Otázka č. 1:

V spoločnom slovníku obstarávania (CPV) verejný obstarávateľ neuvádza HW ako súčasť VO. Vie verejný obstarávateľ potvrdiť, že súčasťou dodania diela je aj dodanie HW? Žiadame verejného obstarávateľa aj o doplnenie spoločného slovníka VO.

Odpoveď č. 1:

Verejný obstarávateľ potvrdzuje, že súčasťou dodania diela je aj dodanie hardvéru tak, ako je to špecifikované v rámci zverejnených súťažných podkladov k tejto zákazke, konkrétne v bode 4.2 *„Stručný opis predmetu zákazky:“*, v ktorom je okrem iného uvedené, citujeme:

a) zhotoviť a dodať dielo (ďalej aj ako „informačný systém“) formou:
   - dodania hardvéru vrátane jeho naloženia, dopravy, zabezpečenia jeho dostatočnej ochrany pred poškodením alebo znehodnotením počas dopravy, vyloženia hardvéru v mieste plnenia, ktoré určí verejný obstarávateľ a vykonávania rozšírenej servisnej podpory výrobcom hardvéru počas záručnej doby v súlade so Zmluvou o dielo,
     (jedna z požiadaviek verejného obstarávateľa),

b) zabezpečiť služby podpory a údržby informačného systému vrátanie služieb pozáručnej licenčnej a technickej podpory softvéru 3. strán a rozšírenej pozáručnej servisnej podpory hardvéru (ďalej aj ako „služby“) v rozsahu obvyklých služieb/činností L3 podpory v súlade s odvetvovými štandardami ITIL po dobu 60 mesiacov od prevzatia poslednej časti diela (po riadnom odovzdaní a prevzatí diela ako celku vrátane odstránenia všetkých identifikovaných vád diela a akceptácie diela ako celku verejným obstarávateľom podpisom Záverečného akceptačného protokolu) formou:
   - poskytovania rozšírenej pozáručnej servisnej podpory hardvéru po dobu 36 mesiacov v rozsahu - zásah na mieste u používateľa do nasledujúceho pracovného dňa od nahlásenia poruchy počas bežnej pracovnej doby od 8.00 hod. do 17.00 hod., zariadenie príde opraviť na vopred určenú adresu servisný technik autorizovaného servisného strediska, zabezpečenie náhradných dielov v termínoch, ktoré sa viažu na nástup na servisný zásah, výmena vadných, nefunkčných dielov za funkčné diely, pričom nefunkčné pevné disky zostávajú vo vlastníctve verejného obstarávateľa.
     (jedna z požiadaviek verejného obstarávateľa),

v prílohách k zverejneným súťažným podkladom k tejto zákazke, konkrétne v:

- Prílohe č. 18 – Katalóg požiadaviek – KDS, stĺpec s označením *„OBLASŤ POŽIADAVKY - Hardvér“*,
- Prílohe č. 16 – SP_Štruktúrovaný rozpočet - KDS, časť 4 s názvom *„Zoznam a cena dodaných HW produktov a cena služby servisnej podpory dodaných HW produktov (záručná a pozáručná):“*,

a v návrhu Zmluvy o dielo a jej prílohách, konkrétne v:

- Zmluve o dielo, článok „PREAMBULA“, bod A, citujeme: *„... potrebuje zabezpečiť vytvorenie, dodanie a implementáciu aplikačného programového vybavenia a zabezpečiť dodanie súvisiacich hardvérových produktov v oblasti poskytovania kvalifikovaných dôveryhodných služieb.“*,
- Zmluve o dielo, článok „PREAMBULA“, bod D, citujeme: *„Účelom tejto Zmluvy o dielo je zabezpečenie vytvorenia aplikačného programového vybavenia, vrátane dodania hardvérových produktov, ktoré bude v plnom rozsahu zodpovedať všetkým funkčným, technickým a legislatívnym požiadavkám Objednávateľa uvedeným v tejto Zmluve o dielo a v súťažných podkladoch verejného obstarávania.“*,
- Zmluve o dielo, bod 1.3, citujeme: *„**Dielo**“ je ucelené informatické a softvérové riešenie vrátane hardvérových produktov, súvisiacej dokumentácie a súvisiacich aktivít, tvorené jednotlivými plneniami Zhotoviteľa podľa bodu 3.1 až bodu 4 tejto Zmluvy o dielo.“*,

- Prílohe č. 1 - Opis predmetu zákazky k Zmluve o dielo, odsek „Špecifikácia zákazky:“, citujeme: „Neoddeliteľnou súčasťou projektu je aj dodávka kompletnej prevádzkovej infraštruktúry (hardvér, softvér, licencie) pre SNCA.“,
- Prílohe č. 1 - Opis predmetu zákazky k Zmluve o dielo, odsek „Špecifikácia Predmetu zákazky:“, citujeme:
  „Predmetom zákazky je poskytnutie služieb, súvisiacich s vytvorením a dodaním hardvérového a softvérového diela s funkcionalitami pre:“,

  „Predmetom zákazky je poskytnutie služieb v nasledovnom rozsahu:

  2) *Dodania hardvéru a softvéru nevyhnutných pre prevádzku diela pre dve automatizované prostredia (testovacie a produkčné) v troch oddelených lokalitách, ktorý pozostáva z:*
     a) *Hardvéru pre prevádzkovanie diela, vrátane vybavenia pre realizáciu procesov SNCA t.j. notebooky, riešenie pre bezpečnú tlač, tlačiarne pre QSCD zariadenia podľa špecifikácie požiadaviek v Prílohe č. 18 „Katalóg požiadaviek - KDS“.“*

  „Verejný obstarávateľ požaduje celé hardvérové dielo dodať v súlade s funkčnými a nefunkčnými požiadavkami, v rozsahu, podľa podmienok a pri zachovaní požadovaných technických, bezpečnostných a iných vlastností diela, podľa Prílohy č. 18 „Katalóg požiadaviek - KDS“.“

Verejný obstarávateľ dopĺňa Spoločný slovník obstarávania (CPV) nasledovne:

- Servery 48820000-2
- Komunikačné zariadenia 32570000-9
- Riadiaca jednotka diskovej pamäte 30233190-9
- Pamäťové jednotky s magnetickým diskom 30233130-1
- Nadbytočné pole nezávislých diskov (RAID) 30233141-1

Otázka č. 2:

Ak je súčasťou VO aj dodanie HW, žiadame verejného obstarávateľa o doplnenie špecifikácie a požiadaviek na HW - sieťové zariadenia, spôsob zálohovania, veľkosť diskovej kapacity,...,

Odpoveď č. 2:

V rámci technologického návrhu infraštruktúry a technologických prostriedkov (výpočtových zdrojov, HW a SW), ktoré navrhne uchádzač za účelom naplnenia všetkých funkčných a nefunkčných požiadaviek, je požadované dodanie minimálne nasledovných výpočtových prostriedkov pre vytvorenie produkčného prostredia a testovacieho prostredia. Jedná sa o minimálne požiadavky, ktoré môžu byť uchádzačom rozšírené o nové ďalšie prvky vzhľadom na návrh a potreby uchádzača pre zabezpečenie iných prostredí (vývojové, predprodukčné, integračné, fix alebo iné) alebo pre zabezpečenie nevyhnutného výpočtového výkonu pre ním dodávané dielo za účelom naplnenia všetkých funkčných a nefunkčných požiadaviek verejného obstarávateľa.

Server

Parameter	**Minimálne požiadavky**
Server / Procesor (výkon)	Server s procesorom typu x86 (AMD Epyc najnovšej generácie alebo ekvivalent) s min. 32 jadrami a s frekvenciou min. 2.5 GHz s výkonom dávajúcim skóre pri osadení dvomi procesormi min. 780 bodov podľa benchmarku SPECrate®2017_fp _base. Server musí mať zapnuté BIOS-om (nie procesorom) riadené zapínanie a vypínanie jadier na procesore a BIOS-om riadené nastavovanie turbo limitov min. na úrovni mínus 1 až 3 bin a to bez zvýšenia latencie pri prepínaní do turbo módu.

