a Bluetooth 5.0	Aruba AP505.pdf
	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.	Monitoring a správa přes CLI, SSH, SNMP 1-3, syslog a web rozhraní	Aruba Instant.pdf
	Správa frekvenčního pásma	automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference	Podpora standardu IEEE 802.11h, technologie Dynamic Frequency Selection (DFS) a Transmit Power Control (TPC)	Aruba Instant.pdf
	Záruka	záruka min. 60 měsíců	Záruka 60 měsíců	Součást nabídkové ceny
Přístupový přepínač 5x **5x Aruba 6000 48G CL4 4SFP Switch**	Základní parametry	L2/3 přepínač v rackovém provedení	1U L2/3 přepínač do 19“ datového rozvaděče	Aruba CX 6000.pdf
	Porty a propustnost	48x 1 GB RJ-45 PoE+ + 4x 1Gb SFP (nesdílené), min. 104 Gb/s	48 portů 1 Gb RJ-45 PoE+ 4 nesdílené porty 1Gb SFP propustnost 104 Gbps	Aruba CX 6000.pdf
	Směrování	min. statické směrování na L3 vrstvě pro IPv4 I IPv6	Statické routování na L3 vrstvě pro IPv4 a IPv6	Aruba CX 6000.pdf
	Propustnost	neblokovaná architektura	Neblokovaná architektura, propustnost plné kapacity všech portů	Aruba CX 6000.pdf
	Automatizace VLAN	Podpora protokolu MVPR pro automatické zjišťování a přiřazení	Podpora MVRP pro automatické zjišťování a dynamické přiřazovaní VLAN	Aruba CX 6000.pdf
	Agregace portů	podpora LACP	Podpora IEEE 802.3ad LACP	Aruba CX 6000.pdf
	Dualstack	IPv4 a IPv6 dualstack včetně podpory ACL a QoS	Integrovaný IPv4 a IPv6 dual stack, plně podporuje ACL i QoS	

Komodita K.1 – Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS				
	VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření	Podpora standardu VLAN IEEE802.1Q, ověřování klientů MAC i protocol based, zařazování do VLAN na základě ověření 802.1X a aplikace politik včetně QoS a ACL	Aruba CX 6000.pdf
	Ověřování uživatelů a zařízení	podpora 802.1X	Plná podpora IEEE 802.1X	Aruba CX 6000.pdf
	PoE	podpora standardů 802.3af a 802.3at (PoE+ 30W/port), celkový PoE výkon min. 370W	Plná podpora IEEE 802.3af a 802.3at, celkový PoE výkon 370 W	Aruba CX 6000.pdf
	Hlučnost	maximální hlučnost max. 30 dB při plné zátěži	Max. hlučnost 29.8 dB při plné zátěži	Aruba CX 6000.pdf
	Zrcadlení portů	Zrcadlení provozu portů pro diagnostiku a bezpečnostní monitoring, min. 4 zrcadlené skupiny	Zrcadlení síťových portů (ingress i egress), 4 zrcadlené skupiny	Aruba CX 6000.pdf
	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	Monitorování správa prostřednictvím CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní. Dual image pro bezpečný, jednoduchý upgrade	Aruba CX 6000.pdf
	Automatizace a integrace	Integrované REST API rozhraní pro ovládání síťových funkcí	Integrované REST API rozhraní pro ovládání síťových funkcí	Aruba CX 6000.pdf
	Záruka	min. 60 měsíců, oprava do 2 pracovních dnů v místě instalace, včetně nároku na opravné verze firmware	60 měsíců, oprava do 2 pracovních dnů v místě instalace, včetně nároku na veškeré verze firmware	Součástí nabídkové ceny
VPN router 13x **13x firewall Fortigate FG-40F**	Porty	min 5x 1GbE (min. 1x WAN), USB pro ext. modem	5 síťových portů 1 GbE (1 WAN), USB port pro externí modem	FG-40F.pdf
	Základní funkce	Koncové VPN zařízení s podporou SD-WAN a integrovaným firewallem	Firewall s plnou VPN funkčností (včetně funkce koncového zařízení), podpora SD-WAN	FG-40F.pdf
	Počet současných spojení	min. 500 000	700 000	FG-40F.pdf
	Propustnost SSL VPN	min. 400 Mbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 25 klientů	490 Mbps, bez omezení počtu klientů	FG-40F.pdf
	Propustnost SSL inspekce	min. 300 Mbps	310 Mbps	FG-40F.pdf
	Propustnost firewallu	min. 5 Gbps pro libovolnou velikost paketu	5 Gbps pro libovolnou velikost paketu	FG-40F.pdf
	Virtualizace	min. 5 virtuálních kontextů	10 virtuálních kontextů (domén)	FG-40F.pdf
	Vysoká dostupnost	režimy Active/Passive i Active/Active se společnou konfigurací	Vysoká dostupnost – cluster v režimu aktivní/aktivní i aktivní/pasivní	FG-40F.pdf
	Dualstack	podpora současného běhu IPv4 a IPv6	Dual stack, plná podpora současného běhu IPv4 a IPv6	FG-40F.pdf
	Aplikační kontrola	detekce aplikací pro definici směrování SD.WAN	Technologie application steering SD-WAN	FG-40F.pdf
	Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení	FortiGuard – výrobce poskytuje a firewall automaticky stahuje a aplikuje	FG-40F.pdf

Komodita K.1 – Zvýšení zabezpečení komunikační sítě, v níž je provozován zabezpečovaný IS ZOS				
			aktualizace bezpečnostních funkcí (signatury, definice apod.)	
	Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu	Ověřování uživatelů vůči LDAP, Active Directory včetně SSO vůči AD. Ověřování na základě certifikátu	FortiOS.pdf
	Management a monitoring	HTTP/S, SSH, SNMP, syslog,	Správa a monitoring http/s (HTML5), SSH, SNMP, syslog	FortiOS.pdf
	SD-WAN	integrovaná podpora SD WAN-min. rozkládání zátěže a vysoká dostupnost více internetových přípojek, řízení na základě SLA provozu	Vestavěná SD-WAN s podporou rozkládání zátěže a vysoké dostupnosti více internetových přípojek, řízení na základě SLA provozu	FortiOS.pdf
	Sledování toků	export síťových toků (Netflow nebo ekvivalent)	Podpora exporty síťových toků Netflow	FortiOS.pdf
	Standardní funkce	NAT, statické a dynamické routování, publikace interních serverů	Statický a dynamický překlad adres NAT, statické i dynamické směrování, publikace interních serverů	FortiOS.pdf
	Kompatibilita	Kompatibilita se stávajícími firewally pro plné využití VPN a SD-WAN funkcí	Plná kompatibilita se stávajícími firewally FG-60 (shodný výrobce a firmware)	FG-40F.pdf
	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	Záruční servis na 60 měsíců v režimu 24x7 poskytovaný výrobcem zařízení. Výměna vadného zařízení následující pracovní den po nahlášení závady v místě instalace, včetně nároku na aktualizace firmware a SD-WAN funkcí	Součástí cenové nabídky

