Kúpna zmluva č. Z20165212_Z

Uzatvorená v zmysle §409 a nasl. Obchodného zákonníka

I. Zmluvné strany

1.1 Objednávateľ:

Obchodné meno:	Hlavné mesto Slovenskej republiky Bratislava
Sídlo:	Primaciálne námestie 1, 81499 Bratislava-Staré Mesto, Slovenská republika
IČO:	00603481
DIČ:	2020372596
IČ DPH:	
Číslo účtu:	SK7275000000000025827813CEKOSKBX
Tel:	+421 259356342

1.2 Dodávateľ:

Obchodné meno:	TooNet, s.r.o.
Sídlo:	Seberiniho 1, 82103 Bratislava, Slovenská republika
IČO:	44962070
DIČ:	2022885601
IČ DPH:	SK2022885601
Číslo účtu:	
Tel:	+421903281193

II. Predmet zmluvy

2.1 Všeobecná špecifikácia predmetu Zmluvy:

Názov:	Nákup informačno komunikačnej technológie
Kľúčové slová:	aktívne sieťové prvky (switche, firewall a VPN systémy na obnovu informačno komunikačnej infraštruktúry WAN/LAN siete.
CPV:	32410000-0 - Lokálne siete (LAN); 32412110-8 - Sieť internet; 32413100-2 - Sieťové smerovače; 32420000-3 - Sieťové zariadenia; 32422000-7 - Sieťové komponenty; 32424000-1 - Infraštruktúra siete; 32430000-6 - Sieť WAN; 60000000-8 - Dopravné služby (bez prepravy odpadu)
Druh/y:	Tovar; Služba
Kategória služieb:	2. Služby pozemnej dopravy, vrátane služieb pancierových automobilov a kuriérskych služieb okrem prepravy poštových zásielok

2.2 Funkčná špecifikácia predmetu Zmluvy:

- Aktívne sieťové a bezpečnostné prvky (firewall, switche, a VPN systémy na ochranu perimetra, bezpečné pripojenie vzdialených pracovísk verejného obstarávateľa a obnova informačno komunikačnej infraštruktúry WAN/LAN siete.
- Ochrana perimetra siete pred prienikmi, bezpečné pripojenie vzdialených pracovísk a obnova informačno komunikačnej infraštruktúry.
- Pre zabezpečenie podmienok pre organizáciu podujatí súvisiacich so slovenským predsedníctvom v Rade EÚ v 2. polovici roku 2016 je nutné aby verejný obstarávateľ mal vybudovanú spoľahlivú a funkčnú infraštruktúru. Táto infraštruktúra musí poskytovať všetky potrebné služby, musí byť schopná odolávať bezpečnostným hrozbám zvonku, ale aj zvnútra organizácie a zároveň nebude náročná na údržbu.
- Základom novej ochrany perimetra IKT infraštruktúry bude next generation firewall od spoločnosti Palo Alto Networks v zapojení vo vysokej dostupnosti a zariadenie FortiNet. Tieto zariadenia nahradia všetky existujúce Novell Border manager servery. Palo Alto firewall bude zabezpečovať nasledovné služby:
- - Ochrana siete pomocou TCP IP a aplikačného firewallu vrátane NAT, port forwardingu, smerovania
- -
  - DNSProxy
  - IPSec a SSLVPN
  - URL filtráciu - filtrovanie prístupu na webové stránky na základe identity používateľa
  - Filtrácia aplikácií a služieb na základe identity používateľa
  - Ochranu komunikácie pred zraniteľnosťami (Antispam, Antivir, Anti-spyware, IPS)
  - QoS

• Na firewalle bude vytvorených niekoľko oddelených bezpečnostných zón:

- Internet
- DMZ - vypublikované služby
- DMZ - email relay
- LAN - lokálne pracovné stanice
- MNGT - manažment zariadení a serverov
- Servers - segment pre pripojenie serverov
- Wifi - segment pre verejnú WiFi
- VPN vzdialení používatelia
- Múzeum
- Knižnica
- Palác
- Laurinská
- Uršulínska