Počet soketov a počet osadených CPU	Server s minimálne dvomi socketmi, osadenými dvomi procesormi.
Pamäť	Min. 512 GB operačnej pamäte; rýchlosť použitých pamäťových modulov min. 5600MT/s; server s min. 32 DIMM slotmi typu DDR5.
LAN konektivita	Min. 4x 10/25Gb Ethernet port (bez SFP28 modulov) a min. 2ks 1Gbps Ethernet adaptér RJ45.
SAN konektivita	Žiadna - HCI riešenie.
Interné úložiská dát	Min. M.2 SSD/NVMe disky v potrebnej kapacite.
USB / SD port	Min. 3x USB porty prístupné zvonku. Vonkajšie USB porty musia byť vypínateľné a zapínateľné počas prevádzky bez potreby rebootu servera. Možnosť osadenia minimálne jedného USB portu vo vnútri servera.
PCI sloty	Min. 3 sloty PCIe x16.
Grafický adaptér	Integrovaný grafický adaptér, 2x VGA port, z toho jeden na prednej strane servera.
Bezpečnosť	TPM 2.0, ochranný kryt, systém na detekciu a indikáciu otvorenia šasi servera.
Napájanie	Navzájom redundantné Hot swap napájacie zdroje, účinnosť min. Titanium.
Chladenie	Navzájom redundantné ventilátory.
Správa a manažment	Servisný procesor pre systémový manažment poskytujúci podporu vzdialeného manažmentu servera prostredníctvom siete Internet alebo intranet pomocou bezpečnej kryptovanej komunikácie (SSL, SSH, AES, 3DES), podpora štandardu IPMI 2.0. Požadujeme aj rozšírené funkcie ako: - Podpora grafického rozhrania; Virtual Media, dvojfaktorová autentifikácia s integráciou do adresárovej služby, podpora záznamu a spätného prehrávania bootovacej obrazovky. - Rozšírená bezpečnostná ochrana na úrovni BIOSu/uEFI servera, verifikácia autenticity firmware, automatická obnova poškodeného / neautentického firmware servera, pravidelné skenovanie firmware servera. - Možnosť štartu, reštartu a vypnutia servera prostredníctvom z siete LAN, nezávisle od operačného systému. - Možnosť automaticky registrovať servisné incidenty vzniknuté v rámci servera u výrobcu. - Zobrazovanie konfigurácie servera a zmeny nastavení na LCD panely servera, s jednoduchou indikáciou chybného komponentu. - Možnosť zobrazovania konfigurácie servera a zmeny nastavení pomocou blootooth/wi-fi protokolu na mobilnom zariadení. - Možnosť zasielania, vyhodnocovania a dlhodobého sledovania telemetrických údajov v cloud nástroji výrobcu HW, vrátane porovnania bezpečnostných nastavení servera voči všeobecne platným bezpečnostným normám. - Licencie, resp. softvér potrebný na prevádzku, konfiguráciu a správu servera uvedenú funkcionalitu poskytuje s kapacitne a časovo neobmedzeným licenčným pokrytím pre daný server.

Vyhotovenie	Server umiestniteľný do technologického stojana (racku), max. výška servera 1U. Požadujú sa koľajnice pre osadenie do stojana a rameno na vedenie kabeláže, umožňujúce výkon servisu servera vysunutého zo stojana v zapnutom stave. Z dôvodu zabránenia možnosti kompromitácie servera „na ceste“ sa požaduje verifikácia stavu dodaného servera voči stavu hardvéru a firmvéru z výrobného závodu výrobcu.
Servisná podpora	Minimálne 5 rokov od dodania s výmenou vadného dielu nasledujúci pracovný deň, nahlasovanie incidentov v režime 24x7, pričom oprava aj výjazd technika na opravu je pokrytý touto podporou. V prípade poruchy a výmeny diskov, ostávajú disky v majetku verejného obstarávateľa. Možnosť predĺženia štandardnej záruky na min. 7 rokov od dodania. Obstarávateľ požaduje možnosť bezplatného sťahovania updatov firmvérov a ovládačov bez porušenia zmluvných podmienok výrobcu aj po uplynutí definovanej servisnej podpory a to priamo obstarávateľom priamo zo stránky výrobcu.
Softvér	Softvér - pre správu distribuovaných prostredí (popísaný samostatne). Predmetom dodávky sú aj licencie pre SW - pre správu distribuovaných prostredí zameraného na poskytovanie funkcionalít PaaS (Platform as a Service) a kontajnerových aplikácií pre operačné systémy Linux pre všetky servery s podporou priamo od výrobcu tohoto softvéru. Verejný obstarávateľ nepredpokladá použitie serverov, virtuálnych serverov ani kontajnerov na báze operačného systému MS Windows.

Pásková knižnica pre zálohovanie

Parameter	**Minimálne požiadavky**
Základná charakteristika	Pásková knižnica s min. 1x LTO9 páskovou hlavou s rozhraním SAS. Pásková knižnica rozšíriteľná na min. 3x páskovú hlavu v rámci základného zariadenia, možnosť použitia páskových hláv rôznych generácií (min. LTO 7, 8 a 9), ako aj rôznych rozhraní (min. SAS a FC). 40ks LTO9 páskové médium označené čiarovým kódom, 1ks čistiace médium. Možnosť osadenia 40 páskových médií v rámci základného zariadenia.
Prevedenie	Knižnica umiestniteľná do technologického stojana (racku) 19". Max. výška páskovej knižnice 3U. Elektrické napájanie páskovej knižnice jednofázové 230V.
Rozšíriteľnosť	Rozšíriteľnosť na 280 páskových médií a 21 páskových hláv pridaním expanzných boxov.
Príslušenstvo	Napájacia kabeláž pre pripojenie zariadenia do elektrickej siete; dátová kabeláž pre pripojenie páskovej knižnice k zálohovaciemu serveru s dĺžkou min. 2m.
Servisná podpora	Minimálne 5 rokov od dodania s výmenou vadného dielu nasledujúci pracovný deň, nahlasovanie incidentov v režime 24x7, pričom oprava aj výjazd technika na opravu je pokrytý touto podporou. V prípade poruchy a výmeny páskových médií, ostávajú páskové médiá v majetku verejného obstarávateľa.

Externá pásková mechnika pre zálohovanie

Parameter	Minimálne požiadavky
Základná charakteristika	Externá pásková mechanika s min. 1x LTO9 páskovou hlavou s rozhraním SAS.
Prevedenie	Externá pásková mechanika umiestniteľná do technologického stojana (racku) 19". Max. výška externej páskovej mechaniky 1U. Elektrické napájanie externej páskovej mechaniky jednofázové 230V.
Príslušenstvo	Napájacia kabeláž pre pripojenie zariadenia do elektrickej siete; dátová kabeláž pre pripojenie zariadenia k zálohovaciemu serveru s dĺžkou min. 2m.
Servisná podpora	Minimálne 5 rokov od dodania s výmenou vadného dielu nasledujúci pracovný deň, nahlasovanie incidentov v režime 24x7, pričom oprava aj výjazd technika na opravu je pokrytý touto podporou. V prípade poruchy a výmeny páskových médií, ostávajú páskové médiá v majetku verejného obstarávateľa.

LAN prepínač / LAN SWITCH - typ 1

Parameter	Minimálne požiadavky
Model – prevedenie	Manažovateľný sieťový prepínač 24 portový s modulárnou šachtou pre uplink sieťový modul. Prepínacia kapacita 176 Gbps. Forwarding rate 130 Mpps. Osadené 2x redundantné identické napájacie zdroje vymeniteľné za chodu AC. Sieťový prepínač umiestniteľný do technologického stojana (racku) 19“. Sieťový prepínač disponujúci dostatočnou kapacitou pre plnohodnotné obslúženie všetkých požadovaných dátových prenosov.
Manažment	Manažment cez CLI, Web, voliteľne Centrálny manažment systém. Možnosť monitorovania cez cloudový dashboard. Podpora NETCONF, RESTCONF, YANG, PnP Agent, PnP. Manažment port.
Stohovanie	Osadený stohovací modul s priepustnosťou stohovacej zbernice 160 Gbps. Možnosť zapojiť až 8 sieťových prepínačov do stohu.
Parametre a protokoly	Layer 2/3 prepínač. MAC adries 32 000. IPv4 smerovacích záznamov: 4000. IPv6 smerovacích záznamov: 2000. Podpora jumbo rámcov 9198 bajtov. Layer 2, Static Routing, Routed Access (RIP, EIGRP Stub, OSPF – 1000 smerovaní), PBR, PIM Stub Multicast (1000 smerovaní), PVLAN, VRRP, PBR, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder, SSO. EIGRP, HSRP, IS-IS, BSR, MSDP, IP SLA, OSPF.
Bezpečnosť	Macsec-128.