(4) 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**	**Dodavatel popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Dodavatel uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém pro správu identit (Identity management – IDM) **AC Identita**	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.	Vlastní produkt AC Identita – systém pro správu identit a přístupů (Identity management (IDM) / Access management (IAM)). Umožňuje udržovat a spravovat identity a organizační strukturu organizace. Spravované identity slouží jako referenční identity pro ostatní vnitřní i vnější informační systémy. Identity budou ukládány v databázi.	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	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 Objednatele (počet záznamů, velikost databází atd.). Minimální počet spravovaných uživatelů je 1000	Dodaná licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů a nijak neomezuje obvyklé nasazení a provoz s ohledem na charakter organizace Objednatele. Počet spravovaných uživatelů není omezen.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Komponenty IDM (databáze, uživatelské rozhraní, integrační a provozní úlohy) lze rozložit mezi více serverů a zvýšit tak výkon a zlepšit odezvu systému.	ACIdentitaUzivatelskaPrirucka.pdf
	Evidence aplikací a rolí	Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.	Systém obsahuje registr aplikací a informačních systémů a jejich uživatelských rolí. Role je možné importovat přes webové služby.	ACIdentitaUzivatelskaPrirucka.pdf
	Uživatelské role	Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.	Systém obsahuje správu uživatelských rolí a umožňuje zařadit uživatele do odpovídající role v příslušných IS.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje podrobnou databázovou historizaci – evidenci všech změn identit identit včetně referenčních objektů a vazeb mezi nimi. Umožňuje poskytování dat v libovolném časovém okamžiku v minulosti i aktuálním.	ACIdentitaUzivatelskaPrirucka.pdf
	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.).	Systém obsahuje grafické prostředí pro intuitivní tvorbu pravidel 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.).	ACIdentitaUzivatelskaPrirucka.pdf
	Logování	Systém bude poskytovat auditní logy ve formátu vhodném pro systém typu správy logů (Log management)	Systém poskytuje auditní logy ve formátu vhodném systém správy logů, včetně nabízeného systému Logmanager.	ACIdentitaUzivatelskaPrirucka.pdf
	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)	Systém umožňuje podrobné logování událostí, včetně: - 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)	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	Správa identit	Systém bude spravovat organizační strukturu obsahující interní a externí identity jako samostatné větve struktury.	Systém podporuje správu organizační struktury v oddělených větvích pro interní a externí identity.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	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.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém podporuje a 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.	ACIdentitaUzivatelskaPrirucka.pdf
	Vysoká dostupnost	Systém musí být možno nasadit na více serverů v režimu vysoké dostupnosti.	Systém podporuje nasazení na více serverů v režimu vysoké dostupnosti i pro zvýšení výkonu.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje webový portál, který slouží uživatelům i správcům jako hlavní (primární) rozhraní pro přístup k datům a funkcím i pro správu a konfiguraci systému.	ACIdentitaUzivatelskaPrirucka.pdf
	Podpora mobilních zařízení	Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno)	Portál má plně responzivní design s automatickým přizpůsobením vzhledu zařízení, ze kterého je na portál přistupováno.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Portál umožňuje přehlednou a detailní správu referenčních objektů, na které se identity odkazují. Systém obsahuje referenční objekty typu systemizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát a další.	ACIdentitaUzivatelskaPrirucka.pdf
	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	Systém umožňuje přidávání a správu dalších typů referenčních objektů i v průběhu správy konkrétní identity s možností okamžitého použití	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
			referenčního objektu u právě spravované identity.	
	Zabezpečení referenčních objektů	Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů	Systém umožňuje nastavit vzájemně nezávislá administrátorská oprávnění pro správu jednotlivých referenčních objektů.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém umožňuje rozšiřování identit a referenčních objektů o další atributy a publikuje nové atributy externím aplikacím prostřednictvím rozhraní webových služeb	ACIdentitaUzivatelskaPrirucka.pdf
	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).	Systém obsahuje hierarchické stromové zobrazení organizační struktury. V zobrazení je možné vyhledávat identity včetně souvisejících uživatelských účtů i systematizovaná místo do úrovně uživatelských účtů a souvisejících identit.	ACIdentitaUzivatelskaPrirucka.pdf
	Vyhledávání – diakritika	Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Parizek vyhledává i Pařízek apod.)	Portál podporuje vyhledávání nezávislé na diakritice.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Součástí správy uživatelů (identit) je i správa údajů o uživatelských digitálních certifikátech. Data o certifikátech je možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožňuje automatické zneplatnění uložených certifikátů po vypršení data platnosti.	ACIdentitaUzivatelskaPrirucka.pdf
	Obrázky	Systém umožní k jednotlivým účtům (identitám) přikládat obrázky – fotografie.	Součástí správy identit je podpora přikládání obrázků / fotografií v běžných formátech, např. jpg.	ACIdentitaUzivatelskaPrirucka.pdf
	Přesun identit	Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními.	Identity je možné přesouvat mezi organizacemi i mezi jejich odděleními.	ACIdentitaUzivatelskaPrirucka.pdf
	Kopírování rolí	Systém umožní kopírovaní aplikačních rolí, pracovních pozic mezi jednotlivými systematizovanými místy.	Aplikační role i pracovní pozice lze kopírovat mezi systematizovanými místy.	ACIdentitaUzivatelskaPrirucka.pdf
	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).	Systém umožňuje zabránit hromadným změnám v případě chybných vstupních dat.	ACIdentitaUzivatelskaPrirucka.pdf
	Aktivní uživatelé	Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem	Systém obsahuje přehled aktuálně přihlášených / pracujících uživatelů portálu.	ACIdentitaUzivatelskaPrirucka.pdf
	Slučování identit	Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.	Systém plně podporuje slučování uživatelů/identit včetně sjednocení navázaných spravovaných účtů.	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	Export údajů	Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu	Integrované exporty portálem zobrazovaných přehledů a seznam a seznamů do CSV	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Integrovaný filtrovací nástroj s podporou vyhledávání identit a referenčních identit. Umožňuje filtrovat libovolné atributy identit včetně přidružených referenčních objektů. Nastavené filtry je možné ukládat pro opakované použití.	ACIdentitaUzivatelskaPrirucka.pdf
	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.)	Hierarchická správa oprávnění administrátorů. Možnost nastavení oprávnění na úrovni organizační jednotky a podřízených úrovní a detailní přiřazení rolí a oprávnění včetně přiřazení činnostní role, aplikační role i editace identity.	ACIdentitaUzivatelskaPrirucka.pdf
	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 uživatelů a správců lze definovat a přidělovat pro jednotlivé části systému – včetně identit, referenčních objektů, notifikací, synchronizací, konfigurací systému, reportů, workflow i webových služeb. Pro každou část je možné definovat akce, které může uživatel/správce s přidělenými oprávnění v konkrétní části IDM provádět.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Podpora definice oprávnění k atributům identit a referenčních objektů, možnost nastavení viditelnosti atributu, možnost uživatelské editace atributu, možnost povinného nastavení či vyplnění atributu, možnost nastavení pořadí atributů.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Na úrovní organizační jednotky je možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, pracovních pozic, systematizovaných míst dostupných pro identity z dané organizační jednotky.	ACIdentitaUzivatelskaPrirucka.pdf
	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 vytváření víceúrovňových schvalovacích workflow.	Integrovaná správa licencí pro jednotlivé evidované aplikace, možnost přiřazování licencí uživatelům/identitám.	ACIdentitaUzivatelskaPrirucka.pdf
	Časová omezení	IDM bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení	Podpora přiřazení rolí konkrétní identitě, systemizovanému místu, skupině i organizační jednotce s možnosti	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
		platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.	nastavení data a času expirace platnosti přiřazení a automatickým odebráním přiřazených rolí pro expiraci platnosti.	
	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.	Podpora přiřazení identit k systematizovaným místům ve vazbě M:N. Identitu lze v IDM evidovat na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém umožňuje zobrazit přidělené role 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.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém umožňuje evidovat a přehledně souhrnně zobrazovat všechny role včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny) nebo zda má nějakou roli od někoho delegovánu.	ACIdentitaUzivatelskaPrirucka.pdf
	Skupiny	IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.	Systém obsahuje správu skupin, které lze vícenásobně začleňovat. Do skupin lze přiřazovat jednotlivé uživatele i systematizovaná místa.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje správu vztahů zastupitelnosti mezi uživateli. Umožňuje uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby své 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.	ACIdentitaUzivatelskaPrirucka.pdf
	Delegování oprávnění	Možnost delegování administrátorských práv.	Systém umožňuje delegovat administrátorská práva.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje správu evidence osobních údajů. Obsahuje správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu jsou	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
			definována oprávnění i aplikační role pro přístup k osobním údajům.	
	Osobní údaje – automatizace	IDM bude obsahovat workflow pro správu životního cyklu osobních údajů subjektu údajů.	Systém obsahuje workflow pro správu životního cyklu osobních údajů subjektu údajů.	ACIdentitaUzivatelskaPrirucka.pdf
	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).	Systém obsahuje uživatelské rozhraní pro samoobslužný reset hesel jednotlivých účtů uživatele. Zasílání kódů pro reset hesla danému uživateli je možné pomocí SMS prostřednictvím vestavěných rozhraní na služby SMS operátorů nebo SMS bránu. Rozhraní umožňuje i běžnou změnu hesla – bez resetu.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje uživatelské samoobslužné rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny jsou kategorizovány a kategoriím je možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje uživatelské samoobslužné rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin.	ACIdentitaUzivatelskaPrirucka.pdf
	Kontextový výběr	Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.	Systém v rámci samoobslužného rozhraní umožňuje na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém uživatelům poskytuje možnost individuálního nastavení zobrazení rozhraní včetně zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku, a to pro každý seznam samostatně.	ACIdentitaUzivatelskaPrirucka.pdf
	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 - E-mailové upozornění schvalovatele na požadavek ke schválení	Systém obsahuje vestavěné workflow pro řízení životního cyklu změn identit a schvalování změn. Workflow poskytuje mimo jiné následující funkce: - Možnost sledování stavu svých požadavků uživateli	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
		- 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	- 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 zobrazení workflow např. aktivity diagram, BPMN nebo Archimate	Průběh workflow lze sledovat v grafické podobě ve formě diagramu se zřejmým stavem probíhajícího workflow ve formátu „activity diagram“	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém provádí automatické zasílání konfigurovatelných emailových upozornění, mj. 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.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém umožňuje zasílání upozornění na vypršení časových termínů v předstihu. Velikost předstihu je možné konfigurovat pro každý typ upozornění samostatně.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje správu šablon upozornění, které umožňují definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám je možné nastavovat různé příjemce pro různé části organizační struktury. Šablony umožňují vložit do obsahu	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
			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.	Systém umožňuje konfigurovat podmínky pro zaslání upozornění. V konfiguraci je možné využít všech atributů identit a referenčních objektů.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém provádí transakčně veškeré změny vyvolané požadavky uživatelů a administrátorů/správců. Změny jsou logovány pro zpětné prokázání co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci systému. Záznamy v logu obsahují původní i nové hodnoty.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém neumožňuje realizovat požadavky ručními změnami textových souborů. Požadavky je nutné zadávat prostřednictvím webového rozhraní – portálu.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje online „dashboard“ s přehledem o aktuálním stavu hlavních částí systému a případných chybách včetně chyb běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu workflow.	ACIdentitaUzivatelskaPrirucka.pdf
	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 na IDM, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.	Systém umožňuje export auditního reportu z údajů o uložených identitách, a to i historických. Auditní reporty lze exportovat ve formátu CSV a obsahují souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na systém, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.	ACIdentitaUzivatelskaPrirucka.pdf
	Auditní report – výběr	Identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů.	Identity pro generování auditního reporty lze vybrat dle libovolných atributů identity včetně přidružených referenčních objektů.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje reporty uživatelů s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
			jiných uživatelů. Reporty lze exportovat do CSV souboru.	
	Reporty – zasílání	Reporty bude možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel.	Systém umožňuje zasílat reporty automaticky e-mailem na základě konfigurovatelných pravidel.	ACIdentitaUzivatelskaPrirucka.pdf
	Reporty – historie	Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.	Systém umožňuje ukládat vygenerované reporty včetně možnosti pozdějšího zobrazení či stažení.	ACIdentitaUzivatelskaPrirucka.pdf
	Reporty – porovnání	Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu.	Systém umožňuje snadno porovnat změny mezi vygenerovanými reporty stejného typu ve webovém prostředí/portálu.	ACIdentitaUzivatelskaPrirucka.pdf
	Webové služby (WS)	IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.	Systém poskytuje rozhraní webových služeb pro napojení dalších systémů. Rozhraní lze konfigurovat ve webovém prostředí/portálu.	ACIdentitaUzivatelskaPrirucka.pdf
	Standardy WS	Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.	Systém poskytuje webové služby v rozšířeném standardu WSDL a podporovat protokol SOAP	ACIdentitaUzivatelskaPrirucka.pdf
	Bezpečnost WS	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.	Systém umožňuje konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.	ACIdentitaUzivatelskaPrirucka.pdf
	Logování WS	Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu	Přístup k webovým službám (volání služeb) je logováno a logy je možné zobrazit ve webovém prostředí/portálu.	ACIdentitaUzivatelskaPrirucka.pdf
	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	Rozhraní webových služeb poskytuje (mimo dalších) 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	ACIdentitaUzivatelskaPrirucka.pdf
	Synchronizace	Ruční i automatické spuštění synchronizací s propojenými systémy.	Systém umožňuje automaticky i ručně spouštět synchronizace s propojenými systémy.	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	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.	Synchronizace je možné spouště i v simulačním režimu režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy lze zobrazit ve webovém prostředí/portálu.	ACIdentitaUzivatelskaPrirucka.pdf
	Simulace – průběh	Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.	Jednotlivé stavy průběhu synchronizací lze přehledně zobrazit v grafické podobě.	ACIdentitaUzivatelskaPrirucka.pdf
	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 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.	Pro každý napojený systém lze používat více režimů synchronizace podle úrovně podpory napojeného systému. Systém umožnuje využívat synchronizace: plná. Změnová, okamžitá na vyžádání, rekoncilační, simulační. Systém zaznamenává všechny běhy synchronizací. Záznam je dostupný prostřednictvím webového rozhraní/portálu. Historie plné synchronizace zahrnuje odkazy na objekty, které byly synchronizovány a informaci, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak historii obsahuje i informace o události, která synchronizaci vyvolala.	ACIdentitaUzivatelskaPrirucka.pdf
	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.	Systém obsahuje správu 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 lze vybírat organizace, které se mají ze systému synchronizovat s danými systémy. Správa je součástí webového prostředí/portálu.	ACIdentitaUzivatelskaPrirucka.pdf
	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	Systém obsahuje integrované konektory pro správu identit v napojených systémech:	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
		- konektor pro napojení na SOAP a REST webové služby - konektor pro napojení na LDAP server s podporou LDAP v3	- 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.	Systém obsahuje konektor pro správu virtuálních aplikací, který umožňuje požadavky na správu identit ve virtuálních aplikacích předávat e-mailem správcům odpovídajících reálných aplikací a zaznamenávat potvrzení splnění požadavků.	ACIdentitaUzivatelskaPrirucka.pdf
	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 Objednatele bude IDM vytvářet a spravovat uživatelské účty. Dále bude spravovat oprávnění uživatelských účtů v systémech v rozsahu, který umožní a zajistí výrobce či Dodavatel daného systému provozovaného u Objednatele. Objednatel zajistí potřebnou součinnost výrobce či Dodavatele 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 Objednatele: - 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.)	Systém bude spravovat identity a řídit oprávnění včetně provádění souvisejících operací potřebných pro automatizaci správy identit v daném systému v: - nabízeném nástroji řízení přístupu do sítě podle standardu IEEE 802.1X - nabízeném nástroji pro správu a řízení oprávnění privilegovaných účtů - nabízeném nástroji pro správu identifikačních prostředků - Microsoft Active Directory - Microsoft Exchange Pro stávající systémy Objednatele bude systém vytvářet a spravovat uživatelské účty a spravovat jejich oprávnění v rozsahu, který umožní a zajistí výrobce či Dodavatel daného systému provozovaného u Objednatele. 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. Jedná se o systémy: - IS ZOS (výrobce Per4mance s.r.o.) - Elektronická karta pacienta (EKP) a Mobilní zadávání dat (MZD) (výrobce	ACIdentitaUzivatelskaPrirucka.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
		- NidlWare (výrobce Pavel Nídl) - AUTOPLAN (výrobce Krob Software s.r.o.) - ServiceDesk, Asset Management (výrobce Alvao s.r.o.)	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	Systém bude napojen na personální systém Avensio, který bude sloužit jako autoritativní zdroj identitních údajů. Budou z něj načítány budou načítány údaje o organizační struktuře, pracovních místech a funkcích, osobách.	ACIdentitaUzivatelskaPrirucka.pdf
	Záruka	Min. 60 měsíců včetně nároku na nové a opravné verze	60 měsíců včetně nároku na nové a opravné verze	Součástí cenové nabídky
Ověřovací systém – dispečink **Imprivata OneSign 30x licence AM/SSO/VDA/SSPW 2x licence virtální centrální appliance**	Obecné požadavky	Platforma pro zajištění služeb vícefaktorového a jednotného (SSO – single sign-on) ověřování	Softwarová platforma poskytující služby služeb vícefaktorového a jednotného (SSO) ověřování	Imprivata OneSign Single Sign-On.pdf
	Klientské systémy	Podpora desktopových a serverových Windows OS (verze 7/2008 a vyšší) a Linuxu	Systém podporuje desktopové i serverové Windows a Linux OS	OneSignSupportedComponents.pdf
	Vysoká dostupnost	Vysoce dostupná architektura z minimálně 2 automaticky zastupitelných prvků (cluster apod.) s jednotnou správou celého řešení	Architektura s vysokou dostupností sestavená ze 2 automaticky zastupitelných prvků s jednotnou správou celého řešení	OneSignSupportedComponents.pdf
	Virtualizace	Podpora provozu ve virtuálním prostředí nabízené serverové virtualizace	Systém podporuje stávající i nabízenou virtualizaci VMware vSphere	OneSignSupportedComponents.pdf
	Bezpečnost	Ověřování administrátorských účtů vůči Active Directory	Systém podporuje ověřování administrátorských účtů vůči Active Directory	OneSignSupportedComponents.pdf
	Adresářové služby	Podpora běžných adresářových služeb – Active Directory, LDAP	Systém podporuje běžné adresářové služby včetně Active Directory a LDAP	OneSignSupportedComponents.pdf
	Bezpečná komunikace	Komunikace mezi jednotlivými komponenty řešení (klient, server, adresářová služba apod.) je šifrována (SSL či kompatibilní)	Komponenty systému komunikují mezi sebou šifrovanými protokoly.	Security_Standards_Brief.pdf
	Autentizace	Zajištění ověření uživatele pro přihlášení k pracovní stanici (PC nebo tenký klient) s využitím více faktorů	Systém zajišťuje ověření uživatele pro přihlášení l pracovní stanici s využitím více faktorů – např. karta, PIN, biometrie	Imprivata OneSign Authentication Methods.pdf
	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.	Systém podporuje autentizační předměty (kontaktní čipové karty, bezkontaktní karty, USB a bezkontaktní tokeny), biometrické prvky (otisk prstu), kombinace jméno/heslo (s vazbou i bez vazby na Active Directory), PIN a jejich vzájemné kombinace.	Imprivata OneSign Authentication Methods.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	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.	Systém podporuje konfiguraci podmínek pro využití vícefaktorového ověřování – včetně dvoufaktorového ověřování povinného jen při prvním přihlášení v daném dni (pro další přihlášení postačí jeden faktor) apod.	Configuring Authentication Methods in User Policies.pdf
	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)	Systém podporuje seamless integraci přihlašovacího procesu bez nutnosti opakovaně zadávat přihlašovací údaje a potvrzovat připojovací dialogy s běžnými produkty pro virtualizaci aplikací a desktopů včetně Microsoft Remote Desktop Services, Citrix XenApp/XenDesktop	OneSignSupportedComponents.pdf
	Tencí klienti	Podpora náhrady běžného uživatelského rozhraní tenkého klienta přihlašovací obrazovkou pro vícefaktorové ověřování	Systém podporuje náhradu běžného uživatelského rozhraní tenkého klienta přihlašovací obrazovkou pro vícefaktorové ověřování	OneSignSupportedComponents.pdf
	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.	Systém podporuje scénáře Koncová stanice v roli kiosku", "Rychlé střídání uživatelů u koncové stanice", "Uživatel přecházející mezi koncovými stanicemi" na běžných PC s OS Windows/Linux i na tenkých klientech	OneSignSupportedComponents.pdf
	Rychlé přihlášení	Podpora rychlého přihlášení, resp. přehlášení uživatele včetně přenesení otevřeného pracovního prostředí (viz. Scénáře) při použití bezkontaktních identifikačních prostředků.	Systém podporuje rychlé přihlášení i přehlášení uživatele včetně přenesení otevřeného pracovního prostředí při použití bezkontaktních identifikačních prostředků.	Configuring Walk-Away Security for Unattended Workstations.pdf
	Obecné požadavky	Podpora jednotného (SSO) automatického přihlášení uživatele do libovolných desktopových aplikací včetně jejich automatického spuštění pro přihlášení do operačního systému.	Systém podporuje automatické jednotné přihlášení (SSO) do libovolných desktopových aplikací včetně jejich automatického spuštění po přihlášení do operačního systému.	Imprivata OneSign Single Sign-On.pdf
	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.	Systém podporuje SSO přihlášení do Windows aplikací, webových aplikací včetně Java aplikací, terminálových aplikací používajících znakové rozhraní apod. Funkčnost nevyžaduje úpravu aplikací.	Application types.pdf
	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.	Přihlašovací údaje do aplikací jsou dostupné jen příslušnému uživateli. Přihlašovací údaje jsou ukládány v ověřovací platformě a jsou centrálně	The Imprivata OneSign Password Manager.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
			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.	Systém obsahuje intuitivní podporu vytváření a správu předpisů (profilů) pro jednotlivé aplikace bez psaní kódu, používání řádkových příkazů apod. Vytvořené předpisy (profily) aplikací je možné přidělovat uživatelům na základě členství v Active Directory skupinách	Imprivata OneSign Single Sign-On.pdf
	Licence	Min. pro 30 uživatelů	Pro 30 uživatelů	Součástí cenové nabídky
	Záruka	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze	Součástí cenové nabídky
Ověřovací systém MONET ProID Kartové centrum + MONET ProID ACEx + MONET ProID Správce karty + Microsoft certifikační autorita + Microsoft Active Directory	Základní popis	Systém pro autentizaci uživatele identifikačním prostředkem vůči adresářové služeb včetně nástrojů pro správu osobního identifikačního prostředku	Systém sestavený s MONET ProID Kartové centrum (Správa certifikátů) + MONET ProID ACEx (obnova certifikátů) + Microsoft certifikační autorita + Microsoft Active Directory s využitím stávajících licencí Microsoft	ProID+KartoveCentrum.pdf ProID+ACEx.pdf ProID+SpravceKarty.pdf WindowsServerSmartCard.pdf
	Rozhraní	Grafické rozhraní v českém jazyce	Všechny komponenty řešení mají grafické rozhraní v českém jazyce.	ProID+KartoveCentrum.pdf ProID+ACEx.pdf ProID+SpravceKarty.pdf WindowsServerSmartCard.pdf
	Obnova certifikátů	Automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů a vyvolání průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik	ACEx zajišťuje automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů a vyvolání průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik	ProID+ACEx.pdf
	Autentizace	Autentizace uživatele ve operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem (Microsoft)	Windows Active Directory (Windows Server) zajišťuje autentizaci uživatele ve operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem (Microsoft)	WindowsServerSmartCard.pdf
	Správa	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK, ..)	Správce karty umožňuje uživatelskou správu uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK, ..)	ProID+SpravceKarty.pdf
	Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti	Správce karty a Kartové centrum umožňují export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti	ProID+KartoveCentrum.pdf ProID+SpravceKarty.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	Předávání veřejných doménových klíčů	Automatizované předávání veřejných klíčů doménových certifikátů do stávajícího systému Microsoft Active Directory	Automatizované předávání veřejných klíčů doménových certifikátů do stávajícího systému Microsoft Active Directory bude zajištěno použitím Microsoft Windows certifikační autority pro doménové certifikáty	AD_PKI.pdf
	Licence	pro 250 uživatelů (včetně externích)	Licence pro 250 uživatelů	Součástí cenové nabídky
	Záruka	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze	Součástí cenové nabídky
Identifikační karty hybridní 300 ks **300x Karta ProID+Q + Mifare DESFire EV1 4K**	Základní popis	Hybridní identifikační karta s kontaktní částí SmartCard a bezkontaktní částí typu Mifare DESFire EV1 4K 13,56 MHz)	Hybridní karta Karta ProID+Q + Mifare DESFire EV1 4K	ProID+Q.pdf https://1url.cz/nrPI4
	Veřejné certifikáty	Karta musí umožnit ukládání a používání vlastních doménových certifikátů a certifikátů veřejných certifikačních autorit – např. I. CA, Postsignum apod.	Karta umožňuje ukládání a používání vlastních doménových certifikátů a certifikátů veřejných certifikačních autorit včetně I. CA, Postsignum apod.	ProID+Q.pdf https://1url.cz/nrPI4
	Identity	Karta musí umožnit ukládání více identit	Karta podporuje ukládaní více identit / certifikátů	ProID+Q.pdf https://1url.cz/nrPI4
	Kvalifikovaný prostředek	Karta musí být možno využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku)	Kartu lze využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku)	ProID+Q.pdf https://1url.cz/nrPI4
	Softwarová podpora	Součástí dodávky bude software pro zpřístupnění jejich rozhraní v operačním systému včetně rozšířených funkcionalit, tzv. Middleware	Middleware k nabízeným kartám je součástí dodávky a volně ke stažení	ProID+Q.pdf https://1url.cz/nrPI4 https://proid.cz/ke-stazeni/
	Záruka	24 měsíců	Záruka 24 měsíců	Součástí cenové nabídky
Identifikační tokeny 140 ks **140x USB token ProID+Q**	Základní popis	Identifikační USB s čipovou částí (SmartCard)	USB identifikační token s čipovou částí SmartCard	ProID+Q.pdf https://1url.cz/nrPI4 https://proid.cz/ke-stazeni/
	Veřejné certifikáty	Token musí umožnit ukládání a používání vlastních certifikátů a certifikátů veřejných certifikačních autorit – např. I. CA, Postsignum apod.	Token umožňuje ukládání a používání vlastních doménových certifikátů a certifikátů veřejných certifikačních autorit včetně I. CA, Postsignum apod.	ProID+Q.pdf https://1url.cz/nrPI4 https://proid.cz/ke-stazeni/
	Identity	Token musí umožnit ukládání více identit	Token podporuje ukládaní více identit / certifikátů	ProID+Q.pdf https://1url.cz/nrPI4 https://proid.cz/ke-stazeni/
	Kvalifikovaný prostředek	Token musí být možno využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku)	Token lze využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku)	ProID+Q.pdf https://1url.cz/nrPI4 https://proid.cz/ke-stazeni/
	Softwarová podpora	Součástí dodávky bude software pro zpřístupnění jejich rozhraní v operačním systému včetně rozšířených funkcionalit, tzv. Middleware	Middleware k nabízeným tokenům je součástí dodávky a volně ke stažení	ProID+Q.pdf https://1url.cz/nrPI4 https://proid.cz/ke-stazeni/
	Záruka	24 měsíců	Záruka 24 měsíců	Součástí cenové nabídky
	Provedení	externí, připojitelná přes USB	Externí čtečka připojeitelná přes USB	Omnikey.pdf