2.3 Technická špecifikácia predmetu Zmluvy:

Technické vlastnosti	Jednotka	Minimum	Maximum	Presne
Firewall & Proxy	0			0
Palo Alto Networks PA-3020, PN: PAN-PA-3020	ks			1
Partner enabled premium support year 1, PA-3020, PN: PAN-SVC-BKLN-3020	ks			2
Bright cloud URL Filtering subscription year 1, PA-3020, PN: PAN-PA-3020-URL2	ks			2
Threat prevention subscription for device renewal, PA-3020, PN: PAN-PA-3020-TP	ks			2
Instalation & configuration services Palo Alto	človekodeň	1	20	
IPSEC&SSLVPNconection:	0			0
FortiGate 100D 24x7 Comprehensive FortiCare, PN: FG-10-00116-247-02-12	ks			1
FortiGate 30D 1 Year 8x5 Enhanced FortiCare, PN: FG-10-00034-311-02-12	ks			3
Email filtering:	0			0
FortiMail VM02 8x5 FortiCare plus FortiGuard Bundle Contract 1 Year, PN:FC-10-0VM02-965-02-12	ks			1
Vmware vSphere Essentials Plus Kit Production Support & Subscription, PN: WMware	ks			1
Prepínače:	0			0
Summit X460-G2 48 FAN Module for Summit X460-G2 Series Switches-front to back airflow, PN:10945	ks			2
Summit X460-G2 48 300W AC Power Supply module for Summit X460,X460-G2 & E4G-400 Series Switches-Extended Temperature Range from-10 to+50 degrees Celsius, PN:10930A	ks			2
Summit X460-G2 48 PWP TAC & OS Summit 16702, PN:97004-16702	ks			2
Summit X440-48t PWP TAC & OS Summit 16505 , PN:97004-16505	ks			14
Summit X440-48p 48 X10/100/1000BASE-T PoE-plus,4X1000BASE-X unpopulated SFP(4 SFP ports shared with 10/100/1000BASE-T ports),SummitStack Stacking ports,1 AC PSU,ExtremeXOS Edge license,connector for external power supply, PN:16506	ks			7
Summit X440-48p PWP TAC & OS Summit 16506 , PN: 97004-16506	ks			17
SummitStack/UniStack Stacking cable, 0.5M , PN:16106	ks			5
SummitStack/UniStack Stacking cable, 1.5M, PN:16607	ks			2
1000BASE-SX SFP, MMF 220 & 550 meters, LC connector, PN:10051H	ks			18
1000BASE-LX SFP, MMF 220 & 550 meters, SMF 10km, LC connector, PN:10052H	ks			6
Instalation & configuration services Extreme switches	človekodeň			8

WiFi:	0			0
Extreme networks AP3825I DUAL RADIO 11AC 3X3:3 MIMO INT ANT 2 EN, PN:WS-AP3825I	ks			8
Extreme networks AP3805I 11AC DUAL RADIO INT ANT, PN:WS-AP3805I	ks			8
Extreme networks controler V2110 V9 VIRT APPL ROW REGULATORY DOMAIN, PN:WS-V2110-9-ROW	ks			1
Extreme networks Identity and Access 1,000 end-system license, PN:IA-ES-1 K	ks			2
LICENSE, UPGRADE NMS-50 TO NMS-ADV-50, PN:NMS-50-A50-UG	ks			1
Extreme networks controler WS-C35 PWP NBD AHR 30135, PN:95604-30135	ks			1
Extreme networks controler V2110 V9 VIRT APPL ROW PWP Software Subscription, PN:95603-S20284	ks			1
Extreme networks NMS - 50 PWP Software Subscription, PN:95603-S20129	ks			1
Extreme networks NMS-50-A50-UG PWP Software Subscription, PN: 97003-S20134	ks			1
Extreme networks Identity and Access 1,000 PWP Software Subscription, PN:95603-S20098	ks			3
Instalation & configuration services WIFI	človekodeň			8
SLA	ks			1