Pripojenie na LAN	Min. 48x 10/100/1000 metalických portov. Minimálne uplink modul osadený 4x 1/10 Gbps SFP/SFP+ šachtami s voliteľným fyzickým rozhraním.
Servisná podpora	Minimálne 5 rokov od dodania s poprednou výmenou zariadenia v prípade poruchy nasledovný pracovný deň v režime 8x5xNBD. Riešenie systémovým inžinierom vendora v prípade dotazu aj naprieč riešeniami vendorov tretích strán.
Optické moduly	**Minimálne požiadavky**
Model – prevedenie	SFP+ 10G single módový transciever modul pre 10G SFP+ porty s podporou kabeláže do 40km 10GBASE-ER SFP.

Samostatný sieťový L3 prepínač pre Dátové Centrá - typ 1

Parameter	**Minimálne požiadavky**
Samostatné manažovateľné prepínače pracujúce na 2. a 3. vrstve OSI	- prevedenie pre samostatné použitie s možnosťou použitia s centrálnym riadiacim systémom, - priepustnosť 7,2 Tbps, resp. 2,4 bpps, - 36 portov 40/100GE QSFP28, - podpora režimov 1/10/25/40 natívne/50 GE - (kombináciou breakout káblov a okrem vyhradených portov), - max. veľkosť 1RU, - Podpora AC napájania, redundantné zdroje, - Hot swap vymeniteľné zdroje aj ventilátory, prúdenie vzduchu portami smerom von.
Vlastnosti	- jednotný softvér (obraz) pre celý rad zariadení, - jednotné konfiguračné rozhranie, - dedikované rozhranie pre OOB, - zdvojenie fyzických zariadení do jedného logického celku vrátanie zdvojnásobenia výkonu (vPC), - MAC adries až do 256 000 záznamov, - voliteľná podpora IEEE 802.1ae MAC Security (MACsec), - subskripcia na 5 rokov - podpora protokolov BGP, Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol Version 2 (RIPv2), Protocol Independent Multicast Sparse Mode (PIM-SM), Source-Specific Multicast (SSM), and Multicast Source Discovery Protocol (MSDP), - IP host záznamov 896 000, - VLAN do 3967, - subkripcia na 5 rokov - podpora VXLAN s MP-BGP EVPN pomocou rozširujúcej licencie, - management aplikácie – Ansible, Chef, Puppet, SALT. YANG a štandard OpenConfig model podpora prostredníctvom RESTCONF/NETCONF, - počet port kanálov až do 512, počet liniek v port kanáli až 32.
Servisná podpora	Minimálne 5 rokov od dodania s poprednou výmenou zariadenia v prípade poruchy nasledovný pracovný deň v režime 8x5xNBD. Riešenie systémovým inžinierom vendora v prípade dotazu aj naprieč riešeniami vendorov tretích strán.

Dátový kábel	Minimálne požiadavky
Model – prevedenie	100 GBASE-CR4 pasívny metalický kábel s dĺžkou 1m.
Optické moduly	**Minimálne požiadavky**
Model – prevedenie	100G QSFP28 Transceiver 100G ER-Lite, 25km single módová optika, duplex, LC

Samostatný sieťový L3 prepínač, prístupový pre Dátové centrá - typ 2

Parameter	Minimálne požiadavky
Samostatné manažovateľné prepínače pracujúce na 2. a 3. vrstve OSI	- prevedenie predvolené pre mód použitia s centrálnym riadiacim systémom softvérovo definovanej siete, - priepustnosť 3,6 Tbps, resp. 1,2 bpps, - 48 univerzálnych portov 1/10/25GE SFP28, 6port 40/100GE QSFP28, - podpora downlink 1/10/25 GE, podpora uplink 40/100GE, - max. veľkosť 1RU, - podpora AC napájania, redundantné zdroje, - Hot swap vymeniteľné zdroje aj ventilátory, prúdenie vzduchu portami smerom von, - podpora MACSec šifrovania na všetkých downlink portoch, - rozšírenie RAM o 16 GB na maximum.
Stredná doba poruchovosti v hodinách MTBF	min. 288 000 hodín

Vlastnosti	- jednotný softvér (obraz) pre celý rad zariadení, - jednotné konfiguračné rozhranie, - dedikované rozhranie pre OOB, - zdvojenie fyzických zariadení do jedného logického celku vrátanie zdvojnásobenia výkonu (vPC), - IEEE 802.3x Flow Control, - IEEE 802.3ad (LACP), - multichassis etherchannel, - IEEE 802.1q, - IEEE 802.1Qbb Priority Flow Control, - IEEE 802.1d (Spanning Tree Protocol), - IEEE 802.1s MST, - IEEE 802.1w RSTP, - IEEE 802.1ab LLDP, - IGMPv2 a IGMPv3 snooping, - IGMP querier, - subskripcia 5 rokov - podpora VXLAN BGP EVPN, podpora Multi-Site nasadenia, - voliteľná podpora protokolu Precision Time Protocol (PTP), - možnosť podpory wire-rate MACSEC enkrypcie, - podpora protokolu pre redundanciu funkcie default gateway, - subskripcia 5 rokov - podpora min. RIPv2, OSPFv2, OSPFv3, PIM, IS-IS a MP BGP, - subskripcia 5 rokov - podpora MSDP, - podpora statického IPv4 a IPv6 smerovania, - podpora policy-based smerovania, - podpora DHCP Option 82, - podpora BFD, - Hardvérová podpora prepínania unicast aj multicast IPv4 a IPv6, - podpora IPv4/IPv6 host záznamov 1 792 000.
Servisná podpora	Minimálne 5 rokov od dodania s poprednou výmenou zariadenia v prípade poruchy nasledovný pracovný deň v režime 8x5xNBD. Riešenie systémovým inžinierom vendora v prípade dotazu aj naprieč riešeniami vendorov tretích strán.
Dátový kábel	**Minimálne požiadavky**
Model – prevedenie	100 GBASE-CR4 pasívny metalický kábel s dĺžkou 1m.

Samostatný sieťový L3 prepínač, prístupový pre Dátové centrá - typ 3

Parameter	Minimálne požiadavky
Samostatné manažovateľné prepínače pracujúce na 2. a 3. vrstve OSI	- prevedenie predvolené pre mód použitia s centrálnym riadiacim systémom softvérovo definovanej siete, - priepustnosť 2,16 Tbps, - 48 portov 100M/1/10GBASE-T, 6port 40/100GE QSFP28, - podpora uplink 10/25/40/50/100GE, - max. veľkosť 1RU, - podpora AC napájania, redundantné zdroje, - Hot swap vymeniteľné zdroje aj ventilátory, prúdenie vzduchu portami smerom von.
Vlastnosti	- jednotný softvér (obraz firmware pre celý rad zariadení), - jednotné konfiguračné rozhranie, - dedikované rozhranie pre OOB, - zdvojenie fyzických zariadení do jedného logického celku vrátanie zdvojnásobenia výkonu (vPC), - IEEE 802.3x Flow Control, - IEEE 802.3ad (LACP), - multichassis etherchannel, - IEEE 802.1q, - IEEE 802.1Qbb Priority Flow Control, - IEEE 802.1d (Spanning Tree Protocol), - IEEE 802.1s MST, - IEEE 802.1w RSTP, - IEEE 802.1ab LLDP, - IGMPv2 a IGMPv3 snooping, - IGMP querier, - subskripcia 5 rokov - podpora VXLAN BGP EVPN, podpora Multi-Site nasadenia, - voliteľná možnosť podpory wire-rate MACSEC enkrypcie, - podpora protokolu pre redundanciu funkcie default gateway, - subskripcia 5 rokov - podpora protokolov RIPv2, OSPFv2, OSPFv3, PIM, IS-IS a MP BGP, MSDP, policy based smerovania, - podpora statického IPv4 a IPv6 smerovania, - podpora policy-based smerovania, - podpora DHCP Option 82, - podpora BFD, - hardvérová podpora prepínania unicast aj multicast IPv4 a IPv6, - podpora IPv4/IPv6 host záznamov 1 792 000.
Servisná podpora	Minimálne 5 rokov od dodania s poprednou výmenou zariadenia v prípade poruchy nasledovný pracovný deň v režime 8x5xNBD. Riešenie systémovým inžinierom vendora v prípade dotazu aj naprieč riešeniami vendorov tretích strán.
Dátový kábel	**Minimálne požiadavky**
Model – prevedenie	100 GBASE-CR4 pasívny metalický kábel s dĺžkou 1,5 m.