Komodita K.2 – Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
Čtečky bezkontaktních karet 10 ks **10x OMNIKEY 5022**	Standardy	podpora obvyklých standardů 13,56 MHz – MIFARE (Classic, Ultralight, Ultralight C / Plus), DESFire, DESFire EV1, DESFire EV2, iCLASS. Čtení i zápis	Podporuje standardy 13,56 MHz – MIFARE (Classic, Ultralight, Ultralight C / Plus), DESFire, DESFire EV1, DESFire EV2, iCLASS. Čtení i zápis	Omnikey.pdf
	Napájení	USB	Napájení prostřednictvím USB	Omnikey.pdf
	Kompatibilita	Windows 7 a vyšší (32 a 64 bit), Linux, MacOS	Kompatibilita Windows Vista+/Server 2008R2+, Linux, MacOS	Omnikey.pdf
	Kompatibilita	s nabízenými tenkými klienty a Ověřovacím systémem – dispečink	Čtečka je kompatibilní s nabízeným tenkými klienty (USB) a Ověřovacím systémem – dispečink (Mifare)	Omnikey.pdf
	Záruka	24 měsíců	Záruka 24 měsíců	Součástí cenové nabídky
Čtečka hybridních karet 120 ks **120x Gemalto/Thales IDBridge CT30**	Provedení	čtečka nabízených čipových (SmartCard) karet, připojitelná přes USB	IDBridge CT30 USB čtečka kontaktních čipový karet (SmartCard)	IDBridge_CT30.pdf
	Provedení	kvalitní provedení, výrobcem deklarovaná trvanlivost min. 100 000 zasunutí/vysunutí karty	Kvalitní provedení, min. 100 000 „insertion cycles“	IDBridge_CT30.pdf
	Kompatibilita	Windows 7 a vyšší (32 a 64 bit), Linux, MacOS	Windows 7 a vyšší, Linux, MacOS	IDBridge_CT30.pdf
	Kompatibilita	s nabízenými počítači a Ověřovacím systémem	Komaptibilní s nabízenými počítači (USB) a Ověřovacím systémem (SmartCard)	IDBridge_CT30.pdf
	Záruka	24 měsíců	24 měsíců	Součástí cenové nabídky

(5) 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**	**Dodavatel popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Dodavatel uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém řízení a monitorování privilegovaných účtů **AC PIMPAM**	Základní popis	Proxy brána určená pro správu a monitoring privilegovaných přístupů	Brána proxy pro správu a monitorování privilegovaných přístupů	ACPimPamUzivatelskaPrirucka.pdf
	Záznam relací	Zaznamenávání uživatelských relací včetně vytváření logů	Systém zaznamenává uživatelské relace vytváří logy o těchto relacích	ACPimPamUzivatelskaPrirucka.pdf
	Logování relací	Nepozměnitelné podklady pro audit a analytické reporty uživatelského chování	Systém ukládá a poskytuje nepozměnitelné podklady pro audit a analytické reporty uživatelského chování	ACPimPamUzivatelskaPrirucka.pdf
	Metadata	Ukládání metadat záznamů pro snadnou orientaci při prohlížení a vyhledávání (min. stisky kláves, kliknutí)	Systém ukládá metadata záznamů relací včetně stisků kláves a kliknutí a umožňuje snadnou orientaci při prohlížení a vyhledávání	ACPimPamUzivatelskaPrirucka.pdf
	Architektura	Samostatná virtuální aplliance, bezagentové řešení (bez nutnosti instalace agentů na monitorované systémy)	Architektura systém je koncipována jako samostatná virtuální appliance, systém nevyžaduje instalaci agentů na monitorované systémy (jedná se o bez agentové řešení)	ACPimPamUzivatelskaPrirucka.pdf

Komodita K.3 – Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS				
	Autentizace	LDAP, Microsoft Active Directory, Radius, TACACS+, Kerberos, X.509, OTP, Web SSO, podpora vícefaktorové autentizace (MFA)	Systém podporuje přímou nebo zprostředkovanou autentizaci prostřednictvím LDAP, MS AD, RADIUS, TACACS+, Kerberos, X.509, OTP, web SSO a podporuje i vícefaktorovou autentizaci (MFA)	ACPimPamUzivatelskaPrirucka.pdf
	Autorizace	Integrované pokročilé workflow pro autorizaci (povolené časy a trvání relace, white/black listy, rozpoznání činnosti v RDP relaci, parametry relace apod.)	Systém obsahuje pokročilé workflow pro řízení autorizace a umožňuje konfigurovat povolené časy a trvání relace, white/black listy, rozpoznání činnosti v RDP relaci i parametry relace	ACPimPamUzivatelskaPrirucka.pdf
	Bezpečné přihlášení	Uživatel privilegovaného účtu se přihlašuje pouze k proxy. Přihlášení k cílovému systému zajišťuje proxy – uživatel nezná přístupové údaje k cílovému systému	Systém poskytuje bezpečné (zprostředkované) přihlášení – uživatel privilegovaného účtu se přihlašuje pouze k systému AC PIMPAM, který zajišťuje přihlášení k cílovému systému, aniž by uživatel znal přístupové údaje k cílovému systému.	ACPimPamUzivatelskaPrirucka.pdf
	Přístupové protokoly a aplikace	Proxy umožňuje zprostředkované (bez znalosti hesla cílového systému) přihlášení k cílovým systémům min. RDP, SSH, Microsoft SQL management, webová GUI	Systém podporuje zprostředkované (bezpečné) přihlášení k cílovým systémům RDP, ssh, MS SQL management, webová grafická rozhraní (GUI)	ACPimPamUzivatelskaPrirucka.pdf
	Notifikace	Zasílání notifikací o zahájení definované relace	Systém umožňuje zaslat notifikaci o zahájení definované relace.	ACPimPamUzivatelskaPrirucka.pdf
	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)	Systém bude integrován s nabízeným systémem AC Identita (IDM), nabízeným systémem LOGManager pro správu logů podporuje integraci s obecnými tiketovacími systémy třetích stran (žádost o schválení přístupu, přístup na základě existujícího tiketu)	ACPimPamUzivatelskaPrirucka.pdf
	Řízení v realném čase	Monitorování relací v raálném čase a jejich okamžité ukončení v případě potřeby	Systém umožňuje monitorovat relace v reálném čase a provést jejich okamžité ukončení v případě potřeby	ACPimPamUzivatelskaPrirucka.pdf
	Vysoká dostupnost	Integrovaná podpora high-availability clusterů: Active/Passive nebo Active/Active	Systém má integrovánu podporu vysoké dostupnosti v režimu clusteru active/passive	ACPimPamUzivatelskaPrirucka.pdf
	Rozšiřitelnost	Podpora modulů (plug-in) pro integraci s dalšími technologiemi / technologickými partnery	Systém je rozšiřitelný o zásuvné moduly pro dalšími technologiemi resp. technologickými partnery	ACPimPamUzivatelskaPrirucka.pdf
	Rozhraní	Webové rozhraní pro přístup uživatelů I konfiguraci, bezpečná publikace do internetu (šifrovaná komunikace)	Systém obsahuje webové rozhraní pro přístup uživatelů I konfiguraci, lze jej bezpečně publikovat do internetu a	ACPimPamUzivatelskaPrirucka.pdf

Komodita K.3 – Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS				
			vynutit šifrovanou komunikaci – např. SSL	
	Zabezpečení přístupových údajů	Integrované bezpečné (šifrované) úložiště přístupových údajů k cílovým systémům	Systém obsahuje integrované bezpečné (šifrované) úložiště přístupových údajů k cílovým systémům	ACPimPamUzivatelskaPrirucka.pdf
	Aktivní bezpečnost	Upozornění a automatické ukončení podezřelé činnosti nebo neoprávněných pokusů o přístup	Systém podporuje upozornění a automatické ukončení podezřelé činnosti nebo neoprávněných pokusů o přístup	ACPimPamUzivatelskaPrirucka.pdf
	SIEM	Podpora odesílání záznamů a událostí do systému SIEM (Security Information and Event Management)	Systém podporuje odesílání záznamů a událostí do systému SIEM	ACPimPamUzivatelskaPrirucka.pdf
	Logy	Nesmazatelnost logů po dobu minimálně 30 dní. Uložení auditních záznamů v zašifrované podobě s přístupem pouze oprávněných uživatelů	Systém zajišťuje nesmazatelnost logů po dobu minimálně 30 dní a uložení auditních záznamů v zašifrované podobě s přístupem pouze oprávněných uživatelů	ACPimPamUzivatelskaPrirucka.pdf
	Bezpečnostní standardy	Podpora zajištění shody se standardy HIPAA, GDPR, PCI, SOX	Systém poskytuje podporu zajištění shody se standardy HIPAA, GDPR, PCI, SOX	ACPimPamUzivatelskaPrirucka.pdf
	Zálohování	Šifrování záloh, přístup k zálohovaným datům výhradně pomocí zabezpečených Disaster Recovery klíčů.	Systém podporuje šifrování záloh a přístupem k zálohovaným datům výhradně pomocí zabezpečených Disaster Recovery klíčů.	ACPimPamUzivatelskaPrirucka.pdf
	Licence	Licence pro monitorování a záznam min. 10 současně pracujících (privilegovaných) uživatelů, min. 100 cílových systémů.	Licence pro 100 cílových systémů bez omezení počtu uživatelů	Součástí cenové nabídky
	Záruka	min. 60 měsíců včetně nároku na podporu výrobce a aktualizace systému včetně nových hlavních verzí	60 měsíců včetně nároku na podporu výrobce a aktualizace systému včetně nových hlavních verzí	Součástí cenové nabídky