Technické vlastnosti	Hodnota / charakteristika
Predmet obstarávania bude vyhovovať príslušným STN normám a hygienickým normám.	áno
Uchádzač predloží vyhlásenie o zhode dodávaných výrobkov.	áno
Technické vlastnosti bezdrôtový prístup	Hodnota / charakteristika
Bezdrôtový prístupový bod typ A – WS-AP3825I	• Vysokovýkonný prístupový bod pre vnútorné používanie
Bezdrôtový prístupový bod typ A – WS-AP3825I	• Určené pre nasadenie v oblastiach s vysokou hustotou prístupových klientov
Bezdrôtový prístupový bod typ A – WS-AP3825I	• Podpora noriem 802.11 a/b/g/n/ac
Bezdrôtový prístupový bod typ A – WS-AP3825I	• Verzia s možnosťou pripojenia vonkajších antén pomocou konektora RP-SMA
Bezdrôtový prístupový bod typ A – WS-AP3825I	• Súprava pre montáž na stenu
Bezdrôtový prístupový bod typ A – WS-AP3825I	Plne kompatibilný a integrovateľný s kontrolérom Extreme networks WS-C35
Výkonnostné parametre prístupový bod typ A	Výkonnostné parametre prístupový bod typ A
Parameter	Počet
Počet rádií	min. 2
MIMO	3x3:3 SS
Priepustnosť 2,4 GHz	40Mbps
Priepustnosť 5 GHz	1,2Gbps
Priepustnosť RFC2285	70 000 pps
Počet SSID na rádio	min. 5
Simultánne hlasové hovory	10 a viac
Počet asociovaných klientov na rádio	min. 100
Bezpečnostné štandardy	WPA, WPA2 (AES), 802.11i, 802.1x, IPSec, IKEv2, PKCS #10, X509 DER / PKCS #12
Vysielací výkon 2,4GHz	22 dBm
Vysielací výkon 5GHz	22 dBm
Zisk 2,4 GHz	3 dBi

Zisk 5 GHz	3 dBi
Počet 10/100/1000 Base-T rozhraní	min. 2
Režimy rozhraní	Active/Active, Active/Passive, LACP
Napájanie	PoE
Max odber	14 W
Váha	Max. 700 g
Bezdrôtová modulácia	802.11ac: BPSK, QPSK, 16QAM, 64QAM, 256QAM with OFDM
Bezdrôtová modulácia	802.11ac Packet aggregation: A-MPDU, A-MSDU
Bezdrôtová modulácia	802.11ac Very High-Throughput (VHT): VHT20/40/80
Bezdrôtová modulácia	802.11ac Advanced Features: LDPC, STBC, Maximum
Bezdrôtová modulácia	Likelihood (ML) Detection
Bezdrôtová modulácia	802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM
Bezdrôtová modulácia	802.11n High-throughput (HT) support: HT 20/40
Bezdrôtová modulácia	802.11n Packet aggregation: A-MPDU, A-MSDU
Bezdrôtová modulácia	802.11n Advanced Features: LDPC, STBC and TxBF
Bezdrôtová modulácia	802.11a: BPSK, QPSK, 16QAM, 64QAM with OFDM
Bezdrôtová modulácia	802.11g: DSSS and OFDM
Bezdrôtová modulácia	802.11b: DSSS
Technické vlastnosti bezdrôtový prístup	Hodnota / charakteristika
Bezdrôtový prístupový bod typ B – WS-3805I	• Vysokovýkonný prístupový bod pre vnútorné používanie
Bezdrôtový prístupový bod typ B – WS-3805I	• Podpora noriem 802.11 a/b/g/n/ac
Bezdrôtový prístupový bod typ B – WS-3805I	• Verzia s možnosťou pripojenia vonkajších antén pomocou konektora RP-SMA
Bezdrôtový prístupový bod typ A – WS-AP3825I	Súprava pre montáž na stenu
Bezdrôtový prístupový bod typ A – WS-AP3825I	Plne kompatibilný a integrovateľný s kontrolérom Extreme networks WS-C35
Výkonnostné parametre prístupový bod typ A	Výkonnostné parametre prístupový bod typ A
Parameter	Počet
Počet rádií	min. 2
MIMO	2x2:2 SS
Priepustnosť 2,4 GHz	300 Mbps
Priepustnosť 5 GHz	860 Gbps
Priepustnosť RFC2285	35 000 pps
Počet SSID na rádio	min. 5
Simultánne hlasové hovory	10 a viac
Počet asociovaných klientov na rádio	min. 100
Bezpečnostné štandardy	WPA, WPA2 (AES), 802.11i, 802.1x, IPSec, IKEv2, PKCS #10, X509 DER / PKCS #12
Vysielací výkon 2,4GHz	24 dBm
Vysielací výkon 5GHz	24 dBm
Zisk 2,4 GHz	3 dBi
Zisk 5 GHz	4,5 dBi
Bezdrôtová modulácia	802.11ac: BPSK, QPSK, 16QAM, 64QAM, 256QAM s OFDM