Samostatný sieťový L3 prepínač, kostrový pre Dátové centrá - typ 4

Parameter	Minimálne požiadavky
Samostatné manažovateľné prepínače pracujúce na 2. a 3. vrstve OSI	- prevedenie predvolené pre mód použitia s centrálnym riadiacim systémom softvérovo definovanej siete, - priepustnosť 25,6 Tbps, , resp. 4,17 bpps, - 32 portov 400G QSFP-DD, - podpora režimov 200G (QSFP56), 100G (QSFP28) and 40G (QSFP+) portov a 4x10G, 4x25G, 4x50G, 4x100G a 2x200G (kombináciou breakout káblov), podpora wire-rate MACsec enkrypcie na posledných 8 portoch, - max. veľkosť 1RU, - podpora AC napájania, redundantné zdroje, - Hot swap vymeniteľné zdroje aj ventilátory, prúdenie vzduchu portami smerom von, - systémová pamäť 32GB, diskové úložisko SSD 128GB.
Vlastnosti	- jednotný softvér (obraz) pre celý rad zariadení, - jednotné konfiguračné rozhranie, - dedikované rozhranie pre OOB, - zdvojenie fyzických zariadení do jedného logického celku vrátanie zdvojnásobenia výkonu (vPC), - MAC adries až do 1 milión záznamov, - IEEE 802.1ae MAC Security (MACsec), - subskripcia na 5 rokov: podpora protokolov BGP, Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol Version 2 (RIPv2), Protocol Independent Multicast Sparse Mode (PIM-SM), Source-Specific Multicast (SSM), and Multicast Source Discovery Protocol (MSDP), - IP host záznamov 2 milióny, - VLAN do 4096 z toho 127 rezervovaných, - subskripcia na 5 rokov vrátane funkcionality: podpora VXLAN s MP-BGP EVPN, podpora Multi-Site nasadenia, - management aplikácie – Ansible. YANG a štandard OpenConfig model podpora prostredníctvom RESTCONF/NETCONF, - počet port kanálov až do 512, počet liniek v port kanáli až 32.
Servisná podpora	Minimálne 5 rokov od dodania s poprednou výmenou zariadenia v prípade poruchy nasledovný pracovný deň v režime 8x5xNBD. Riešenie systémovým inžinierom vendora v prípade dotazu aj naprieč riešeniami vendorov tretích strán.
Dátový kábel	**Minimálne požiadavky**
Model – prevedenie	100 GBASE-CR4 pasívny metalický kábel s dĺžkou 1,5 m.

NextGen firewall - typ 1

Parameter	Minimálne požiadavky
Porty	min. 8x RJ45, min. 2x SFP, min. 2x 10G SFP+.

Priepustnosť so stavovou inšpekciou	min. 6 Gbps
IPS priepustnosť	min. 6 Gbps
Počet spojení	min. 400K
Počet nových spojení za sekundu	min. 100K
Priepustnosť TLS	min. 1 Gbps
Počet VPN spojení	min. 400
Prevedenie	Firewall umiestniteľný do technologického stojana (racku) 19". Max. výška firewall-u 1U.
Disk	Min. 200 GB.
Ostatné vlastnosti	**1. Funkcie firewallu** - Stavová a nestavová filtrácia paketov na kontrolu prenosu. - Detailná kontrola prenosu na základe aplikácie, identity používateľa a obsahu. - Podpora Network Address Translation (NAT), vrátane dynamického a statického NAT. - Podpora firewallových operácií na vrstve 2 a vrstve 3. **2. Systém prevencie prienikov (IPS)** - Integrovaný systém prevencie prienikov (IPS) s hĺbkovou inšpekciou paketov. - Detekcia známych a neznámych hrozieb založená na signatúrach a detekcii anomálií. - Aktualizácie hrozieb v reálnom čase a automatické aktualizácie signatúr. - Podpora vytvárania a prispôsobovania vlastných pravidiel pre špecifické potreby siete. - Ochrana proti sieťovým útokom, ako sú DDoS, SQL injection a cross-site scripting (XSS). **3. Pokročilá ochrana pred malvérom** - Pokročilá detekcia hrozieb s inšpekciou súborov a malvéru. - Podpora pre sandboxing na analýzu správania neznámych súborov. - Kontinuálna analýza súborov s retrospektívnou bezpečnosťou, poskytujúca upozornenia na súbory, ktoré boli neskôr identifikované ako škodlivé. - Integrácia s globálnymi databázami hrozieb. **4. Filtrovanie URL a webová bezpečnosť** - Filtrovanie URL na kontrolu prístupu k webovému obsahu na základe kategórie, úrovne rizika a reputácie. - Detailné politiky pre filtrovanie podľa používateľov, aplikácií a obsahu. - Integrácia s inteligenciou hrozieb na blokovanie škodlivých webových stránok v reálnom čase. - Prispôsobiteľné filtrovanie URL pre konkrétne domény alebo kategórie obsahu. **5. Funkcie VPN** - Podpora pre Site-to-Site VPN a Remote Access VPN pomocou protokolov IPSec a SSL. - Podpora šifrovania pomocou AES-256, AES-GCM.

	- Bezpečný prístup pre vzdialených používateľov, integrácia s riešeniami viacfaktorovej autentifikácie (MFA). **6. Inteligencia hrozieb a bezpečnostná automatizácia** - Kontinuálne informačné kanály hrozieb v reálnom čase na ochranu pred novými hrozbami. - Automatizované reakcie na hrozby s uplatňovaním politiky na základe detegovaných hrozieb. - Podpora pre dynamické zoznamy ACL (access control lists) a automatizované aktualizácie bezpečnostnej politiky na základe inteligencie hrozieb. - Schopnosť integrácie s externými platformami SIEM (Security Information and Event Management) pre centralizované logovanie a analýzu. **7. Vysoká dostupnosť a škálovateľnosť** - Podpora nasadenia vo vysokej dostupnosti (HA) s aktívnou/aktívnou alebo aktívnou/pasívnou redundanciou. - Podpora pre clustering a vyvažovanie záťaže medzi viacerými zariadeniami. - Možnosti škálovateľnosti na zvýšenie kapacity podľa rastu sieťovej prevádzky a bezpečnostných požiadaviek. **8. Logovanie, reportovanie a monitorovanie** - Podpora centralizovaného logovania a monitorovania sieťovej prevádzky a bezpečnostných udalostí. - Podpora pre logovanie na externé úložisko alebo systémy SIEM. - Detailné logovanie s možnosťou vytvárania správ o bezpečnostných udalostiach, zdravotnom stave systému a prenosových tokoch. - Dashboard v reálnom čase s vizualizáciami prenosových vzorcov, detegovaných hrozieb a celkového výkonu systému. **9. Centralizovaná správa a kontrola politiky** - Podpora centralizovanej konzoly na konfiguráciu, monitorovanie a aktualizáciu politík naprieč viacerými zariadeniami. - Podpora riadenia prístupu na základe rolí (RBAC) na delegovanie a obmedzenie administratívneho prístupu podľa rolí. - Jednoduché grafické používateľské rozhranie (GUI) s podporou príkazového riadku (CLI) pre pokročilú konfiguráciu.
Servisná podpora	Minimálne 5 rokov od dodania zariadenia verejnému obstarávateľovi. Predmetom dodávky sú nové, doposiaľ nepoužívané plne funkčné zariadenia vrátane komplexnej implementácie a integrácie do existujúceho produkčného prostredia. Plnenie predmetu zmluvy musí byť vykonané tak, aby nedošlo k prerušeniu existujúcich prevádzkových procesov obstarávateľa.