(6) 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**	**Dodavatel popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Dodavatel uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém pro správu logů LOGManager-M server DELL	Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware	LOGmanager je systém pro zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware	Logmanager Datasheet.pdf
	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 Objednatele	Systém bude dodán ve formě hardwarové appliance (hw se specializovaným firmware/software) a bude samostatně funkční nezávisle na infrastruktuře Objednatele	Logmanager Datasheet.pdf

Komodita K.4 – Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
	Provedení	Určené pro montáž do stávajícího serverového datového rozvaděče 19", hloubka max 900 mm, včetně výsuvných kolejnic a ramene pro vedení kabelů.	Systém je určen pro montáž do 19“ datového rozvaděče, hloubka je menší než 800 mm a součástí dodávky budou výsuvné kolejnice a rameno pro vedení kabelů.	Logmanager Datasheet.pdf
	Ovládání	Grafická webová konzole pro administrátory I operátory, umožňuje kompletní správu systému včetně úvodního nastavení.	Systém je ovládán prostřednictvím grafická webová konzole pro administrátory I operátory, konzole umožňuje kompletní správu systému včetně úvodního nastavení.	Logmanager Datasheet.pdf Logamanager Dokumentace.pdf
	Autentizace	Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze.	Systém podporuje autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP systém umožňuje autentizaci z lokální databáze.	Logamanager Dokumentace.pdf
	Uživatelské role	Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému.	Systém obsahuje podpora uživatelských rolí, které obsahují přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému.	Logamanager Dokumentace.pdf
	Sběr dat (logů)	Bezagentový sběr logů s výjimkou systémů Windows	Systém zajišťuje bezagentový sběr logů z podporovaných systém s výjimkou Windows OS. Pro detailní logování OS Windows je vhodné do OS instalovat agenty, které jsou součástí dodávky.	Logamanager Dokumentace.pdf
	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	Agenty OS Windows je možné spravovat a aktualizovat z administrátorské konzole systému. Agent se systémem komunikuje šifrovaně, obsahuje lokální buffer pro případ ztráty komunikace, provádí překlad kódů na text poskytuje textový popis události shodný s Windows Event Viewerem	Logamanager Dokumentace.pdf
	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).	Systém podporuje příjem a zpracování logů, událostí i dalších strojově generovaných dat protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně).	Logamanager Dokumentace.pdf
	Formáty logů	Mini. RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog	Systém podporuje formáty logů RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog a další, včetně vlastních parserů.	Logamanager Dokumentace.pdf
	Třídění logů	Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv.	Systém podporuje příjem logů na rozsahu více než 50 TCP a UDP portů pro zjednodušené třídění vstupních zpráv	Logmanager Dokumentace.pdf

Komodita K.4 – Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
	Zpracování logů	Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy	Systém obsahuje parsování a normalizaci přijatých událostí/logů. Není nutné instalovat externí aplikace nebo systémy	Logmanager Dokumentace.pdf
	Ochrana logů	Zamezení mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci.	Systém zamezuje mazání nebo modifikování již uložených logů. Každý log má unikátní identifikátor pro jeho jednoznačnou identifikaci.	Logmanager Dokumentace.pdf
	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.	Systém obsahuje grafická vizualizaci logů, událostí a strojových dat (grafy událostí) včetně dynamická vizualizace – změnou volby (filtru apod.) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Systém mám Integrovánu podporu zobrazení TOP X událostí za zvolené časové období.	Logmanager Datasheet.pdf Logmanager Dokumentace.pdf
	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	Systém obsahuje předpřipravené dashboardy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. Dashboardy jsou průběžné aktualizovány výrobcem. Systém má integrovánu podporu tvorby uživatelských dashboardů včetně ukládání.	Logmanager Dokumentace.pdf
	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	Systém poskytuje ochranu proti ztrátě logů při přetížení systému. Ukládá nezpracované logy/události do vyrovnávací paměti o kapacitě větší než 25 GB a notifikuje správce systému při riziku zaplnění vyrovnávací paměti	Logmanager Dokumentace.pdf
	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.	Systém má vestavěnu podporu doplňování logů dalšími údaji včetně umístění zařízení, typu zařízení, kritičnost zařízení a dalších k jednotlivým zdrojům dat, aplikacím, zařízením i IP rozsahů.	Logmanager Dokumentace.pdf
	Archivace	Integrovaná archivace logů včetně zajištění integrity archivů, obnova	Systém obsahuje archivaci logů včetně zajištění integrity archivů a umožňuje jejich obnovu	Logmanager Dokumentace.pdf
	Rozpoznávání IP, MAC	Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce podle MAC adresy	Systém automaticky doplňuje reverzní DNS záznamy k IP adresám a výrobce podle MAC adresy	Logmanager Dokumentace.pdf
	Časová razítka	Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, slouží jako výchozí časový údaj pro systém	Systém mám integrovánu podporu doplňkové značky (razítka) navíc k časovému údaji zaznamenané	Logmanager Dokumentace.pdf

Komodita K.4 – Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
			událostí/logu a tato značka 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.	Systém poskytuje jednoduché multikriteriální vyhledávání událostí bez nutnosti speciálních znalosti (např. SQL dotazů apod.) napříč všemi typy dat a zařízení.	Logmanager Dokumentace.pdf
	Rychlé vyhledávání	Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování)	Systém průběžně indexuje ukládané položky a poskytuje rychlé vyhledávání i v aktuálně uložených položkách	Logmanager Dokumentace.pdf
	Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran	Systém automaticky doplňuje geolokační informace k událostem z interní databáze a umožňuje jejich grafické znázornění na mapě bez služeb třetích stran	Logmanager Dokumentace.pdf
	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.	Systém obsahuje integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (např. SQL dotazů apod.). Výrobce průběžně aktualizuje přednastavené reporty.	Logmanager Dokumentace.pdf
	Integrace	Integrované REST API rozhraní pro napojené systémy, musí umožnit autorizovaný přístup ke strukturované databázi logů.	Systém obsahuje integrované REST API rozhraní pro napojené systémy, které umožňuje autorizovaný přístup ke strukturované databázi logů. Přístup k API je součástí dodávky.	Logmanager Dokumentace.pdf
	Parsery	Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění – okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb	Systém obsahuje integrovaný grafický vizuální nástroj pro tvorbu vlastních parserů logů. Nástroj umožňuje testování a ladění parserů formou okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb	Logmanager Dokumentace.pdf
	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	Systém obsahuje specifické parsery Active Directory, Vmware, Windows (vč. DNS, DHCP), Exchange, MS SQL, Fortinet, HPE/Aruba, Dell servery, Synology, Linux, Apache i nabízený Systém pro analýzu síťového provozu GreyCortex	Logmanager Dokumentace.pdf
	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.	Systém obsahuje předpřipravené alerty a integrovaný grafický vizuální nástroj pro uživatelské vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Systém podporuje	Logmanager Dokumentace.pdf

Komodita K.4 – Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
			odesílání alertů SMTP, Syslog, TCP protokoly	
	Výkon	Min. 2000 EPS (events per second), krátkodobá (min. 10 min) přetižitelnost systému 200%	Trvalý výkon systému je 2000 EPS, s krátkodobou přetížitelností 200% po dobu 10 min.	Logamanager Datasheet.pdf Logmanager Dokumentace.pdf
	Kapacita	Využitelná diskové kapacita pro ukládání data min. 12 TB, disky musí být chráněny min. RAID 5	Čistá využitelná diskové kapacita pro ukládání data je 12 TB, disky jsou chráněny RAID 5	Logmanager Dokumentace.pdf
	Řízení diskového systému	Hardwarový řadič RAID se zálohovanou vyrovnávací pamětí (zápis I čtení) o kapacitě min 2 GB	Systém obsahuje hardwarový řadič RAID s vyrovnávací paměti read/write 2 GB (součást serveru DELL, který je základem appliance)	Logamanager Datasheet.pdf Logmanager Dokumentace.pdf
	Úložiště logů	Logy musí být ukládány do databáze (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat.	Logy jsou ukládány do interní databáze systému jejíž licence je součástí licence systému, databáze podporuje kompresi ukládaných dat.	Logmanager Dokumentace.pdf
	Napájení	Systém musí mít redundantní napájení (min. 2 nezávislé zdroje)	Systém obsahuje 2 nezávislé zdroj, konfigurované pro redundanci napájení (součást serveru DELL, který je základem appliance)	Logmanager datasheet.pdf Logmanager Dokumentace.pdf
	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.	Systém obsahuje 2x LAN 1 Gb port + 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 (součást serveru DELL, který je základem appliance).	Logmanager Datasheet.pdf Logmanager Dokumentace.pdf
	Aktualizace	Integrovaná aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade	Systém obsahuje integrovaný nástroj pro aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade.	Logmanager Dokumentace.pdf
	Zálohování	Integrované zálohování a obnova konfigurace	Systém obsahuje integrované zálohování a obnova konfigurace.	Logmanager Dokumentace.pdf
	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.	Systém podporuje škálovatelnost propojením s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, celkového výkonu včetně vyhledávání a dostupnosti. Navenek se propojené systémy chovají jako jeden.	Logmanager Dokumentace.pdf
	Dokumentace	Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce	Součástí dodávky a podpory systému je plnohodnotná dokumentace v českém	Logmanager Dokumentace.pdf

Komodita K.4 – Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
			jazyce (výrobcem je česká společnost). Anglická dokumentace je obsahově totožná s českou.	
	Záruka	Min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace	60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace	Součástí cenové nabídky

(7) 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**	**Dodavatel popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Dodavatel uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém pro analýzu síťového provozu **GREYCORTEX All-in-one model XS + MA-SC-200-SW**	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	Systém umožnuje monitorování síťové aktivity v reálném čase, identifikaci potenciálních kybernetických hrozeb a bezpečnostních rizik a anomálního chování a tvorbu upozornění o jejich výskytu v reálném časem	GREYCORTEX Datasheet.pdf
	Architektura	Integrovaná aplliance (hw se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), provozovaný v prostředí Objednatele. Samostatně funkční nezávisle na infrastruktuře Objednatele či dalších (např. cloudových) službách.	Systém bude dodán jako all-in-one integrovaná appliance – hw se specializovaným firmware.	GREYCORTEX Datasheet.pdf
	Provedení	Určené pro montáž do stávajícího serverového datového rozvaděče 19", hloubka max 900 mm, včetně výsuvných kolejnic a ramene pro vedení kabelů.	Hardwarovou základnou systému je server DELL R350 určený pro montáž do stávajícího serverového datového rozvaděče 19". Hloubka do 800 mm, součástí dodávky budou výsuvné kolejnic a rameno pro vedení kabelů.	GREYCORTEX Datasheet.pdf
	Ovládání	Grafická webová konzole (HTTPS) pro administrátory I operátory, pro správu a používání systému. SSH pro CLI – automatizace, monitorování.	Systém obsahuje jednotnou grafickou webovou konzoli s podporou https pro administrátory i operátory pro správu a používání systému. Dále disponuje SSH přístupem s CLI pro ovládání, automatizaci a monitorování.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	Viditelnost	Systém zajišťuje detailní viditelnost do síťové komunikace s "drill down" prokliky na veškerá uložená data.	Systém poskytuje detailní viditelnost do síťové komunikace s podporou "drill down" prokliků do veškerých uložených dat.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	Sběr dat	Systém bude získávat data na základě zrcadleného síťového provozu bez potřeby instalace agentů na zařízení v síti.	Systém umožňuje a bude konfigurován pro získávání dat na základě zrcadleného	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf

Komodita K.5 – Zavedení nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS				
			síťového provozu bez potřeby instalace agentů na zařízení v síti.	
	Zrcadlení komunikace	Podpora SPAN portů a síťových TAPů pro získávání dat zrcadlené komunikace	Systém podporuje SPAN porty a síťové TAPy pro získávání dat zrcadlené síťové komunikace	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	Pasivní sběr	Systém bude zcela pasivní vůči síťovém provozu, monitorovaný provoz přes systém nebude procházet a systém jej nebude nijak ovlivňovat.	Systém je zcela pasivní vůči síťovém provozu, monitorovaný provoz přes systém neprochází a systém síťový provoz nijak neovlivňuje.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	Netflow protokoly	Systém umožní analyzovat síť na základě zpracování statistických protokolů typu NetFlow v5, NetFlow v9, IPFIX, NetStream a případně dalších ekvivalentních.	Systém umožňuje analyzovat síť na základě zpracování statistických protokolů typu NetFlow v5, NetFlow v9, IPFIX, NetStream a kompatibilních.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	Záznam provozu	Zaznamenávání síťového provozu, minimálně základních parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6.	Systém zaznamenává síťový provoz včetně parametrů cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	Integrace	Integrace s nabízeným Systémem pro správu, minimálně v úrovni syslog	Systém bude integrován s nabízeným systémem pro správu logů LOGmanager na úrovní syslog a předpřipravené integrace v systému LOGmanager	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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	Systém získává, vizualizuje a integruje kontextuální informace v jednotném grafickém rozhraní včetně hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS provozu a Active Directory a IP geolokace	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	Monitorování zařízení	Identifikace zařízení v síti (koncová zařízení, servery, IoT, síťové prvky), rozpoznání změn v síti a notifikace výskytu nového zařízení (obecně assetu)	Systém umožňuje identifikovat zařízení v síti včetně koncových zařízení, serverů, IoT a síťových prvků. Systém rozpoznává změny v síti a notifikuje o výskytu nového zařízení / assetu.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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.	Systém obsahuje integrovaný modul/funkcionalitu pro detailní analýzu sítě včetně 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.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf

Komodita K.5 – Zavedení nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS				
	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	Systém umožňuje zobrazit síťový provoz a provádět jeho hloubkovou analýzu – okamžité vyhledávání a vizualizaci pro forenzní analýzu a podporu threat huntingu bez speciálního dotazovacího jazyka a bez hlubokých znalostí konkrétních komunikačních protokolů	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	HTTP komunikace	Podpora pro příjem a analýzu HTTP provozu – včetně položek typu URL a hostname	Systém obsahuje podpora pro příjem a analýzu HTTP provozu včetně položek typu URL a hostname	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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 služeb. Schopnost identifikace nestandardního síťové chování na základě modelu chování daného zařízení a jeho služeb.	Systém obsahuje integrované strojové učení - samostatné učení na základě matematických metod pro analýzu síťové aktivity, vytváření a disponuje automatickou průběžnou modifikací modelů chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb. Systém umožňuje identifikovat nestandardní síťové chování na základě modelu chování daného zařízení a jeho služeb.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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	Systém umožňuje detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Umožňuje identifikovat příznaky potenciálně škodlivého chování jako jsou 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	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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.	Systém disponuje detekcí nežádoucích vzorů chování na síti jako jsou útoky, anomálie datového provozu, nežádoucí aplikace, viry a botnety ve vnitřní síti, odchozí spam a provozní problémy. Podporuje detekci anomálií vzhledem k dlouhodobému profilu chování zařízení na síti.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	False-positive události	Integrovaná podpora identifikace neplatných událostí pomocí mechanismu false-positives, potlačení identifikovaných událostí při příštím výskytu	Systém obsahuje integrovanou podporu identifikace neplatných událostí pomocí mechanismu false-positives a umožňuje	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf

Komodita K.5 – Zavedení nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS				
			potlačit takto identifikované události při příštím výskytu	
	Autentizace	Podpora autentizace vůči LDAP, včetně podpory RBAC (přiřazení úrovně oprávnění na základě členství uživatele v konkrétní LDAP skupině).	Systém podporuje autentizaci vůči LDAP a Active Directory včetně podpory RBAC (přiřazení úrovně oprávnění na základě členství uživatele v konkrétní LDAP/AD skupině).	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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.	Systém obsahuje funkcionalitu tvorby 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). Funkcionalita umožňuje generovat statistiky a podrobné výpisy ve volitelných časových intervalech. Systém umožňuje tvorbu Top N statistik podle různých kritérií včetně počtu přenesených bytů, paketů a toků pro výpis nejaktivnějších či anomálně komunikujících assetů.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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.	Systém umožňuje vytvářet automatizované manažerských reportů včetně možnosti exportu do PDF a CSV formátu. Podporuje automatické zasílání reportů emailem a obsahuje předpřipravené reporty v českém i anglickém jazyce.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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.	Systém obsahuje předpřipravené a umožňuje vytvářet uživatelské notifikace na základě překročení prahových hodnot definovaných při implementaci či v průběhu provozu. Systém je schopen upozorňovat a informovat uživatele prostřednictvím e-mailu o všech identifikovaných událostech a událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. Systém podporuje logování notifikací.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	Výkon	min. 0,2 Gb/s trvalý síťový provoz, min. 200 Netflow/sec	Nabízená konfigurace umožňuje trvalý provoz 200 Mbps (0,2 Gb/s), 250 obohacených toků za sekundu a 500	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf

Komodita K.5 – Zavedení nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS				
			Netflow za sekundu z 500 monitorovaných adres.	
	Kapacita	úložná kapacita SSD s ochranou min. RAID 1 pro min. 30 denní historii při plném výkonu	Úložná kapacita SSD 800 GB s ochranou RAID1 pro min. 30 denní historii při plném výkonu.	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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.	Systém bude vybaven 2x LAN 1Gb portem pro monitorování a 1x 1Gb portem 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 (součást iDRAC serveru DELL R350).	GREYCORTEX Datasheet.pdf GREYCORTEX Dokumentace.pdf
	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	60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace	Součástí cenové nabídky

(8) Požadavky na nástroje pro zajišťování úrovně dostupnosti informací

Komodita K.6 – Nástroje pro zajišťování úrovně dostupnosti informací				
Část	**Parametr**	**Popis povinného parametru**	**Dodavatel popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Dodavatel uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Rozšíření stávajících serverů **Originální paměťové moduly, SSD disky, HBA a BOSS DELL**	RAM	18x modul 32 GB RAM 2Rx4 DDR4 RDIM 2666 MHz 6x modul 32 GB RAM 2Rx4 DDR4 RDIM 2933 MHz	Originální paměťové moduly DELL pro servery R640 a R740 18x 32 GB RAM 2Rx4 DDR4 RDIM 2666 MHz 6x 32 GB RAM 2Rx4 DDR4 RDIM 2933 MHz	DELL_R640.pdf DELL_R740.pdf
	HBA	3x HBA SAS 12Gb včetně kabeláže, kompatibilita s nabízenou diskovou virtualizací.	Řadič DELL HBA330 pro servery DELL R740	DELL_R740.pdf
	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	Originální SSD DELL 6x 960 GB SSD SATA Mixed Use 6Gbps 512e, 2.5" Hot-Plug 12x 3.84TB SSD SATA Read Intensive 6Gbps 512e, 2.5" Hot-Plug 3x originální BOSS (Boot Optimized Server Storage) PCIe karta FH s integrovaným řadičem RAID1, každá karta s 2x M.2 240 GB SATA SSD. BOSS	DELL_R640.pdf DELL_R740.pdf

Komodita K.6 – Nástroje pro zajišťování úrovně dostupnosti informací				
			podporuje bootování hypervizoru.	
	Záruka	Nabízené komponenty převezmou záruku serverů a budou součástí konfigurace vedené v systému podpory výrobce	Nabízené originální komponenty převezmou záruku serverů a budou součástí konfigurace vedené v systému podpory výrobce	https:///support. dell.com
Rozšíření NAS **Synology DX517 Seagate ST8000NT001**	Diskové police	Disková police pro rozšíření kapacity stávajících NAS (DS412+ nebo DS916+) určené pro ukládání záloh	Disková police Synology DX517 pro NAS DS916+, určená pro ukládání zálohy	https://www.synology.com/cs-cz/products/DX517#specs
	HDD	Celková disková kapacita min. 40 TB RAW / 32 TB RAID5 sestavená z HDD SATA (256 MB cache), výrobcem určené pro NAS nebo servery	5x HDD Seagate IRONWOLF Pro ST8000NT001, 8 TB, 256 MB cache, určeny výrobcem pro NAS. Celková kapacita 40 TB RAW / 32 TB RAID 5	Seagate.pdf
	Záruka	36 měsíců	36 měsíců	Součástí cenové nabídky
Licence SDS **3x VMware vSAN Standard / 1 CPU**	Provedení	Licence software vysoce dostupného virtualizovaného softwarově definovaného diskového úložiště pro stávají 3 virtualizační servery	3x trvalá licence VMware vSAN Standard / 1 CPU v aktuální verzi	vSAN.pdf
	Replikace	Software musí umožnit minimálně synchronní replikace dat (zrcadlení, RAID1) mezi uzly SDS (virtualizačními servery)	Software umožňuje synchronní replikaci dat (zrcadlení, RAID1) mezi všemi uzly SDS / virtualizačními servery	vSAN.pdf
	Vysoká dostupnost	Automatické překlenutí výpadku jednoho prvků systému – jednoho serveru či jeho komponenty (např. jednoho disku). Včetně podpory zotavení a obnovení	Software umožňuje automaticky překlenout výpadek jednoho prvku systému – jednoho serveru či jeho komponenty (např. jednoho disku). Software obsahuje podporu zotavení a obnovení po obnově provozu prvku.	vSAN.pdf
	Podpora virtualizace	Software bude provozován na úrovni hypervizorů (bude do nich zaintegrován) nabízené serverové virtualizace	Software je integrální součástí hypervizoru VMware ESXi, aktivuje se nabízenou licencí	vSAN.pdf
	Jednotná správa	Správa SDS bude zaintegrována do nástroje pro správu serverové virtualizace pro jednotnou správu	Správa vSAN bude integrální součástí nástroje správy serververové virtualizace vCenter a bude tak zajištěna jednotná správa	vSAN.pdf
	Vyrovnávací paměť	Integrovaná podpora vyrovnávací paměti pro čtení i zápis s využitím flash médií (SSD, NVMe disků apod.)	vSAN obsahuje integrovanou podporu vyrovnávací paměti (cache) pro čtení i zápis, která využívá využívá flash média - SSD a NVMe disky	vSAN.pdf
	Konzistence dat	Integrovaná kontrola dat kontrolními součty (checksum)	vSAN obsahuje integrovaná kontrola dat kontrolními součty (checksum) pro zajištění konzistence dat.	vSAN.pdf
	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).	vSAN lze škálovat scale-in i scale-out. Je možné za provozu přidávat další uzly SDS v RAID režimu a rozprostřít mezi ně data. Nabízená licence není kapacitně omezena a umožňuje navyšovat kapacitu licencovaných uzlů přidáním disků.	vSAN.pdf
	Škálovatelnost funkcí	Změnou typu licence lze aktivovat (bez potřeby instalace) pokročilé funkce – min. deduplikace, šifrování uložených dat apod.	vSAN umožňuje aktivovat pokročilé funkce včetně deduplikace a šifrování	vSAN.pdf

Komodita K.6 – Nástroje pro zajišťování úrovně dostupnosti informací				
			uložených dat změnou licence bez nutnosti instalace funkcí.	
	Serverová virtualizace – integrace	Integrovaná podpora technologií stávající serverové virtualizace – replikace virtuálních strojů, podpora virtuálních distribuovaných přepínačů, správa politik úložišť	vSAN nativně podporuje stávající serverovou virtualizaci VMware vSphere ESX včetně pokročilých technologií replikace virtuálních strojů, virtuální distribuované přepínače, správa politik úložišť.	vSAN.pdf
	Řízení výkonu	Integrovaná podpora limitace IOPS (vstupně/výstupních operací za sekundu) virtuálních serverů	vSAN obsahuje integrovanou podporu omezení IOPS (vstupně/výstupních operací za sekundu) virtuálních serverů	vSAN.pdf
	iSCSI	Integrovaná podpora publikace kapacity SDS prostřednictvím protokolu iSCSI (tzv. ISCI target)	vSAN obsahuje integrovanou podporu publikace kapacity SDS prostřednictvím protokolu iSCSI - tzv. ISCI target	vSAN.pdf
	Záruka	Podpora výrobce, včetně nároku na nové verze po dobu min 60 měsíců	Podpora výrobce, včetně nároku na nové verze po dobu min 60 měsíců	Součástí cenová nabídky
Bezpečné úložiště **DELL PowerEdge T350 s Veeam Hardened Repository SW**	Provedení	umístitelné do racku, včetně montážního materiálu	Server optimalizovaný pro umístění do racku se specifikacemi EIA-310	DELL_T350.pdf
	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	1x CPU 6 jader, Intel Xeon E-2356G SPECrate®2017_int_base 53.6 bodů SPECrate®2017_fp_base 49.3 bodů	http://spec.org/
	RAM	32 GB, min. 3200 MT/s	32 GB RAM, 3200 MT/s	DELL_T350.pdf
	Úložiště firmware	Min. 2x SSD 240 GB, read intensive, samostatný HW řadič RAID1	BOSS-S2 controller card + with 2x M.2 Sticks 240G, RAID1	DELL_T350.pdf
	Úložiště data	Min. 7x 8 TB, NLSAS 12Gb, 7 200 ot/min	7x 8TB Hard Drive SAS ISE 12Gbps 7.2K 512e 3.5in Hot-Plug (SAS je výkonnější/lepší řešení než NLSAS)	DELL_T350.pdf
	Rozšiřitelnost	Min. 1 volná pozice HDD pro rozšíření kapacity, aktivní, připojená k RAID/PCIe	1 volná pozice (z celkem 8) pro rozšíření kapacity, aktivní, připojená k řadiči RAID	DELL_T350.pdf
	RAID hardware	SAS 12Gb, RAID 1,5,6, zálohovaná zapisovací cache min. 8 GB	PERC H755 RAID Controller, 8GB NV R/W Cache, SAS, 12 Gb, RAID 0,1,5,6	DELL_T350.pdf
	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	2x 1GbE RJ-45, čip BCM5720 s podporou virtualizace VMware NetQueue and Microsoft VMQ. 10Gb porty nejsou osazeny, protože nejsou požadovány. Při osazení (rozšíření konfigurace) podporují NPAR. 1x 1Gb RJ-45 – samostatný port pro vzdálený management – součást iDRAC	DELL_T350.pdf
	USB	min. 2 USB konektory – min. 1x verze 3.0, min. min .1x na čelním panelu s podporou bootování	7x USB port – 1x USB 3.0 na předním panelu s podporou bootování, 1x USB 3.0 a 5x USB 2.0 na zadním panelu	DELL_T350.pdf
	Management	Servisní modul s možnosti samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a	Integrovaný servisní modul iDRAC 15G Enterprise, možnost samostatného	DELL_T350.pdf

Komodita K.6 – Nástroje pro zajišťování úrovně dostupnosti informací				
		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)	přístupu po management síti (vyhrazený port), 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	2x napájecí zdroj 600W v redundantní konfiguraci, specifikace Platinum	DELL_T350.pdf
	Souborový systém	XFS	Veeam Hardened Repository (VHR) bude instalováno se souborovým systémem XFS	Veeam_Hardened_repository.pdf
	Protokoly	SMB/CIFS, SNMP, http/s a ssh (management)	Systém podporuje protokol CIFS/SMB pro ukládání dat (VHR), SNMP pro monitorování (iDRAC) a http/s a ssh pro management (VHR a iDRAC)	DELL_T350.pdf Veeam_Hardened_repository.pdf
	Výkon	zápis min. 3 TB / hod	Systém podporuje zápis rychlostí více než 3000 GB/hod, tj. 3 TB/hod. Může být prokázáno měřením při implementaci.	DELL_T350.pdf Veeam_Hardened_repository.pdf
	Ochrana dat	min RAID5, automatická relokací vadných datových bloků	Ochrana dat je zajištěna hardwarovým RAID serveru, který podporuje automatickou relokaci vadných datových bloků disků	DELL_T350.pdf
	Retence dat	programově nastavitelné retenční lhůty na uložený objekt (např. soubor), po dobu retence nelze objekt modifikovat	VHR umožňuje programově nastavit retenční lhůty na uložený objekt - typicky soubor zálohy, po dobu retence nelze objekt modifikovat	Veeam_Hardened_repository.pdf
	Redundance	redundantní rotační díly a napájecí zdroje	Server obsahuje redundantní rotační díly (disky) a napájecí zdroje	DELL_T350.pdf
	Ochrana proti přepisu dat	režim WORM (Write Once – Read many times Memory)	VHR podporuje režim WORM	Veeam_Hardened_repository.pdf
	Kompatibilita	Kompatibilita se stávajícím zálohovacím systémem, podpora ukládání záloh, řízení jejich historie a řízení retenčních lhůt	VHR je přímo podporován stávajícím zálohovacím systéme Veeam Backup & Recovery včetně ukládání záloh, řízení jejich historie a řízení retenčních lhůt. VHR je nativní součástí „ekosystému" Veeam Backup & Recovery	Veeam_Hardened_repository.pdf
	Audit	Integrovaný logovací systém – systémové událostí, provádění příkazy, přihlášení/odhlášení, datové operace	VHR společně s Veeam Backup & Recovery obsahuje Integrovaný logovací systém systémových událostí, provádění příkazů, přihlášení/odhlášení a datových operací	Veeam_Hardened_repository.pdf