Bezdrôtová modulácia	802.11ac Packet aggregation: A-MPDU, A-MSDU
Bezdrôtová modulácia	802.11ac Very High-Throughput (VHT): VHT20/40/80
Bezdrôtová modulácia	802.11ac Advanced Features: LDPC, STBC, Maximum Likelihood (ML) Detection
Bezdrôtová modulácia	802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM
Bezdrôtová modulácia	802.11n High-throughput (HT) support: HT 20/40
Bezdrôtová modulácia	802.11n Packet aggregation: A-MPDU, A-MSDU
Bezdrôtová modulácia	802.11n Advanced Features: LDPC, STBC and TxBF
Bezdrôtová modulácia	802.11a: BPSK, QPSK, 16QAM, 64QAM with OFDM
Bezdrôtová modulácia	802.11g: DSSS and OFDM
Bezdrôtová modulácia	802.11b: DSSS
Počet 10/100/1000 Base-T rozhraní	min. 1
Napájanie	PoE
Max odber	10W
Váha	Max. 400 g
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Stavový firewall novej generácie (Next Generation Firewall).
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí byť v prevedení HW appliance
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí mať jednotný systém aplikácie záplat a aktualizácií (aktualizácie alebo fixy musia
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	pokrývať operačný systém aj firewall)
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Zariadenie musí vedieť identifikovať aplikáciu z obsahu dátového toku a nie len podľa použ. portu
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí umožniť tvorbu vlastných signatúr pre detekciu aplikácií
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí vedieť k IP adrese priradiť identitu užívateľa. Identitu užívateľa musí vedieť získať
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	z adresárových služieb (MS Active Directory, LDAP) z terminálových služieb (MS Terminal
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	Services, Citrix XenAPP), zo Syslog správ a cez API rozhranie
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Výrobca musí poskytovať neustálu aktualizáciu IPS signatúr,
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	signatúr pre ochranu pred škodlivým kódom a URL databázy
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí vedieť vykonať SSL/TLS dekrypciu šifrovanej prevádzky pre potreby jej analýzy.
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí umožniť prevádzku vo vysokej dostupnosti v režime Active-Standby a Active-Active
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí vedieť poskytovať QoS pre definovanú prevádzku, a to aj na základe aplikácie
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	a kategórie aplikácií, URL a URL kategórie, používateľa
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	Musí vedieť generovať informácie o dátových tokoch NetFlow v9/IPFIX
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Podpora statického smerovania a smerovacích protokolov RIP, OSPF, OSPF v3, BGP
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	a smerovania multicastov
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí umožniť vytváranie virtuálnych firewallov
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí umožniť definíciu bezpečnostných zón a ich používanie pri tvorbe bezpečnostných politík.
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí podporovať protokol IPv6 (NAT64, NPTv6, IPv6 over IPSec medzi IPv4 koncovými bodmi,

Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	IPv4 over IPSec medzi IPv6 koncovými bodmi, DHCPv6 Relay, SLAAC, NPTv6).
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Možnosť prevádzky DNS Proxy servera
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Podpora DHCP v režime Server alebo Relay. Pri funkcii DHCP servera musí umožňovať statické
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	prideľovanie IP adries zariadeniam
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí vedieť vytvárať IPSec VPN tunelov s podporou IKEv1 a IKEv2.
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	• Musí podporovať agregáciu rozhraní pomocou protokolu LACP.
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	Musí byť plne kompatibilné s existujúcim firewallom PA3020. Musí byť schopné vytvoriť cluster zapojenie s existujúcim firewallom PA3020 s jednotnou sadou bezpečnostných politík.
Centrálny Firewall-Všeobecné požiadavky - Palo Alto netwoks PA3020	Zmena politík na jednom zariadení sa musí automaticky aplikovať na clustrový box.
Tvorba bezpečnostných politík	• Musí umožniť tvorbu bezpečnostných politík na základe aplikácie alebo aplikačnej skupiny
Tvorba bezpečnostných politík	• Musí umožniť tvorbu bezpečnostných politík na základe užívateľskej identity a príslušnosti
Tvorba bezpečnostných politík	užívateľa v užívateľskej skupine.
Tvorba bezpečnostných politík	• Musí podporovať sandboxovú analýzu neznámych hrozieb.
Tvorba bezpečnostných politík	• Musí vedieť poskytovať IPS ochranu založenej na štatistickej analýze, heuristickej analýze,
Tvorba bezpečnostných politík	analýze protokolu, pasívneho DNS monitoringu a vlastnej signatúry.
Tvorba bezpečnostných politík	• Musí vedieť detegovať a blokovať škodlivý kód ako sú počítačové vírusy, spywary, botnety,
Tvorba bezpečnostných politík	počítačové červy a trojské kone.
Tvorba bezpečnostných politík	• Musí vedieť kontrolovať webovskú prevádzku na základe URL kontroly. URL kontrolu musí
Tvorba bezpečnostných politík	vedieť vykonávať voči lokálnej databáze ale aj voči databáze uloženej v cloude.
Tvorba bezpečnostných politík	• Musí podporovať definovanie bezpečnostnej politiky na kontrolu webovej prevádzky
Tvorba bezpečnostných politík	na základe samostatnej URL a kategórie URL
Tvorba bezpečnostných politík	• Musí umožňovať vytváranie vlastnej kategorizácie webových stránok.
Tvorba bezpečnostných politík	• Musí umožniť aplikovanie bezpečnostných politík na smerované/prekladané (L3) a aj
Tvorba bezpečnostných politík	transparentné (L2) dátové toky a to pre IPv4 ako aj pre IPv6.
Tvorba bezpečnostných politík	• Musí umožniť vytváranie bezpečnostných politík na základe času a denného obdobia.
Tvorba bezpečnostných politík	• Musí umožniť vytváranie bezpečnostných politík pozostávajúcich z objektov
Tvorba bezpečnostných politík	• Musí byť schopné vykonať validáciu bezpečnostnej politiky pred jej aplikáciou do prevádzky.
Tvorba bezpečnostných politík	• Musí byť schopné porovnať aktuálnu konfiguráciu voči niektorej známej z minulosti
Správa zariadenia	• Oddelené CPU pre správu zariadenia a pre poskytovanie firewallových služieb
Správa zariadenia	• Samostatné Ethernetové rozhranie pre Out-of -Band správu zariadenia
Správa zariadenia	• Správa zariadenia pomocou webového grafického používateľského rozhrania (GUI) a cez
Správa zariadenia	príkazový riadok protokolom SSHv2. SSH prístup musí vedieť umožniť aj pomocou verejného
Správa zariadenia	kľúča. GUI prístup musí vedieť umožniť aj pomocou osobného certifikátu.