NextGen firewall - typ 2

Parameter	**Minimálne požiadavky**
Porty	min. 8x RJ45, min. 8x 1/10G SFP+.
Priepustnosť so stavovou inšpekciou	min. 10 Gbps
IPS priepustnosť	min. 10 Gbps

Počet spojení	min. 1.5M
Počet nových spojení za sekundu	min. 150K
Priepustnosť IPsec	min. 5 Gbps
Počet VPN spojení	min. 2000
Prevedenie	Firewall umiestniteľný do technologického stojana (racku) 19". Max. výška firewall-u 1U.
Disk	Min. 900 GB.
Ostatné vlastnosti	**1. Funkcie firewallu** - Stavová a nestavová filtrácia paketov na kontrolu prenosu. - Detailná kontrola prenosu na základe aplikácie, identity používateľa a obsahu. - Podpora Network Address Translation (NAT), vrátane dynamického a statického NAT. - Podpora firewallových operácií na vrstve 2 a vrstve 3. **2. Systém prevencie prienikov (IPS)** - Integrovaný systém prevencie prienikov (IPS) s hĺbkovou inšpekciou paketov. - Detekcia známych a neznámych hrozieb založená na signatúrach a detekcii anomálií. - Aktualizácie hrozieb v reálnom čase a automatické aktualizácie signatúr. - Podpora vytvárania a prispôsobovania vlastných pravidiel pre špecifické potreby siete. - Ochrana proti sieťovým útokom, ako sú DDoS, SQL injection a cross-site scripting (XSS). **3. Pokročilá ochrana pred malvérom** - Pokročilá detekcia hrozieb s inšpekciou súborov a malvéru. - Podpora pre sandboxing na analýzu správania neznámych súborov. - Kontinuálna analýza súborov s retrospektívnou bezpečnosťou, poskytujúca upozornenia na súbory, ktoré boli neskôr identifikované ako škodlivé. - Integrácia s globálnymi databázami hrozieb. **4. Filtrovanie URL a webová bezpečnosť** - Filtrovanie URL na kontrolu prístupu k webovému obsahu na základe kategórie, úrovne rizika a reputácie. - Detailné politiky pre filtrovanie podľa používateľov, aplikácií a obsahu. - Integrácia s inteligenciou hrozieb na blokovanie škodlivých webových stránok v reálnom čase. - Prispôsobiteľné filtrovanie URL pre konkrétne domény alebo kategórie obsahu. **5. Funkcie VPN** - Podpora pre Site-to-Site VPN a Remote Access VPN pomocou protokolov IPSec a SSL. - Podpora šifrovania pomocou AES-256, AES-GCM. - Bezpečný prístup pre vzdialených používateľov, integrácia s riešeniami viacfaktorovej autentifikácie (MFA). **6. Inteligencia hrozieb a bezpečnostná automatizácia** - Kontinuálne informačné kanály hrozieb v reálnom čase na ochranu pred novými hrozbami.

	- Automatizované reakcie na hrozby s uplatňovaním politiky na základe detegovaných hrozieb. - Podpora pre dynamické zoznamy ACL (access control lists) a automatizované aktualizácie bezpečnostnej politiky na základe inteligencie hrozieb. - Schopnosť integrácie s externými platformami SIEM (Security Information and Event Management) pre centralizované logovanie a analýzu. **7. Vysoká dostupnosť a škálovateľnosť** - Podpora nasadenia vo vysokej dostupnosti (HA) s aktívnou/aktívnou alebo aktívnou/pasívnou redundanciou. - Podpora pre clustering a vyvažovanie záťaže medzi viacerými zariadeniami. - Možnosti škálovateľnosti na zvýšenie kapacity podľa rastu sieťovej prevádzky a bezpečnostných požiadaviek. **8. Logovanie, reportovanie a monitorovanie** - Podpora centralizovaného logovania a monitorovania sieťovej prevádzky a bezpečnostných udalostí. - Podpora pre logovanie na externé úložisko alebo systémy SIEM. - Detailné logovanie s možnosťou vytvárania správ o bezpečnostných udalostiach, zdravotnom stave systému a prenosových tokoch. - Dashboard v reálnom čase s vizualizáciami prenosových vzorcov, detegovaných hrozieb a celkového výkonu systému. **9. Centralizovaná správa a kontrola politiky** - Podpora centralizovanej konzoly na konfiguráciu, monitorovanie a aktualizáciu politík naprieč viacerými zariadeniami. - Podpora riadenia prístupu na základe rolí (RBAC) na delegovanie a obmedzenie administratívneho prístupu podľa rolí. - Jednoduché grafické používateľské rozhranie (GUI) s podporou príkazového riadku (CLI) pre pokročilú konfiguráciu.
Servisná podpora	Minimálne 5 rokov od dodania zariadenia verejnému obstarávateľovi. Predmetom dodávky sú nové, doposiaľ nepoužívané plne funkčné zariadenia vrátane komplexnej implementácie a integrácie do existujúceho produkčného prostredia. Plnenie predmetu zmluvy musí byť vykonané tak, aby nedošlo k prerušeniu existujúcich prevádzkových procesov obstarávateľa.

Loadbalancer + Web aplikačný firewall (WAF)

Parameter	**Minimálne požiadavky**
Šasi	max. veľkosť 1U
Zdroj	min. 650W
Redundantný	áno
Počet procesorov	min. 1x 16-core
Pamäť	min. 64GB
L4 Priepustnosť	min. 40 Gbps

L4 HTTP Počet žiadostí za sekundu	min. 2,3M
L4 Pripojenia za sekundu	min. 450K
L4 Max Concurrent Connections (1)	min. 36M
L7 Priepustnosť	min. 30 Gbps
L7 Pripojenia za sekundu (1-1)	min. 180K
L7 Počet žiadostí za sekundu (1-inf)	min. 500K
L7 Počet žiadostí za sekundu (inf-inf)	min. 1,2M
Maximum SSL súbežných pripojení	min. 4,0M
Minimálne požiadavky na funkcionalitu Loadbalancing	- Podpora vlastných skriptov pre monitorovanie dostupnosti služieb. - TCP optimalizácia pre každého pripojeného klienta nezávisle. - Podpora kopresie a cache. - SSL Session a SSL Connection mirroring cez viacero ADC zariadení. - Dynamické ladenie a nastavovanie TCP parametrov. - Schopnosť pripojenia sa na monitorovacie nástroje tretích strán cez otvorené API. - Granulárne logovanie všetkých častí komunikácie per aplikácia. - Schopnosť pracovať aj so 4k kľúčmi. - Podpora viac ako 19 LB metód. - Podpora filtrovania paketov. - Podpora ToS, QoS (marking/preservation/mimic). - Ratio based load balancing s CARP persistenciou. - Podpora pre dynamickú veľkosť záznamov TLS. - TCP Nagle Auto mode. - TCP Auto Buffer Tuning. - Schopnosť skontrolovať pripravenosť systému prímať príkazy pomocou CLI/REST API. - Schopnosť spustiť testovaci monitor alebo probe z WEB UI. - Podpora TLS Session Hash and Master Secret Extension (RFC 7627). - Podpora for MQTT Protocol. - Podpora TLS 1.3. - Podpora full proxy HTTP/2. - Vlastný skriptovací jazyk s podporou HTTP/2. - Schopnosť konvertovať HTTP/3 požiadavky od klientov na HTTP/2 a HTTP/1 na strane backendu. - Podpora pre HTTP/3. - DNS Firewall. - Inšpekcia a validácia DNS Protokolu. - ACL na základe typu záznamu DNS.