Komodita K.6 – Nástroje pro zajišťování úrovně dostupnosti informací				
	Záruka	60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze software a firmware	60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze software a firmware	Součástí cenové nabídky
Dispečerské pracoviště 5x **5x HP t640 Thin Client** **15x monitor Dell P2422H** **5x Zvuková lišta Dell Slim Soundbar SB521A** **5x monitor Philips 172B9TN** **5x PC ASUS PN41**	**Terminál**			
	Provedení	Pasivní provedení bez rotačních dílů (HDD, ventilátor apod.), možnost umístění "nastojato" i "naležato"	Tenký klient HP T640 bez rotačních dílů s možností umístění svisle i vodorovně	HP_t640.pdf
	Rozměry	max. 25 x 25 x 6 cm	196 x 196 x 35 mm	HP_t640.pdf
	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	Čelní panel: 3x USB 3.1, z toho 1x USB-C, audio combo (sluchátka, mikrofon) Zadní panel: 4x USB, z toho 2x USB 3.1, audio combo (sluchátka, mikrofon) 3x Display Port 1.2 a 1x LAN RJ-45 1Gb s podporou WoL	HP_t640.pdf
	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	64 bitový CPU AMD Ryzen R1505G s výkonem 3925 bodů dle https://www.cpubenchmark.net, integrovaný HD grafický čip s podporou UHD/4K (3840 x 2160 @ 60 Hz) současně na všech Display Portech. RAM 8 GB	HP_t640.pdf
	Grafika	podpora vícemonitorového provozu, rozlišení min. 4K/UHD (3840 x 2160 @ 60Hz)	Vícemonitorový provoz - UHD/4K (3840 x 2160 @ 60 Hz) současně na všech Display Portech.	HP_t640.pdf
	Kompatibilita	Microsoft RDP; Remote FX; Citrix ICA, Citrix HDX, VMware PCoIP	Kompatibilní s Microsoft RDP; Remote FX; Citrix ICA, Citrix HDX, VMware PCoIP	HP_t640.pdf
	Bezpečnost	Plná podpora 802.1X	Plná podpora 802.1X	HP_t640.pdf
	Operační systém	Windows 10 IoT Enterprise 64-bit a vyšší	Operační systém Windows 10 IoT Enterprise 2019 64 bit	HP_t640.pdf
	VESA	Podpora standardu VESA pro montáž na monitor, zeď apod.	Montážní otvory standardu VESA 100 pro montáž na monitor, zeď a ostatní plochy	HP_t640.pdf
	Spotřeba	do 10 W	Spotřeba (Energy Consumption) do 9,62W	HP_t640.pdf
	Periferie	včetně klávesnice a myši	Klávesnice a myš součástí dodávky	HP_t640.pdf
	Záruka	36 měsíců včetně nároku na nové verze firmware	36 měsíců včetně nároku na nové verze firmware	Součástí cenové nabídky
	Monitor 3x			
	Provedení	24" (min. 23,8" viditelná plocha), tenký rámeček, matný – antireflexní povrch, design shodný s multimediálním monitorem	24" (min. 23,8" viditelná plocha), tenký rámeček, matný antireflexní povrch, design shodný multimediálním monitorem (vybavený zvukovou lištou)	P2422h Datasheet.pdf
	Panel	technologie IPS, podsvícení LED, odezva do 5 ms	Technologie panelu IPS s LED podsvícením, odezva 5 ms	P2422h Datasheet.pdf
	Rozlišení	FullHD, min. 1920 x 1080	Rozlišení FullHD 192x1080	P2422h Datasheet.pdf

Komodita K.6 – Nástroje pro zajišťování úrovně dostupnosti informací				
	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: 1x HDMI 1.4, Display Port 1.2, 1x VGA. Digitální porty s podporou HDCP 1.4. DP kabel součástí dodávky	P2422h Datasheet.pdf
	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	5x USB 3.2 (1x vstup, 4x výstup včetně kabelu k počítači, výstupní porty na snadno dostupné spodní hraně monitoru	P2422h Datasheet.pdf
	Ergonomie	Integrovaná technologie pro omezení vlivu modrého světla	Technologie ComfortView Plus omezující negativní vliv modrého světla a blikání obrazu	P2422h Datasheet.pdf
	Nastavení polohy	Výškově stavitelný, otočný kolem svislé osy, nastavitelný sklon, otočný na výšku (PIVOT)	Výškově stavitelný stojan, otočný kolem svislé osy, nastavitelný sklon, zobrazovač otočný na výšku (PIVOT)	P2422h Datasheet.pdf
	Záruka	min. 36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace	min. 36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace	Součástí cenové nabídky
	Zvuková lišta 1x			
	Provedení	Originální zvuková lišta k nabízeným 24" monitorům s magnetickým upevněním, bez omezení polohovacích možností monitoru	Originální zvuková lišta DELL k monitorům P2422H neomezující polohovací možnosti monitoru. Magnetické uchycení.	SB521 Guide.pdf
	Porty	USB pro napájení I zvuk	Jednotné USB připojení pro napájení i zvuk	SB521 Guide.pdf
	Výkon	min 3 W	Výkon 2x 1,8W, celkový 3,6 W	SB521 Guide.pdf
	Záruka	min 36 měsíců	36 měsíců	Součástí cenové nabídky
	Monitor dotykový 1x			
	Provedení	17" LCD dotykový monitor, ovládání prstem i předmětem	17“ LCD dotykový monitor s možností ovládání prstem i předmětem (stylusem)	Philips 172B9TN Datasheet.pdf
	Dotyková vrstva	kapacitní nebo resistivní (min. 5 vodičová) nebo jiná srovnatelná technologie umožňující dotykové ovládání displeje	Kapacitní technologie dotykového ovládání	Philips 172B9TN Datasheet.pdf
	Rozlišení	min. 1280 x 1024	Rozlišení 1280 x 1024	Philips 172B9TN Datasheet.pdf
	Odezva	max. 5 ms	Typická odezva 1 ms	Philips 172B9TN Datasheet.pdf
	Porty – video	min. 1x Display Port 1.2, 1x HDMI 1.4, včetně Display Port kabelu pro připojení k počítači	Porty: VGA (Analog), DVI-D (digital, HDCP), DisplayPort 1.2, HDMI 1.4. DP kabel součástí dodávky	Philips 172B9TN Datasheet.pdf
	Porty – data	USB pro připojení dotykové vrstvy	USB port pro připojení dotykové vrstvy	Philips 172B9TN Datasheet.pdf
	Ergonomie	široký pozorovací úhel, min 150 stupňů vertikálně i horizontálně	Pozorovací úhly 170º horizontálně a 160º vertikálně	Philips 172B9TN Datasheet.pdf
	Audio	2 integrované reproduktoru, audio jack	2 integrované reproduktory (stereo), audio konektor (jack)	Philips 172B9TN Datasheet.pdf
	Kompatibilita	ovladače nebo integrovaná podpora Windows 7/8,10/11, Linux, Mac	Kompatibilita s Windows 7-11, Linux Android, Mac (otestování Dodavatelem)	Philips 172B9TN Datasheet.pdf
	Záruka	min. 36 měsíců poskytovaná výrobcem	36 měsíců poskytovaná výrobcem	Součástí cenové nabídky
	Řídící PC dotykového monitoru			

Komodita K.6 – Nástroje pro zajišťování úrovně dostupnosti informací				
	Provedení	Pasivní provedení bez rotačních dílů (HDD, ventilátor apod.)	ASUS PN41, mini PC v pasivním provedení bez rotačních dílů	ASUS PN41.pdf
	Rozměry	max. 20 x 20 x 6 cm	115 x 115 x 49 mm	ASUS PN41 spec.pdf
	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	Čelní panel: 1 x USB 3.1 Type-C, 1 x USB 3.1, 1 x Audio Jack Zadní panel: 1 x USB 3.2 Type-C, 1 x HDMI, 2 x USB 3.2, 1 x 2.5G (RJ45) LAN	ASUS PN41 spec.pdf
	Bezdrátová konektivita	Wi-Fi min 802.11an, Bluetooth 5	WiFi 802. 11ac (zahrnuje starší standard 802.11an), Bluetooth 5	ASUS PN41 spec.pdf
	CPU	64 bit CPU, výkon min. 3000 bodů dle https://www.cpubenchmark.net	64 bitový CPU Intel N5100, výkon 3401 bodů dle https://www.cpubenchmark.net	ASUS PN41 spec.pdf
	Grafika	podpora vícemonitorového provozu, rozlišení min. 4K/UHD (3840x2160/60Hz)	podpora vícemonitorového provozu, rozlišení 4K/UHD (3840x2160/60Hz)	ASUS PN41 spec.pdf
	Paměť	min. 4 GB	4 GB	ASUS PN41 spec.pdf
	Úložiště	min. 128 GB NVMe SSD	128 GB NVMe SSD	ASUS PN41 spec.pdf
	Bezpečnost	Plná podpora 802.1X	Plná podpora 802.1X (zajišťuje operační systém Windows)	ASUS PN41 spec.pdf
	Operační systém	Windows 10Pro a vyšší	Windows 10 Pro s bezplatným upgradem na verzi 11	ASUS PN41 spec.pdf
	Spotřeba	do 15 W	Spotřeba do 10W při běžném provozu, TDP CPU 6 W	ASUS PN41 spec.pdf
	Periferie	včetně klávesnice a myši	Klávesnice a myš součástí dodávky	ASUS PN41 spec.pdf
	Záruka	36 měsíců včetně nároku na nové verze firmware	36 měsíců včetně nároku na nové verze firmware	Součástí cenové nabídky
Operátorské pracoviště výjezdového stanoviště 13x **13x monitor DELL S2722DZ** **13x PC DELL OptiPlex 5000**	**Monitor multimediální, videokonferenční**			
	Provedení	27", tenký rámeček, matný – antireflexní povrch	27“ multimediální monitor s tenkým rámečkem a matným (antireflexním) povrchem displeje.	S2722DZ Datasheet.pdf
	Panel	technologie IPS, podsvícení LED, odezva do 5 ms	Technologie IPS s LED podsvícením, odezva obrazu 4 ms	S2722DZ Datasheet.pdf
	Rozlišení	QHD, min. 2 560 × 1 440	QHD, 2560 x 1440, 75Hz	S2722DZ Datasheet.pdf
	Porty – video	min. 1x Display Port 1.2, 1x HDMI 1.4, včetně Display Port kabelu pro připojení k počítači	Porty 1 x HDMI 1.4, 1 x DP 1.2, DP kabel součástí dodávky	S2722DZ Datasheet.pdf
	Porty – audio	Audio výstup jack	1x audio výstup (jack)	S2722DZ Datasheet.pdf
	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	Port IN: 1x USB-C s přenosem obrazu (DP 1.2) a zvuku, napájením PD 65 W i při vypnutém monitoru Porty OUT: 2x USB 3.2 snadno dostupné na boku monitoru	S2722DZ Datasheet.pdf
	Reproduktory	min. 2 integrované reproduktory, výkon min. 2x 5 W	2x integrovaný reproduktor, každý s výkonem 5W	S2722DZ Datasheet.pdf

Komodita K.6 – Nástroje pro zajišťování úrovně dostupnosti informací				
	Mikrofony	min. 2 integrované mikrofony, tlumení ruchů, MUTE tlačítko	2x integrovaný mikrofon s potlačením echa a ruchů, MUTE tlačítko pro ztlumení mikrofonu na spodním okraji monitoru	S2722DZ Datasheet.pdf
	Kamera	Integrovaná kamera min. 2Mpix, podpora Microsoft Hello, fyzické zakrytí pro bezpečnost (krytka, zasunutí apod.)	Integrovaná kamera s rozlišení 2560 x 1920 (5 Mpix), podpora a certifikace pro Windows Hello, fyzické zakrytí kamery jednoduchým zasunutím do těla monitoru.	S2722DZ Datasheet.pdf
	Ergonomie	Integrovaná technologie pro omezení vlivu modrého světla	Technologie ComfortView Plus pro omezení vlivu modrého světla a blikání obrazu	S2722DZ Datasheet.pdf
	Nastavení polohy	Výškově stavitelný, otočný kolem svislé osy, nastavitelný sklon, otočný na výšku (PIVOT)	Výškově stavitelný stojan, otočný kolem svislé osy, displej otočný na výšku (PIVOT)	S2722DZ Datasheet.pdf
	Záruka	min. 36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace	36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace	Součástí cenové nabídky
	Stolní počítač			
	Provedení	Stolní provedení, možnost umístění nastojato i naležato	DELL Optiplex 5000 small form factor ve stolním provedení s možností svislého i vodorovného umístění.	OptiPlex 5000 Datasheet.pdf
	Rozměry	formát SFF nebo menší	Formát small form factor	OptiPlex 5000 Datasheet.pdf
	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	Čelní panel: 2x USB 3.2 (z toho jeden Type-C), 2x USB 2.0, audio (mikrofon, sluchátka), slot pro SD kartu, DVD mechanika Zadní panel: 4x USB 3.2, 2x USB 2.0, DisplayPort 1.4, HDMI 2.0, LAN RJ-45 1 Gb s podporou WoL	OptiPlex 5000 Datasheet.pdf
	Bezdrátová konektivita	Wi-Fi min 801.11ac, Bluetooth 5	WiFi 6 802.11ax (zahrnuje i 802.11ac), Bluetooth 5.2	OptiPlex 5000 Datasheet.pdf
	CPU	64 bit CPU, výkon min. 19 500 bodů dle https://www.cpubenchmark.net	64 bit CPU Intel Core i5-12500, výkon 19 983 dle https://www.cpubenchmark.net	OptiPlex 5000 Datasheet.pdf
	Grafika	podpora vícemonitorového provozu, rozlišení min. 4K/UHD (3840x2160/60Hz)	Intel UHD Graphics 770 s podporou třímonitorového provozu a rozlišením až 5120x3200 @ 60 Hz	OptiPlex 5000 Datasheet.pdf
	Paměť	min. 16 GB	16 GB	OptiPlex 5000 Datasheet.pdf
	Úložiště	min. 512 GB NVMe SSD	512 GB NVMe SSD	OptiPlex 5000 Datasheet.pdf
	DVD, SD	integrovaná optická mechanika DVD, čtečka SD karet	Integrovaná optická mechanika 8x DVD+/-RW a čtečka SD karet na čelním panelu	OptiPlex 5000 Datasheet.pdf
	Bezpečnost	Plná podpora 802.1X	Plná podpora 802.1X zajištěná operačním systémem	OptiPlex 5000 Datasheet.pdf