Správa zariadenia	• Musí umožniť definovanie administrátorských rolí a prístup ad. umož.podľa ich zaradenia k rolám
Správa zariadenia	• Musí umožňovať v rámci definície role sprístupniť alebo zakázať CLI
Správa zariadenia	• Musí umožniť tvorbu administrátorských kont lokálne. Administrátorské prístupy musí vedieť
Správa zariadenia	overiť aj pomocou RADIUS protokolu a z LDAP databázy
Správa zariadenia	• Musí vedieť zaslať udalosti o stave zariadenia a o stave bezpečnostných politík pomocou
Správa zariadenia	protokolov Syslog, SNMP a SNTP.
Správa zariadenia	• Musí umožňovať zaznamenávanie všetkých administrátorských zásahov pre potreby auditu.
Integrácia	• Zariadenie musí byť zintegrované so všetkými (pevné aj bezdrôtové) dodávanými sieťovými prvkami
Integrácia	(pevné aj bezdrôtové, prepínače extreme networks, Extreme networks NMS, Extreme networks Identity and Access).
Integrácia	• Zariadenie musí umožňovať autentifikovať používateľov prostred. Radius, Ldap a Kerberos protokolu
Integrácia	Inštalácia dodaného zariadenia v mieste sídla obstarávateľa. Jeho pripojenie do siete, komplexná konfigurácia zariadenia
Integrácia	ako slave zariadenia k existujúcemu primárnemu FW PA3020.
Bezpečnostný monitoring	• Zariadenie musí byť schopné vytvárať štatistické reporty z prevádzky podľa rôznych kritérií
Bezpečnostný monitoring	ako napr najnavšt.stránky, aplikácie, objem dát podľa používateľov, IP adries, geolokácie a pod
Bezpečnostný monitoring	• Musí obsahovať reporting o zachytených hrozbách, podľa používateľov, spojení, zdrojov a pod
Bezpečnostný monitoring	• Musí obsahovať sadu preddefinovaných reportov a taktiež možnosť vytvárať vlastné reporty
Bezpečnostný monitoring	• Musí byť schopné zobraziť trendy vývoja hrozieb, vyťaženia a pod
Bezpečnostný monitoring	• Musí obsahovať analýzu podozrivej komunikácie hostov v sieti pre detekovanie komunikácie
IBezpečnostný monitoring	na známe C&C server
Bezpečnostný monitoring	• Musí obsahovať korelačný engine generujúci udalosti koreláciou viacerých elementárnych
Bezpečnostný monitoring	udalostí zachytených firewallom
Bezpečnostný monitoring	• Výsledok sandbox analýzy musí byť dostupný z content logu a naopak, aby bolo možné
Bezpečnostný monitoring	identifikovať priamo používateľa alebo PC na ktoré bol stiahnutý alebo zaslaný škodlivý kód
Výkonnostné parametre Centrálny Firewall	Výkonnostné parametre Centrálny Firewall
Parameter	Počet
Počet interfejsov 10/100/1000 RJ45	Min 12
Počet optických (SFP) interfejsov	Min 8
Počet VLANs	Min 4096
Počet logických interfejsov (L2, L3, tunnel)	Min 1000
FW priepustnosť	Min 2Gbps
IPS+AV priepustnosť	Min 2Gbps
VPN priepustnosť	Min 500Mbit
Počet nových spojení /s	Min 50 000
Počet konkurentných spojení	Min 250 000
Počet VPN tunnelov	Min 500