	- DNS load balancing. - Kompletné DNSSEC podpisovanie. - Centralizovaná DNSSEC key management. - DNS DDoS Detekcia a mitigácia. - Mitigácia hrozieb pomocou blokovania škodlivých IP adries. - Pokročilá DNS analytika a reporting.
Minimálne požiadavky na funkcionalitu Web aplikačný firewall (WAF)	- Ochrana voči L7 útokom aplikáciách. - Detekcia a mitigácia L7 DoS. - Detekcia a mitigácia Brute force. - Detekcia a mitigácia Heavy URL. - Detekcia a mitigácia OWASP TOP 10 útokov. - XML Firewall. - Ochrana JSON a AJAX volaní. - Zabezpečenie parametrov zmanipulovaných klientom. - Validácia prihlasovacích údajov a aplikačného toku. - Detekcia a mitigácia bot-ov a non-human aktivity vrátane tzv. Headless bot-ov. - Ochrana pred únikom citlivých dát pomocou blokovania a maskovania informácií. - Autmatická korelácia viacerých útokov do jedného incidentu. - Podpora pozitívnej a negatívnej bezpečnostnej politiky. - Podpora detekcie a blokovania útočníkov na základe geolokačnej informácie. - Podpora skenovania súborov pomocou ICAP. - Ochrana SMTP a FTP protokolova na aplikačnej vrstve. - Podpora PCI-DSS, HIPAA, SOX, Basel II. - Preddefinovaná bezpečnostná politika pre Microsoft Outlook Web Access a Microsoft SharePoint. - Možnosť aplikovania rôznej bezpečnostnej politiky na IP adresu, doménové meno a URI. - Možnosť importovať výsledky z penetračných testov web aplikácií. - Podpora pre filtrovanie a vynucovanie politiky pre WebSocket komunikáciu. - Blokovanie IP adries, ktoré opakovane porušujú bezpečnostnú politiku priamo v dedikovaných HW komponentoch. - Podpora vytvárania unikátneho odtlačku zariadenia/klienta. - Podpora vrstvených bezpečnostných politík. - Podpora pre vynútenie globálnych bezpečnostných vlastností a nastavení cez všetky bezpečnostné politiky. - Vyhodnotenie reputácie klienta pri automatickom budovaní bezpečnostnej politiky. - Podpora pre SPA - Single Page Applications. - Automatická detekcia typov back-end serverov. - Podpora parsovania JSON parametrov. - Automatické nastavenie parametrov pre L7 DDoS ochranu. - Možnosť nevynucovať (iba sa učiť a budovať) bezpečnostnú politiku pre určité doménové mená. - Možnosť deaktivovať konkrétne signatúry pre URL, HTTP hlavičku a parametre. - Podpora nasadenia na SPAN/Mirror porte. - Možnosť šifrovať senzitívne údaje na strane klienta bez nutnosti úpravy chránenej aplikácie.

	- Detekcia automatickej modifikácie formulárových dát na strane klienta bez potreby úpravy chránenej aplikácie. - Podpora aplikácií postavených na GraphQL. - Možnosť mitigácie tzv. False-positives na základe offline ML modelu. - Detekcia a mitigácia SSRF útokov. - Možnosť exportovať a kompletnú WAF politiku v JSON formáte. - Podpora OpenAPI serializáciu pre Array, Style, Explode a parametre Path. - SSL VPN Vzdialený prístup. - Podpora Radius autentifikacie.
Servisná podpora	Minimálne 5 rokov od dodania zariadenia verejnému obstarávateľovi.

NTP Server

Parameter	**Minimálne požiadavky**
Príslušenstvo	Min. 1x GNSS anténa (GPS / Galileo / GLONASS / Beidou). Min. 1x 20 m anténny kábel Belden H155 alebo ekvivalent (SMA male / N-Norm male). Min. 2x dvojdielna súprava napájacieho kábla. Min. 1x Accessory-kit - montážna sada na anténu.
Zdroj	Min. 2x 100-240 V AC / 100-200 V DC. Redundantný.
Referenčné vstupy	Min. GNS, PPS, 10MHz, IRIG, NTP with OCXO-HQ .
Výstupy	Min. 1x LAN 10/100 MBit, RJ45 konektor. Min. 3x LAN 10/100/1000 MBit, RJ45 konektor. Min. 2x RS232, nezávislý, 9pin D-Sub female konektor, s časovými reťazcami viacerých formátov údajov. Min. 1x PPS, TTL - 50 ohm, pulse duration 200 msec active high, female BNC konektor. Min. 1x štandardná frekvencia 10 MHz, TTL - 50 ohm, female BNC konektor. Min. 1 x Alarm Relay Output, change-over contact, 3pin DFK konektor.
Iné	Inštalácia a konfigurácia zariadenia. Drobný materiál, poprípade kabeláž potrebná pre inštaláciu zahrnuté v cene dodávky.
Servisná podpora	Minimálne 5 rokov od dodania zariadenia verejnému obstarávateľovi.

HSM

Parameter	**Minimálne požiadavky**
Popis	Min. výkon podpisu RSA (tps) pre dĺžky kľúča - 2048 bit / 3949, 4096 bit / 814. Min. výkon podpisu hlavnej krivky ECC (tps) pre dĺžky kľúčov NIST - 256 bit / 7553. Min. symetrické šifrovanie (KB/s) 1024 bajtov čistého textu - 3 DES 168 bit / 685, AES 128 bit / 825. Min. generovanie kľúča s aktiváciou ECC (kľúčov/s) - RSA 2048 bit / 20, ECDSA P-256 bit / 3580, ECDSA P-521 bit / 2480. HSM umiestniteľný do technologického stojana (racku) 19“. Max. výška HSM 1U.

Asymetrické algoritmy	RSA, Diffie-Hellman, ECMQV, DSA, El- Gamal, KCDSA, ECDSA, ECDH, Edwards (Ed25519, Ed25519ph).
Symetrické algoritmy	AES, AES-GCM, Arcfour, ARIA, Camellia, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, 3DES. Hash / Message-Diges: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160, SHA-3 (224, 256, 384, 512 bit).
Podporované operačné systémy	Microsoft Windows Server a Linux Red Hat, SUSE.
Súlad s bezpečnosťou	Plný súlad NIST Suite B implementation.
Certifikácia	Certifikácia FIPS 140-3 Level 3. Certifikácia eIDAS a Common Criteria EAL4 + AVA_VAN.5 a ALC_FLR.2 podľa EN 419 221-5 Protection Profile.
Servisná podpora	Minimálne 5 rokov od dodania zariadenia verejnému obstarávateľovi.

Technologický stojan (rack), zdroj nepretržitého napájania (UPS)

Technologický stojan s PDU	
Parameter	**Minimálne požiadavky**
Prevedenie rozvádzača	- 19 palcový stojanový rozvádzač so zváraným skeletom a s nosnosťou viac ako 1700 kg - Využiteľná kapacita 42U s pôdorysom (600 mm x 1070 mm) - S predprípravou pre inštaláciu klimatizačných jednotiek umiestnených na strope - Výška rozvádzača bez klimatizačnej jednotky nepresiahne výšku 2m - Rozvádzač má predné jednodielne dvere a dva bez použitia náradia ručne odnímateľné kryty - Dvere rozvádzača s viacbodovým zámkom s posuvným zamykacím systémom, ktorý zabezpečí dokonalé tesnenie dverí voči skeletu rozvádzača. - Rozvádzač obsahuje dva páry 19 palcových vertikálnych líšt pre jednoduché a bezpečné osadenie inštalovaných zariadení. - Všetky oddeliteľné časti rozvádzača sú galvanicky vzájomne pospájané, rozvádzač obsahuje spoločný zemniaci bod. - Jednotný kľúč pre všetky zámky.
Prevedenie PDU - rozvádača	- Rozvádzač musí byť osadený dvoma monitorovanými PDU napájacími panelmi. - Výstup min. 20x IEC 60320 C13, a 4x IEC 60320 C19. - Vstup IEC 60309 16 A 2P + E. - Vrátane napájacieho kábla dĺžky min. 3m. - Maximálny vstupný prúd 16A. - Menovité výstupné napätie 230V. - Rozmery PDU v mm - D x Š x V = (902 x 44 x 62).