Komodita K.6 – Nástroje pro zajišťování úrovně dostupnosti informací				
	Operační systém	Windows 10 Pro a vyšší	Windows 10 Pro s možností bezplatného upgrade na Windows 11 Pro	OptiPlex 5000 Datasheet.pdf
	Periferie	včetně klávesnice a myši	Klávesnice a myš součástí dodávky	OptiPlex 5000 Datasheet.pdf
	Záruka	min. 36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace	36 měsíců poskytovaná výrobcem, oprava následující pracovní den v místě instalace	Součástí cenové nabídky
Řídící software operačního střediska **Vlastní (zakázkový) vývoj**	Základní funkce	Software pro automatizace krizového scénáře typu "červené tlačítko" – převodu provozu aplikací operačního střediska do záložního operačního střediska (fail-over)	zakázkový software pro automatizaci krizového scénáře typu "červené tlačítko". Spuštění scénáře na vyžádání zajistí převod provozu aplikací operačního střediska do záložního operačního střediska (fail-over)	Vlastní vývoj pro tuto zakázku
	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	Software zajistí automatickou rekonfiguraci síťových služeb včetně směrování, adresních prostorů a jmenných služeb, blokaci internetu v případě útoku, rekonfigurace datových zdrojů (SQL, Oracle), aktivaci souvisejících virtuálních serverů a souvisejících operací	Vlastní vývoj pro tuto zakázku
	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)	Proces spuštění scénáře bude možno aktivovat z libovolné pracovní stanice po ověření oprávnění uživatele k požadované operaci. Součástí řešení bude i zpětný převod provozu do primárního operačního střediska (fail-back)	Vlastní vývoj pro tuto zakázku
	Provedení	Provoz v prostředí stávající virtualizační platformy Vmware	Software bude provozován v prostředí stávající virtualizační platformy VMware	Součástí cenové nabídky

(9) Požadavky na vozidlové komunikační jednotky

Komodita K.7 – Vozidlové komunikační jednotky				
Část	**Parametr**	**Popis povinného parametru**	**Dodavatel popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Dodavatel uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Komunikační jednotka 40x **40x**	Provedení	odolný tablet pro umístění do vozidla	Tablet v odolné provedení určený pro náročné provozní podmínky s možností umístění do vozidla a provozu ve vozidle	TOUGHBOOK_G2.pdf
	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),	Úhlopříčka displeje 10.1“, rozlišení 1920x1200, antrireflexní provedení s vysokým jasem až 1000 cd/m2	TOUGHBOOK_G2.pdf

Komodita K.7 – Vozidlové komunikační jednotky				
Odolný tablet Panasonic Toughbook G2			s čitelností na slunci. Podpora ovládání v rukavicích	
	CPU	výkon CPU dle https://www.cpubenchmark.net min. 6200 bodů, nízká spotřeba, TDP do 35W	CPU Intel Core i5-10310U s výkonem 6520 bodů dle https://www.cpubenchmark.net, TDP 25W	TOUGHBOOK_G2.pdf
	Video	výkon video/grafického procesoru dle https://www.videocardbenchmark.net min. 850 bodů	Grafický procesor Intel UHD Graphics s výkonem 1482 bodů dle https://www.videocardbenchmark.net	TOUGHBOOK_G2.pdf
	RAM	min. 16 GB	16 GB	TOUGHBOOK_G2.pdf
	úložiště	min. 512 GB NVMe SSD	512 GB NVMe SSD	TOUGHBOOK_G2.pdf
	Bezdrátové připojení	WiFi 6, 802.11ax, 2.4 + 5 GHz Bluetooth min. 5.0 WWAN (LTE,3G)	Intel WiFi 6 AX201, 802.11ax Bluetooth 5.1 WWAN 4G EM7455 with eSIM support modem (LTE, 3G)	TOUGHBOOK_G2.pdf
	Porty	min 1x USB 3 min 1x USB 3 Type-C s podporou Power Delivery	1x USB 3.1 1x USB 3.1 Type-C s podporou Power Delivery	TOUGHBOOK_G2.pdf
	Kamery	čelní min. 2 Mpix s bezpečnostní krytkou zadní min. 8 Mpix	Čelní 2 Mpix s bezpečnostní krytkou a podporu Windows Hello Zadní 8 Mpix	TOUGHBOOK_G2.pdf
	Bezpečnost	integrovaný čip TPM 2.0 integrovaná kontaktní nebo bezkontaktní čtečka čipových karet (SmartCard)	Integrovaný bezpečnostní čip TPM 2.0 Integrovaná kontaktní čtečka čípových karet - Smart Card Reader	TOUGHBOOK_G2.pdf
	Reproduktory	integrovaný reproduktor nebo audio in/out	Integrovaný stereo reproduktor (2ks) a audio konektor pro headset (sluchátka, mikrofon)	TOUGHBOOK_G2.pdf
	Senzory	GPS	Vestavěná GPS U-Blox NEO-M8N	TOUGHBOOK_G2.pdf
	Napájení	interní baterie, náhradní baterie, napájecí adaptér	Interní a 1 ks náhradní baterie, napájecí adaptér	TOUGHBOOK_G2.pdf
	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.	Součástí dodávky bude zabezpečený (hardened) operační systém s podporou Windows aplikací, potlačeným uživatelským prostředím (uživatel má k dispozici pouze definovanou aplikaci) a autentizací pomocí SmardCard, včetně reinstalačního image.	TOUGHBOOK_G2.pdf
	Hmotnost	do 2000 g bez příslušenství	Méně než 1200g bez příslušenství	TOUGHBOOK_G2.pdf
	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	Ochrana proti vniknutí IP65 (prach, voda) Pracovní teplota -29 až +63 °C Odolnost proti pádu 180 cm	TOUGHBOOK_G2.pdf
	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)	60 měsíců poskytovaná výrobcem s podporou a hlášením závad v režimu 24x7 v českém jazyce a opravou	Součástí cenové nabídky

Komodita K.7 – Vozidlové komunikační jednotky				
			následující pracovní den u zákazníka (on-site)	
Sada příslušenství **40x Klávesnice FZ-VEKG21L6** **5x popruh FZ-VSTG21U** **40x Pero** **35x Dokovací stanice PCPE-HAV2007** **5x Dokovací stanice PCPE-HAVG103**	Přídavná klávesnice 40x	Odnímatelná klávesnice s touchpadem a držákem/stojánkem tabletu, krytí IP-65	Klávesnice FZ-VEKG21L6, odnímatelná, s touchpadem a držákem tabletu, krytí IP65	TOUGHBOOK_G2_prislusenstvi.pdf
	Popruh 5x	Otočný popruh pro bezpečné upevnění tabletu na paži a možností práce na výšku i na šířku	Popruh FZ-VSTG21U Otočný popruh pro bezpečné upevnění tabletu na paži a možností práce na výšku i na šířku	TOUGHBOOK_G2_prislusenstvi.pdf
	Pero 40x	Pero určené pro dotykový displej tabletu, pro ovládání aplikací a podepisování	Pero (digitizer) určené pro dotykový displej tabletu, pro ovládání aplikací a podepisování je součástí tabletu	TOUGHBOOK_G2.pdf
	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.	Automobilová dokovací stanice PCPE-HAV2007 pro pevné a bezpečné uchycení tabletu včetně příslušenství. Napájení tabletu. Snadné vkládání a vyjímání tabletu. Umožní pevné přichycení klávesnice.	TOUGHBOOK_G2_prislusenstvi.pdf
	Dokovací stanice bez klávesnice 5x	Automobilová dokovací stanice pro pevné a bezpečné uchycení tabletu včetně příslušenství. Napájení tabletu. Snadné vkládání a vyjímání tabletu.	Automobilová dokovací stanice PCPE-HAVG103 pro pevné a bezpečné uchycení tabletu včetně příslušenství. Napájení tabletu. Snadné vkládání a vyjímání tabletu.	TOUGHBOOK_G2_prislusenstvi.pdf
	Záruka	Min. 24 měsíců	24 měsíců	Součástí cenové nabídky

(10) Požadavky na správu identifikačních prostředků

Komodita K.8 – Správa identifikačních prostředků				
Správa identifikačních prostředků **MONET ProID Kartové centrum** **MONET ProID Card Management System (CMS)** **MONET ProID QSeal**	Obecné požadavky	Systém pro evidenci a správu životního cyklu identifikačních prostředků	Softwarový systém pro evidenci a správu životního cyklu identifikačních prostředků sestavený s komponent ProID Kartové centrum, Card Management Systém a QSeal	ProID+KartoveCentrum.pdf ProID+CMS.pdf ProID+QSeal.pdf
	Prostředky	Podpora kontaktních, bezkontaktních i hybridních identifikačních prostředků	Systém podporuje kontaktní, bezkontaktní i hybridní identifikační prostředky	ProID+KartoveCentrum.pdf ProID+CMS.pdf
	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)	Systém umožňuje evidovat: - typ prostředku - druh prostředku - stav prostředku - historii prostředku - držitele prostředku - data uložená na prostředku v požadované míře detailu a další údaje	ProID+KartoveCentrum.pdf ProID+CMS.pdf

	Integrace	Napojení na Active Directory (zdroj dat o uživatelích, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty)	Systém umožňuje napojení na Active Directory a interní (doménovou) certifikační autoritu a bude s těmito systémy propojen pro získávání dat, autentizaci a autorizaci a práci s certifikáty	ProID+KartoveCentrum.pdf ProID+CMS.pdf
	Uživatelské rozhraní	Webové rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory	Systém obsahuje webové rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory	ProID+KartoveCentrum.pdf ProID+CMS.pdf
	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	Systém umožňuje spravovat doménové i kvalifikované certifikáty ve webovém prostředí a podporuje úkony: - 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	ProID+KartoveCentrum.pdf ProID+CMS.pdf
	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).	Systém umožňuje použití jakékoli veřejné certifikační autority od kvalifikovaných poskytovatelů certifikačních služeb, umožní-li takový poskytoval přístup ke svému systému prostřednictvím API (aplikačního rozraní) nebo obdobným způsobem.	ProID+KartoveCentrum.pdf ProID+CMS.pdf
	Operace	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů	Systém podporuje operace recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů	ProID+KartoveCentrum.pdf ProID+CMS.pdf
	Potisk	Integrované prostředí pro generování podkladů pro potisk identifikačních karet externím Dodavatelem i na vlastní tiskárně	Systém obsahuje prostředí pro generování podkladů pro potisk identifikačních karet externím poskytovatelem tiskových služeb i na vlastní tiskárně	ProID+KartoveCentrum.pdf ProID+CMS.pdf
	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.	Systém obsahuje integrované aktivní (funkční a přístupné) aplikační rozhraní (API) pro bezpečné (autorizované) poskytování veřejných informací o uložených prostředcích, certifikátech a kvalifikovaných elektronických pečetí pro systémy třetích stran včetně dokumentace.	ProID+KartoveCentrum.pdf ProID+CMS.pdf

	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.	Systém poskytuje elektronické pečetě pomocí čipové karty s kvalifikovaným certifikátem prostřednictvím otevřené webové služby – aplikačního rozhraní. Řízení oprávnění uživatelů požadujících pečetění probíhá vůči Active Directory. Součástí dodávky není provedení integrace s napojenými systémy využívajících kvalifikované pečeti.	ProID+QSeal.pdf
	Licence	pro 350 uživatelů (včetně externích)	pro 350 uživatelů (včetně externích)	Součástí cenové nabídky
	Záruka	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze	60 měsíců včetně podpory výrobce a nároku na nové a opravné verze	Součástí cenové nabídky

2.11. Parametry architektury technického řešení

(1) Architektura komodit bude 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.

2.12. Parametry rozhraní

(1) Veškeré nabízené aktivní síťové prvky disponují rozhraním SNMP v2 nebo vyšší pro management a vzdálenou správu.

2.13. Kompatibilitu s ostatními systémy

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

2.14. Typy klientů

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

2.15. Bezpečnost informací

(1) Veškeré nástroje pro správu musí umožňují správu interních účtů (min. jméno a heslo) a většina nástrojů podporuje i napojení na LDAP/Active Directory.

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

(3) Veškeré nástroje pro správu budou komunikovat se zařízeními šifrovanými protokoly (SSH apod.). I v případě vestavěných nástrojů (např. www rozhraní hardware) bude 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. Dodavatel využije stávající certifikát ZZS KVK.

2.16. Technologické vazby

(1) Dodavatelem implementovaná řešení vyžadují vazby na dále vyjmenované systémy Objednatele

(a) Síťová infrastruktura LAN, VPN včetně firewallů a přípojek WAN a internet.

(b) Serverový hardware včetně podpůrných non-IT technologií (datové rozvaděče, záložní napájení apod.

(c) Adresářová služba Active Directory a navázané systémy Microsft (Exchange, SQL apod.) i třetích stran

(d) Objednatelem provozované aplikace, které budou integrovány s IDM, kartovým systémem, logmanagementem, popř. dalšími systémy

(e) Koncová zařízení uživatelů, včetně pracovníků operačního střediska

(2) Pro úspěšnou realizaci zakázky bude Dodavatel vyžadovat součinnosti nezbytnou pro využití vyjmenovaných vazeb. Součinnosti mohou být technického charakteru (poskytnutí přístupů, dokumentací apod.) i netechnického (organizačního) charakteru (zajištění a podpora jednání s třetími stranami (dodavateli aplikací a služeb), komunikace s uživateli apod.).

3. Implementační služby

3.1. Obecné parametry

(1) Dodavatel provede minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel zahrnul 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 provedeny 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 jsou zahrnuty v nabídkové ceně k položce, ke které se vztahují.

(3) Dodavatel zahrnul do nabídky i další související služby v dále uvedeném rozsahu:

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 Objednatele 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 Objednatelem 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 Dodavateli 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) Veškerá dokumentace bude zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office) používaných Objednatelem.

3.2. Zpracování prováděcí dokumentace

(1) Dodavatel 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 Dodavatele provede předimplementační analýzu, která bude zohledňovat stávající prostředí Objednatele ve vztahu ke konkrétnímu nabízenému plnění Dodavatele, zejména pak s ohledem na Dodavatelem 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 Objednatele.

(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 Objednatele (provoz a správu systému zajišťuje externí partner) min. v rozsahu doporučení parametrů pro sledování.

(k) Požadované součinnosti Objednatele.

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

(3) Prováděcí dokumentace zohlední podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného Dodavatelem 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) Dodavatel zapracuje do svého řešení tzn. i do prováděcí dokumentace relevantní opatření, která vzejdou ze vstupní externí penetrační testů, provedených třetí stranou.

(5) Prováděcí dokumentace bude ve lhůtě do 10 pracovních dní od předání Dodavatelem připomínkována Objednatelem a připomínky budou ze strany Dodavatele 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 Dodavateli jejich řádné zpracování.

(6) **Prováděcí dokumentace bude před zahájením realizace dalších etap plnění výslovně schválena Objednatelem**.

(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.