Možnosť pridať virtuálne systémy	Min 5
Počet bezpečnostných pravidiel	Min 2500
Počet NAT pravidiel	Min 2500
Počet bezpečnostných profilov	Min 150
Počet aplikačných profilov	Min 250
Počet QoS tried	Min 8
Počet súčasne používaných syslog serverov	Min 4
Technické vlastnosti IPSEC & SSL VPN conection	Hodnota / charakteristika
IPSEC & VPN conection-Všeobecné požiadavky – FortiGate 100D	1 ročná hardvérová podpora od výrobcu Fortinet pre zariadenia FortiGate 100D. Úroveň podpory 24x7 Comprehensive FortiCare.
IPSEC & VPN conection-Všeobecné požiadavky – FortiGate 100D	Pre túto podporu nie je možná alternatíva. Obstarávateľ požaduje dodanie HW podpory pre už implementované zariadenia.
IPSEC & VPN conection - Všeobecné požiadavky – FortiGate 30D	1 ročná hardvérová podpora od výrobcu Fortinet pre zariadenia FortiGate 30D. Úroveň podpory 8x5 Enhanced FortiCare.
IPSEC & VPN conection - Všeobecné požiadavky – FortiGate 30D	Pre túto podporu nie je možná alternatíva. Obstarávateľ požaduje dodanie HW podpory pre už implementované zariadenia.
PTechnické vlastnosti Email filtering	Hodnota / charakteristika
Email filtering - Všeobecné požiadavky – FortiMail VM02	1 ročná hardvérová a softvérová podpora od výrobcu Fortinet pre zariadenia Fortimail VM02. Úroveň podpory 8x5 FortiCare plus FortiGuard Bundle Contract.
Email filtering - Všeobecné požiadavky – FortiMail VM02	Súčasťou podpory je Hardware Replacement, Firmware and General Upgrades, 8x5 Enhanced Support, Anti-Virus, Anti-Spam.
Email filtering - Všeobecné požiadavky – FortiMail VM02	Pre túto podporu nie je možná alternatíva. Obstarávateľ požaduje dodanie HW podpory pre už implementované zariadenia.
Technické vlastnosti prepínače	Hodnota / charakteristika
Pevný prístup - Všeobecné požiadavky	Dodávka stacking káblov kompatibilných pre 40Gbps stakovanie prepínačov Summit X460, Summit X440 48t, Summit X440 48p. Dlzka kábla 1,5m.
Pevný prístup - Všeobecné požiadavky	Dodávka stacking káblov kompatibilných pre 40Gbps stakovanie prepínačov Summit X460, Summit X440 48t, Summit X440 48p. Dlzka kábla 0,5m.
Pevný prístup - Všeobecné požiadavky	Dodávka SFP 1 Gbps modulov, 1000BASE-SX SFP, MMF 220 & 550 meters, LC connector kompatibilných s prepínačmi Summit X460, Summit X440 48t, Summit X440 48p
Pevný prístup - Všeobecné požiadavky	Dodávka SFP 1 Gbps modulov, 1000BASE-SX SFP, MMF 220 & 550 meters, LC connector dosah 10km, kompatibilných s prepínačmi Summit X460, Summit X440 48t, Summit X440 48p
Pevný prístup - Všeobecné požiadavky -prepínač X460-G2	Doplnenie Fan modulov do existujúcich prepínačov Extreme networks Summit X460-G2 48. FAN moduly musia podporovať inštaláciu do Extreme networks Summit X460-G2 pričom nesmie byť obmedzená alebo
Pevný prístup - Všeobecné požiadavky -prepínač X460-G2	alebo znížená záruka a podpora výrobcu na zariadenie Extreme networks Summit X460-G2. FAN moduly musia byť dodaná vrátane 1 ročnej HW záruky.
Pevný prístup - Všeobecné požiadavky -prepínač X460-G2	Doplnenie 300W AC napájacích zdrojov do existujúcich prepínačov Extreme networks Summit X460-G2 48. Napájacie zdroje musia podporovať inštaláciu do Extreme networks Summit X460-G2
Pevný prístup - Všeobecné požiadavky -prepínač X460-G2	(inštalácia priamo do pozícii v prepínačoch) pričom nesmie byť obmedzená alebo znížšná záruka a podpora výrobcu na zariadenie Extreme networks Summit X460-G2. Napájacie zdroje musia byť dodané
Pevný prístup - Všeobecné požiadavky -prepínač X460-G2	vrátane 1 ročnej HW záruky.