Zdroj nepretržitého napájania (UPS)	
Parameter	**Minimálne požiadavky**
Prevedenie UPS	- Max. výška zdroja nepretržitého napájania 6U (UPS vrátane batérií), všetok hardvér potrebný pre montáž do technologického stojana (racku) musí byť súčasťou dodávky. - On-line s dvojitou konverziou, automatický test batérií, výmena batérií počas chodu, eco mód pre šetrenie energie. - Vstavané meranie spotrebovanej energie a zobrazovanie účinnosti UPS, grafický displej s podsvietením, interný bypass (automatický aj manuálny). - Nominálny výstupný výkon min. 8 kVA / 8 kW. - Napájanie na vstupe UPS 230 V / 40 Hz - 70 Hz (automaticky nastaviteľné). - Napájanie na výstupe 230 V / 50 Hz -60 Hz (+/-3 Hz - automaticky nastaviteľné, ± 0,1 Hz užívateľsky nastaviteľné). - Min. 1x port RJ-45 10/100 Base-T, s monitoringom prostredia a podporovanými protokolmi: HTTP, HTTPS, IPv4, IPv6, NTP, SMTP, Modbus TCP, SNMP v1, SNMP v2c, SNMPv3. - Manažment softvér potrebný pre inštaláciu musí byť súčasťou dodania. - Pripojenie vstupu UPS svorkovnica alebo zásuvka podľa potreby. - Pripojenie výstupu UPS min. 6x IEC 320 C13 + 4x IEC 320 C19. - Požadovaný čas zálohovania min. 5 minút pri záťaži 8 kW.
Servisná podpora	Minimálne 5 rokov od dodania zariadenia verejnému obstarávateľovi.

Softvér - pre správu distribuovaných prostredí

Parameter	**Minimálne požiadavky**
Funkčný popis	Riešenie / Platforma pre správu distribuovaných prostredí, zamerané na poskytovanie funkcionalít PaaS (Platform as a Service) a kontajnerových aplikácií pre operačné systémy Linux aj Windows. Hlavným cieľom je umožniť prevádzku a správu veľkého množstva aplikácií prostredníctvom moderných nástrojov a technológií, ktoré zjednodušujú a automatizujú ich vývoj a nasadenie. Platforma musí umožňovať samoobslužné používanie (napr. pomocou GitOps pristupu) a umožniť vývojárom jednoduchú tvorbu a prevádzku aplikácií v kontajneroch. Taktiež musí podporovať automatické škálovanie aplikácií na základe ich zaťaženia, čo zaručuje efektívne využívanie systémových zdrojov. Zásadná je klastrová architektúra, ktorá zabezpečuje vysokú dostupnosť, rozloženie záťaže a možnosť zálohovania dát. Systém musí ponúkať užívateľské rozhranie pre vývojárov aj správcov, podporu pre serverless prostredia (FaaS), integrovaný register kontajnerov s možnosťou riadenia ich verzií a bezpečnostných pravidiel. Okrem toho musí podporovať klastrové služby pre Linux a Windows kontajnery a automatizovanú správu zdrojov a systémových operácií. Jednou z požiadaviek je možnosť správy platformy cez príkazový riadok, webové rozhranie a IDE (integrované vývojové prostredie). Platforma musí mať aj integrovaný marketplace, ktorý umožňuje pridať ďalšie funkcie a nástroje. Dôležitá je bezvýpadková aktualizácia platformy a aplikácií, čo je kľúčové pre minimalizáciu prestojov počas prevádzky.

	Platforma musí byť takisto kompatibilná s nástrojmi na podporu tvorby aplikácií - konkrétne nástroje na tvorbu integrácií, streamovania dát, jednotného prihlasovania aplikácií a tvorbu API rozhraní.
Požiadavky na správu a bezpečnosť	Platforma musí podporovať inštaláciu na rôzne typy infraštruktúr vrátane fyzických (bare metal) a virtuálnych serverov, ale aj verejných cloudových prostredí ako AWS, Microsoft Azure či Google Cloud. Automatizácia správy a škálovania klastrov je jedným z hlavných cieľov, pričom riešenie musí ponúkať centralizovanú správu klastrov, bezpečnostných politík a monitorovacích dashboardov, ktoré umožnia správcom sledovať stav infraštruktúry a rýchlo reagovať na problémy. Z bezpečnostného hľadiska musí platforma detekovať zraniteľnosti v kontajneroch, poskytovať auditné nástroje na sledovanie zmien v systéme a umožniť integráciu s Open Policy Agent pre rozšírenie bezpečnostných politík. Súčasťou bezpečnostných požiadaviek je tiež vizualizácia sieťovej komunikácie medzi kontajnermi a odporúčania na optimalizáciu oprávnení, ktoré zvyšujú bezpečnosť systému.
Všeobecné požiadavky na softvérový produkt	- Samoobslužná platforma pre vývojárov aplikácií, ktorá umožňuje vytvárať a prevádzkovať aplikácie v Linux a Windows kontajneroch. - Platforma musí umožňovať automatické škálovanie prevádzkovaných aplikácií. - Platforma musí mať klastrovú vrstvu služieb pre Linuxové a Windows kontajnery, ktorá zabezpečí ich vysokú dostupnosť a rozloženie záťaže. - Platforma musí umožňovať automatizáciu činností ako je prideľovanie zdrojov, či systémová správa platformy. - Platforma musí umožňovať správu platformy pomocou príkazového riadku, web konzoly a integrovaných vývojárskych prostredí. - Platforma musí mať integrovaný register kontajnerov so samostatnými repozitármi pre rôzne aplikácie (separácia images per app), musí umožňovať nastavovanie vlastných pravidiel (napr. mazanie starších image podľa definovaných pravidiel či “garbage collection”), - Platforma musí mať integrovaný katalóg služieb. - Integrovaný marketplace pre rozšírenie platformy o ďalšie funkcionality. - Platforma musí umožňovať jednoduchý “debugging” kontajnerových aplikácií bežiacich v klastri. - Platforma musí umožňovať updatovanie softvérového produktu bez výpadku služieb prevádzkovaných v spustených kontajneroch. - Platforma musí umožňovať aktualizáciu aplikácii prevádzkovaných v spustených kontajneroch bez výpadku služieb nimi poskytovaných. - Platforma musí poskytovať webové služby (API) pre integráciu s CI/CD nástrojmi ako GitLab. - Platforma musí poskytovať nástroje pre vytváranie a testovanie kontajnerov. - Platforma musí poskytovať nástroje pre centralizované nasadzovanie aplikácií. - Autentifikácia používateľov softvérového produktu musí umožňovať integráciu s Active Directory. - Autentifikácia používateľov softvérového produktu musí podporovať SSO pre integráciu s viacerými identifikačnými autoritami. - Platforma musí poskytovať API pre zálohovanie a obnovu aplikácii (vrátane ich nastavenia) v klasteri vrátane ich perzistentných dát. - Platforma musí umožňovať zálohovanie konfigurácie a obnovu do pôvodného stavu v prípade poruchy. - Platforma musí mať integrované role a umožňovať prideľovanie rôznych úrovní práv na rôzne časti platformy týmto roliam, musí mať samostatnú rolu umožňujúcu monitorovanie kontajnerov a tiež samostatné role pre

	nasadzovanie kontajnerov, musí umožňovať prístup len k niektorým repozitárom v registry, s rôznymi právami (čítanie images, zápis images). - Platforma musí umožňovať audit a logovanie zmien (najmä zmien v registri images a tiež deploymentov a rollbackov), musí umožňovať vytváranie a prezentáciu reportov v UI. - Platforma musí mať integrovaný natívny kontajner storage s nasledovnými vlastnosťami: o dopĺňa celkové riešenie o vrstvu softvérovo definovaného úložiska dát (storage), o poskytuje perzistentné úložisko dát pre kontajnery, o poskytuje automatickú dynamickú škálovateľnosť perzistentného storage pre kontajnery, o umožňuje vývojárom aplikácií pridávať, či meniť veľkosť perzistentného storage bez nutnosti zásahu zo strany správcu platformy, o poskytuje vysokú dostupnosť storage rovnako ako ostatné súčasti platformy. - Platforma musí byť on-premise riešenie, ktoré bude celé realizované v dátových centrách verejného obstarávateľa. - Platforma musí podporovať automatizovanú inštaláciu do public cloudov ako AWS, Microsoft Azure, Google Cloud Platform, Microsoft Azure Government, bare metal, Red Hat OpenStack Platform, VMware vSphere.
Požiadavky na vytváranie, nasadzovanie a beh aplikácií	- Softvérový produkt poskytuje užívateľské prostredie určené pre vývojárov, umožňujúce jednoduchým spôsobom sledovať topológiu aplikácie, stav vytvárania a nasadenia aplikácie. - Softvérový produkt poskytuje užívateľské prostredie zamerané na správu produktu. - Softvérový produkt poskytuje vývojové prostredie (IDE) v prehliadači. - Softvérový produkt umožňuje jednoduchý prevádzku prostredia pre chod serverless (FaaS). - Softvérový produkt umožňuje automatické škálovanie aplikácií.
Požiadavky na správu platformy (Day 2 operations)	- Možnosť Inštalácie na Bare Metal servery, Virtuálne servery a do public cloud prostredí. - Softvérový produkt umožňuje automatické škálovanie prevádzkovaných klastrov. - Upgrade Softvérového produktu je plne automatizovaný. - Softvérový produkt je nezávislý na jedinom dodávateľovi HW/SW pre úložisko a sieťové prvky.