3.3. Harmonogram realizace

(1) Dodavatel 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) Dodavatel akceptuje 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 Objednateli, připomínkové řízení	D+60
E1.3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Objednatelem	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) Dodavatelem požadované součinnosti pro splnění harmonogramu

Nezbytnou podmínkou úspěšné implementace je kvalitní součinnost specialistů, ale i správců a klíčových uživatelů Objednatele. Dodavatel si je vědom velkého časového vytížení zaměstnanců Objednatele, proto omezí požadavky na součinnost na nezbytné minimum. Vzhledem k rozsahu projektu předpokládáme následující časové nároky na činnosti, u nichž je nezbytné součinnost (účast) pracovníků Objednatele:

(a) Projektové schůzky, úvodní workshop – 24 hod

(b) Připomínkování, schvalování dokumentace – 12 hod

(c) Asistence při instalaci a testování implementovaných systémů – 40 hod

(d) Akceptační testy – 24 hod

(e) Školení – 26 hodin

(f) Jednání s třetími stranami (dodavatelé aplikací, konektivity apod.) – 16 hod

(g) Zkušební provoz – 8 hodin

(h) Jiná součinnost (zajištění přístupů, poskytnutí dokumentací apod.) – 10 hod

3.4. Školení

(1) Dodavatel zajistí školení pracovníků Objednatele – 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 Objednatele 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 Objednatele.

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

(3) Náklady na školení jsou zahrnuty v nabídkové ceně k položce, ke které se vztahují.

(4) S ohledem na pandemii COVID-19 bude 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 Objednatelem nejpozději týden před realizací školení, a to podle aktuálního stavu pandemie a dle doporučení relevantních orgánů (Ministerstvo zdravotnictví ČR, Hygienická stanice atp.).

3.5. Provedení akceptačních testů a přechod do zkušebního (testovacího) provozu

(1) Dodavatel navrhne způsob a provedení akceptačních testů. Akceptační testy budou 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) V rámci zpracování cílového stavu (prováděcí dokumentace) navrhne Dodavatel pro každou komoditu 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 bude vyhotoven písemný akceptační protokol.

(3) Dodavatel 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. V případě předávání díla po částech (viz bod (4)) je Dodavatel 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) Dodavatel plánuje předávat dílo 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 Dodavatel v rámci zkušebního provozu vyřeší 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.

3.6. Požadavky na dokumentaci

(1) Dodavatel 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 Dodavatelům IT technologií do prostředí Objednatele 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) Dodavatel 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.

4. Záruky

(1) Dodavatel poskytuje 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) Dodavatel ve své nabídce uvádí ceny záruk 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 Objednatelem (tj. rozdíl mezi Standardními zárukami a podporami a požadavky Objednatele) Dodavatele uvádí 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 Objednatele. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

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

5. Požadavky na podporu provozu

5.1. Obecná pravidla provozu

(1) Pro hlášení servisních požadavků zajistí Dodavatel Objednateli 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 je součástí nabídky. Provozní doba helpdeskového systému je 8-17 hod. v pracovních dnech.

(2) Pravidla vzdáleného přístupu budou vítěznému Dodavateli předána při podpisu smlouvy.

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

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

5.2. Parametry podpory 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 Dodavatel 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 Objednateli účtovat.

(b) Řešení Incidentů může být zahájeno na základně požadavku Objednatele, na základě Objednatelem schváleného požadavku třetí strany nebo na základě schváleného podnětu Dodavatele.

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

(3) Pro případ, že bude Objednatel 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.

5.3. Způsob poskytování servisní podpory

(1) Servisní podpora bude poskytována zejména následujícím způsobem:

(a) Prostřednictvím pracovníka Dodavatele Vzdálenou správou

(b) Prostřednictvím pracovníka Dodavatele přímo na pracovišti Objednatele

(c) Prostřednictvím pracovníka Dodavatele formou vzdálené konzultace

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

(3) Objednatel je povinen zabezpečit Dodavateli podmínky pro řádné plnění, zejména

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

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

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

(d) umožnit Dodavateli 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) Dodavatel je v případě potřeby též z vlastní iniciativy oprávněn požádat Objednatele o dodatečné údaje o Incidentu a o nezbytnou součinnost Objednatele na řešení Incidentu, bez které nelze zahájit či pokračovat v řešení Incidentu.

(5) Objednatel je povinen

(a) elektronicky potvrdit Dodavateli 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.

5.4. Postup při řešení incidentů

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

(2) Součástí nahlášení požadavku Objednatelem 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) Dodavatelem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku.

(4) Dodavatel 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) Dodavatel neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Objednateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Objednatele a předpokládaný termín vyřešení požadavku.

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

(7) Zjistí-li Dodavatel 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 Objednatele.

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

(9) Objednatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok Dodavatele 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 Objednatele se Požadavek považuje za vyřešený.

(12) Po vyřešení požadavku Dodavatel požadavek uzavře v systému HelpDesk a informuje Objednatele.

(13) Objednatel 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.

5.5. Záruky na servisní služby

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

AUTOCONT a.s.

OBJASNĚNÍ A DOPLNĚNÍ NABÍDKY

Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS

Popis splnění požadavků na povinné parametry - **AUTOCONT a.s.**				
Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
Část	**Parametr**	**Popis povinného parametru**	**-**	**Popis upřesnění/doplnění**
	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		ACIdentitaUzivatelskaPrirucka.pdf – bod 2 – Práce s informačním systémem IDM
	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.		ACIdentitaUzivatelskaPrirucka.pdf – bod 2 – Práce s informačním systémem IDM
	Evidence aplikací a rolí	Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby.		ACIdentitaUzivatelskaPrirucka.pdf – bod 6.6 – Číselník aplikace, bod 10.1 - Konektory
	Logování	Systém bude poskytovat auditní logy ve formátu vhodném pro systém typu správy logů (Log management)		ACIdentitaUzivatelskaPrirucka.pdf – bod 16.1 - Logování
	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)		ACIdentitaUzivatelskaPrirucka.pdf – bod 16.1 – Logování, bod 2.7 - Historie
	Vysoká dostupnost	Systém musí být možno nasadit na více serverů v režimu vysoké dostupnosti.		ACIdentitaUzivatelskaPrirucka.pdf – bod 2 – Práce s informačním systémem IDM
	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.		ACIdentitaUzivatelskaPrirucka.pdf – bod 2.1 – Přihlášení do aplikace
	Podpora mobilních zařízení	Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno)		ACIdentitaUzivatelskaPrirucka.pdf – bod 2.1 – Přihlášení do aplikace
	Vyhledávání - diakritika	Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Parizek vyhledává i Pařízek apod.)		ACIdentitaUzivatelskaPrirucka.pdf – bod 2.6 – Vyhledávání a filtrování v aplikaci
	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.		ACIdentitaUzivatelskaPrirucka.pdf – bod 3.1.10 – Certifikáty, bod 10.1 Konektory

Popis splnění požadavků na povinné parametry - **AUTOCONT a.s.**				
Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
	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.		ACIdentitaUzivatelskaPrirucka.pdf – bod 6.6.6 – Správa licencí k aplikacím, bod 17.3 – Modul Workflow
	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.		ACIdentitaUzivatelskaPrirucka.pdf – bod 2 – Práce s informačním systémem IDM
	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.		ACIdentitaUzivatelskaPrirucka.pdf – bod 17.3 – Modul Workflow
	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.		ACIdentitaUzivatelskaPrirucka.pdf – bod 17.3 – Modul Workflow
	Kontextový výběr	Samoobslužné rozhraní umožní na úrovni organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.		ACIdentitaUzivatelskaPrirucka.pdf – bod 17.3 – Modul Workflow
	Reporty - porovnání	Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu.		ACIdentitaUzivatelskaPrirucka.pdf – bod 16.3.2 – Porovnání reportů
	Webové služby (WS)	IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.		ACIdentitaUzivatelskaPrirucka.pdf – bod 10.1.1 – Modul webových služeb
	Standardy WS	Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP.		ACIdentitaUzivatelskaPrirucka.pdf – bod 10.1.1 – Modul webových služeb
	Bezpečnost WS	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.		ACIdentitaUzivatelskaPrirucka.pdf – bod 10.1.1 – Modul webových služeb
	Logování WS	Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu		ACIdentitaUzivatelskaPrirucka.pdf – bod 10.1.1 – Modul webových služeb
	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		ACIdentitaUzivatelskaPrirucka.pdf – bod 10.1.1 – Modul webových služeb
	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		ACIdentitaUzivatelskaPrirucka.pdf – bod 10.1 - Konektory

Popis splnění požadavků na povinné parametry - **AUTOCONT a.s.**				
Komodita K.2 - Zavedení nástrojů pro správu a ověřování identit uživatelů a správců IS ZOS				
		- 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.		ACIdentitaUzivatelskaPrirucka.pdf – bod 10.1 - Konektory
	Bezpečná komunikace	Komunikace mezi jednotlivými komponenty řešení (klient, server, adresářová služba apod.) je šifrována (SSL či kompatibilní)		Přiložen Security_Standards_Brief.pdf

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

Popis splnění požadavků na povinné parametry - **AUTOCONT a.s.**				
Komodita K.3 - Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS				
Část	**Parametr**	**Popis povinného parametru**	**-**	**Popis upřesnění/doplnění**
A	Logování relací	Nepozměnitelné podklady pro audit a analytické reporty uživatelského chování		ACPimPamUzivatelskaPrirucka.pdf – bod 2.1 Aplikace PIMPAM
	Architektura	Samostatná virtuální aplliance, bezagentové řešení (bez nutnosti instalace agentů na monitorované systémy)		ACPimPamUzivatelskaPrirucka.pdf – bod 8.2 Architektura aplikace PIMPAM
	Autentizace	LDAP, Microsoft Active Directory, Radius, TACACS+, Kerberos, X.509, OTP, Web SSO, podpora vícefaktorové autentizace (MFA)		ACPimPamUzivatelskaPrirucka.pdf – bod 2.2 Autentizace do systému PIMPAM
	Autorizace	Integrované pokročilé workflow pro autorizaci (povolené časy a trvání relace, white/black listy, rozpoznání činnosti v RDP relaci, parametry relace apod.)		ACPimPamUzivatelskaPrirucka.pdf – bod 6.1 Autorizace
	Notifikace	Zasílání notifikací o zahájení definované relace		ACPimPamUzivatelskaPrirucka.pdf – bod 2.4.2 Upozornění/Notifikace
	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)		ACPimPamUzivatelskaPrirucka.pdf – bod 8.5 Konektory/Integrace
	Vysoká dostupnost	Integrovaná podpora high-availability clusterů: Active/Passive nebo Active/Active		ACPimPamUzivatelskaPrirucka.pdf – bod 8.2 Architektura aplikace PIMPAM
	Rozšiřitelnost	Podpora modulů (plug-in) pro integraci s dalšími technologiemi / technologickými partnery		ACPimPamUzivatelskaPrirucka.pdf – bod 8.5 Konektory/Integrace
	Rozhraní	Webové rozhraní pro přístup uživatelů I konfiguraci, bezpečná publikace do internetu (šifrovaná komunikace)		ACPimPamUzivatelskaPrirucka.pdf – bod 2.2 Autentizace do systému PIMPAM
	Zabezpečení přístupových údajů	Integrované bezpečné (šifrované) úložiště přístupových údajů k cílovým systémům		ACPimPamUzivatelskaPrirucka.pdf – bod 5.3 Spravované účty

Popis splnění požadavků na povinné parametry - **AUTOCONT a.s.**				
Komodita K.3 - Zavedení nástroje pro řízení přístupových oprávnění interních i externích správců IS ZOS				
	Aktivní bezpečnost	Upozornění a automatické ukončení podezřelé činnosti nebo neoprávněných pokusů o přístup		ACPimPamUzivatelskaPrirucka.pdf – bod 7.1 Aktuální relace
	SIEM	Podpora odesílání záznamů a událostí do systému SIEM (Security Information and Event Management)		ACPimPamUzivatelskaPrirucka.pdf – bod 8.3 Logování
	Logy	Nesmazatelnost logů po dobu minimálně 30 dní. Uložení auditních záznamů v zašifrované podobě s přístupem pouze oprávněných uživatelů		ACPimPamUzivatelskaPrirucka.pdf – bod 8.3 Logování
	Bezpečnostní standardy	Podpora zajištění shody se standardy HIPAA, GDPR, PCI, SOX		ACPimPamUzivatelskaPrirucka.pdf – bod 2.1 Aplikace PIMPAM
	Zálohování	Šifrování záloh, přístup k zálohovaným datům výhradně pomocí zabezpečených Disaster Recovery klíčů.		ACPimPamUzivatelskaPrirucka.pdf – bod 8.2 Architektura aplikace PIMPAM

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

Popis splnění požadavků na povinné parametry - **AUTOCONT a.s.**				
Komodita K.4 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
Část	**Parametr**	**Popis povinného parametru**	**-**	**Popis upřesnění/doplnění**
	Napájení	Systém musí mít redundantní napájení (min. 2 nezávislé zdroje)		Upřesněno v Logmanager_vyjadreni_vyrobce.pdf Logmanager_datasheet.pdf Logmanager-m dell poweredge-r6515-spec-sheet.pdf
	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.		Upřesněno v Logmanager_vyjadreni_vyrobce.pdf Logmanager_datasheet.pdf Logmanager-m dell poweredge-r6515-spec-sheet.pdf DELL-server-power-consumption-monitor-and-mgmt.pdf DELL-idrac9.pdf

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

Popis splnění požadavků na povinné parametry - **AUTOCONT a.s.**				
Komodita K.5 - Zavedení nástroje pro detekci kybernetických bezpečnostních událostí vůči IS ZOS				
Část	**Parametr**	**Popis povinného parametru**	**-**	**Popis upřesnění/doplnění**

	Výkon	min. 0,2 Gb/s trvalý síťový provoz, min. 200 Netflow/sec		Pro nabízený model Greycortex All-on-one XS upřesněno v GCX HW models 2023.pdf
	Kapacita	úložná kapacita SSD s ochranou min. RAID 1 pro min. 30 denní historii při plném výkonu		Pro nabízený model Greycortex All-on-one XS upřesněno v GCX HW models 2023.pdf
	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.		Pro nabízený model Greycortex All-on-one XS upřesněno v GCX HW models 2023.pdf a dále pro server DELL R350 s iDRAC Enterprise (HW platforma modelu XS) v Dell-R350.pdf DELL-server-power-consumption-monitor-and-mgmt.pdf DELL-idrac9.pdf

Komodita K.8 - Správa identifikačních prostředků

Popis splnění požadavků na povinné parametry - **AUTOCONT a.s.**				
Komodita K.8 - Správa identifikačních prostředků				
Část	**Parametr**	**Popis povinného parametru**	**-**	**Popis upřesnění/doplnění**
	Rozhraní	Integrované aktivní aplikační rozhraní (API) pro bezpečné (autorizované) poskytování veřejných informací o uložených prostředcích, certifikátec a kvalifikovaných elektronických pečetí pro systémy třetích stran včetně dokumentace.		Seznam služeb poskytovaných aplikačním rozhraním je uveden v příloze WDSL.zip. Pro využití rozhraní je nezbytná autentizace a autorizace přistupujícího uživatele či aplikace. Detaily ověření jsou z bezpečnostních důvodů dostupné pouze zákazníkům / uživatelů produktu na základě smlouvy.
	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.		Podropný popis je součástí přílohy ProID_QSeal_doc.pdf