Požiadavky na multiklaster	- Centralizovaná správa plne automatizovaného vytvárania nových klastrov. - Centralizovaná správa upgrade spravovaných klastrov. - Centralizované kontinuálne nasadzovanie do skupiny klastrov pre dané prostredie (napr. test, preprod, či prod), ktoré je vizualizované v UI. - Centralizovaná správa nastavenie bezpečnostných politik. - Centralizovaný monitoring spravovaných klastrov. - Centralizovaný monitoring dashboard . - Centralizovaná správa nastavenie bezpečnostných politik. - Centralizovaný monitoring spravovaných klastrov. - Súčasťou automatizovaného vytvárania, či upgradu klastrov je možnosť spúšťať automatizačné úkony, ktoré nastavujú nekontajnerizovanú infraštruktúru mimo Softvérový produkt, ako sú napríklad sieťové prvky, úložisko, DNS, či Load Balancery. - Dynamické vyhľadávanie pre zobrazovanie a investigaciu aplikácií naprieč spravovanými klastrami. - Automatizovaná analytika softvérového produktu, ktorá proaktívne kontroluje stav klastrov a navrhuje opravné kroky. - Centralizovaná správa obsahuje politiky pre nastavenie bezpečnosti, odolnosti, a konfiguračnej správy. - Súčasťou automatizovaného nasadzovania, či upgradu aplikácií je možnosť spúšťať automatizačné úkony, ktoré nastavujú nekontajnerizovanú infraštruktúru mimo Softvérový produkt, ako sú napríklad sieťové prvky, úložisko, DNS, či Load Balancery.
Požiadavky na bezpečnosť	- Platforma zobrazuje zraniteľnosti v aktuálne bežiacich kontajneroch. - Governance a risk dashboard, ktorá zobrazuje bezpečnostné riziká a porušenia predpísaných bezpečnostných politik. - Hromadná správa bezpečnostných politik skupiny klastrov. - Integrácia s Open Policy Agent (OPA) pre rozšírenie bezpečnostných a iných politík. - Poskytuje pohľad na aplikácie, ich kontajnerové image a nastavenia z hľadiska bezpečnosti. - Zobrazuje sieťovú komunikáciu naprieč samotného klastra. - Obsahuje politiky pre kontrolu pri vytváraní a nasadzovaní kontajnerových image z hľadiska známych zraniteľností. - Obsahuje prehľadný dashboard stavu compliance klastrov pre potreby auditu. - Vizualizuje povolenú a zakázanú sieťovú komunikáciu a doporučuje úpravu sieťovej komunikácie pre odobratie nadbytočných sieťových oprávnení. - Analýza oprávnení prístupu k citlivým informáciám. - Bezpečnostný softvér poskytuje API pre integraciu s externými DevOps systémami, zahrňujúcimi CI/CD nástroje, skenovanie image a SIEM (security integration event management) riešeniami. - Ponúka kontajnerovú base image, čím zaručuje podporu a updaty. - Súčasťou nápravy klastrov, ktoré nespĺňajú požiadavky z pohľadu compliance, je možnosť spúšťať automatizačné úkony, ktoré nastavujú nekontajnerizovanú infraštruktúru mimo softvérový produkt.

Požiadavky na integráciu	- Platforma musí podporovať tvorbu a správu klastrov pre Stream Messaging, ako napr. Apache Kafka. - Platforma musí podporovať governance APIs, ako je API dokumentácia, API schéma, API poskytovatelia, API konzumenti. - Platforma taktiež musí podporovať správu API, ako sú prevádzkové parametre, verzovanie, logy, metriky, alerty. - Pri API musí platforma podporovať implementáciu, teda Developer portál, API katalog, sdk, Mock APIs. - Platforma musí podporovať prevádzku aplikačných serverov i aplikačných frameworkov zameraných na mikroslužby, vrátane podpory reaktívneho vývoja pre vytváranie distribuovaných aplikácií.
Podpora	- Podpora priamo od výrobcu dodávaného softvérového produktu. - Dĺžka podpory 5 rokov od prevzatia softvérového produktu verejným obstarávateľom. - Nárok na aktuálne verzie softvérového produktu, prístupné prostredníctvom portálu výrobcu dodávaného softvérového produktu. - Prístup k opravným balíkom dodávaného softvérového produktu. - Podpora poskytovaná v rozsahu 24 hodín denne v 7 dni v týždni. - Podpora poskytovaná telefonicky, formou emailu, alebo cez ticketovací portál výrobcu dodávaného softvérového produktu. - Prístup k dokumentácii prostredníctvom webového portálu výrobcu dodávaného softvérového produktu. - Prioritizácia riešenia nahlásených prípadov podpory podľa ich dopadu na celkovú funkčnosť dodávaného softvérového produktu. - Doba odozvy pre príslušnú úroveň závažnosti musí byť garantovaná v nasledujúcom rozsahu: - Závažnost 1. úrovne – kritická. - Produkt nie je použiteľný, čo vedie k celkovému narušeniu práce, alebo k inému závažnému dopadu na prevádzku. Reakčná doba: 1 hodina. - Závažnost 2. úrovne – vysoká. - Zlyhanie veľmi dôležitej čiastkovej funkčnosti produktu. Prevádzka je vážne obmedzená. Reakčná doba: 4 hodiny. - Závažnost 3. úrovne – nízka. - Zlyhanie menej dôležitej čiastkovej funkčnosti produktu. Produkt nefunguje podľa špecifikácií stanovených výrobcom. Prevádzka je obmedzená len čiastočne. Reakčná doba: 1 pracovný deň. - Závažnost 4. úrovne – iná. - Nezávažný problém. Môže to byť napr. žiadosť o dokumentáciu, obecnú informáciu, žiadosť o vylepšenie a pod. Reakčná doba: 2 pracovné dni.
Licencia	Verejný obstarávateľ požaduje dodať licencie k softvérovému produktu v počte adekvátnom pre Aplikačnú vrstvu (vrátane DB) – minimálne pre servery.
Dokumentácia	Verejný obstarávateľ požaduje dodať k prevzatému softvérovému produktu technickú dokumentáciu (dokumenty je možné poskytnúť aj v elektronickej forme). Verejný obstarávateľ akceptuje technickú dokumentáciu v slovenskom, českom, alebo anglickom jazyku. Odkazy na informačné zdroje na internete nebude verejný obstarávateľ akceptovať.

Inštalačné a konfiguračné práce

Predmetom dodávky sú všetky potrebné inštalačné a konfiguračne práce v minimálne dvoch lokalitách podľa požiadaviek, definovaných verejným obstarávateľom. Verejný obstarávateľ požaduje vykonať implementačné, inštalačné a konfiguračné práce všetkých zariadení, pričom kabeláž a drobný inštalačný materiál sú už zahrnuté v rámci ceny dodaných zariadení.

Do ceny za dodané hardvérové zariadenia uchádzač započíta aj cenu všetkých dopravných nákladov, poistení a prípadných nákladov na vynesenie hardvéru na poschodie v mieste realizácie predmetu zákazky a cenu za práce/aktivity v nasledovnom rozsahu:

- High level design.
- Low level design.
- Fyzická inštalácia hardvéru - vybalenie, kompletizácia a montáž dodaného hardvéru do technologického stojana (racku) vrátane aktualizácie firmvéru a základnej konfigurácie po prvom štarte.
- Zapojenie káblov/kabeláže.
- Konfigurácia systémových nastavení hardvéru a implementáciu softvéru podľa doporučení výrobcu.
- Likvidácia odpadu/obalových materiálov.
- Vypracovanie/aktualizácia dokumentácie (technickej, prevádzkovej, užívateľskej, administrátorskej a bezpečnostnej).
- Realizácia akceptačných testov.
- Zaškolenie obsluhy.