Pevný prístup - Všeobecné požiadavky -prepínač X460-G2	1 ročná hardvérová podpora od výrobcu Extreme Networks pre zariadenia Summit X460-G2 48port. Úroveň podporyPWP TAC & OS Summit 16702.
Pevný prístup - Všeobecné požiadavky -prepínač X460-G2	Pre túto podporu nie je možná alternatíva. Obstarávateľ požaduje dodanie HW podpory pre už implementované zariadenia.
Pevný prístup - Všeobecné požiadavky -prepínač Summit X440-48t	1 ročná hardvérová podpora od výrobcu Extreme Networks pre zariadenia 'Summit X440-48t ' 48x 10/100/1000BASE-.
Pevný prístup - Všeobecné požiadavky -prepínač Summit X440-48t	Úroveň podpory PWP TAC & OS Summit 16505. Pre túto podporu nie je možná alternatíva. Obstarávateľ požaduje dodanie HW podpory pre už implementované zariadenia.
Pevný prístup - Všeobecné požiadavky - Prepínač A	Spravovanie zariadení pomocou konzoly, SSHv2, Telnet, HTTP/HTTPS, SNMP v1, v2c v3
Pevný prístup - Všeobecné požiadavky - Prepínač A	Možnosť definovania komplexnosti hesla pre lokálnych administrátorov
Pevný prístup - Všeobecné požiadavky - Prepínač A	Musia mať vyčlenený port pre Out of Band manažment
Pevný prístup - Všeobecné požiadavky - Prepínač A	Možnosť vytvárania niekoľkých virtuálnych smerovačov
Pevný prístup - Všeobecné požiadavky - Prepínač A	Všetky dodané prepínače musia byť spolu integrovateľné do rovnakého stohu. Prepínače musia byť integrovateľné do stohu cez 40GB stohovacie porty s už existujúcimi prepínačmi summit X460,
Pevný prístup - Všeobecné požiadavky - Prepínač A	Summit X440 48t.
Pevný prístup - Všeobecné požiadavky - Prepínač A	Podpora odzrkadlenia prevádzky na monitorovací port
Pevný prístup - Všeobecné požiadavky - Prepínač A	Podpora protokolov IPv4 a IPv6
Pevný prístup - Všeobecné požiadavky - Prepínač A	Podpora min. 4095 Vlanov
Pevný prístup - Všeobecné požiadavky - Prepínač A	Podpora Jumbo Frame 9216 Byte
Pevný prístup - Všeobecné požiadavky - Prepínač A	Podpora štandardu RFC 3619 – EAPS
Pevný prístup - Všeobecné požiadavky - Prepínač A	Podpora štandardu IEEE 802.1ab – LLDP
Pevný prístup - Všeobecné požiadavky - Prepínač A	Podpora štandardu IEEE 802.3ad – LACP
Pevný prístup - Všeobecné požiadavky - Prepínač A	Podpora protokolu 802.1x s možnosťou autentizácie viacerých užívateľov na jednom porte
Pevný prístup - Všeobecné požiadavky - Prepínač A	Možnosť vytvorenia agregovanej linky cez niekoľko zariadení, ktoré nie sú zapojené do rovnakého stohu
Pevný prístup - Všeobecné požiadavky - Prepínač A	Operačný systém všetkých zariadení musí používať rovnaký binárny súbor a musí byť kompatibilný s prepínačmi Summit X460, Summit X440
Pevný prístup - Všeobecné požiadavky - Prepínač A	Operačný systém zariadení musí byť rozšíriteľný pomocou modulov bez nutnosti reštartovania zariadenia.
Pevný prístup - Všeobecné požiadavky - Prepínač A	Operačný systém zariadení musí vedieť spúšťať lokálne scripty
Pevný prístup - Všeobecné požiadavky - Prepínač A	Používanie ACL nemôže zaťažiť sprocesovanie dátových tokov
Pevný prístup - Všeobecné požiadavky - Prepínač A	Zariadenia musia vedieť chrániť sieť na základe analýzy prevádzky – DoS (Ping of Death, Ping Sweep, Ping Flood, Port Sweep, TCP Flood, atď.) ,
Pevný prístup - Všeobecné požiadavky - Prepínač A	Flood útoky na porty (prihlasovacie služby, RPC, NFS, File Sharing, X Windows, Name služby, Mailové služby, Webové služby, atď.)
Pevný prístup - Všeobecné požiadavky - Prepínač A	Zariadenia musia vedieť naštartovať z viacerých binárnych súborov uložených lokálne.
Pevný prístup - Všeobecné požiadavky - Prepínač A	Zariadenia musia vedieť načítať si konfiguráciu z viacerých lokálne uložených konfiguračných súborov
Pevný prístup - Všeobecné požiadavky - Prepínač typ A X440-48p	Prepínač poskytujúce napájanie koncových zariadení podľa štandardov 802.3af (PoE) a 802.3at (PoE+)
Pevný prístup - Všeobecné požiadavky - Prepínač typ A X440-48p	Prepínač s plnou podporou stohovania s prepínačmi Summit X460, Summit X440 48t, Summit X440 48P
Pevný prístup - Všeobecné požiadavky - Prepínač typ A X440-48p	Podpora externej napájacej jednotky

Pevný prístup - Všeobecné požiadavky – Integrácia	Demontáž starých prepínačov. Inštalácia dodaných zariadení v mieste sídla obstarávateľa. Pripojenie prepínačov do siete, ich zostohovanie, upgrade na aktuálnu verziu firmware.
Pevný prístup - Všeobecné požiadavky – Integrácia	Konfigurácia Vlan, 802.1x a všetkých nastavení podľa súčasnej konfigurácie obstarávateľa.
Výkonnostné parametre Prepínač typ A:	Výkonnostné parametre Prepínač typ A:
Parameter	Počet
Počet 10/100/100BASE-T portov	Min 48
Z toho Combo portov	Min 4
Počet 100/1000BASE-X portv (SFP)	Min 4
Stohovacie porty	Min. 2
Agregované prepínacie pásmo	Min 120Gbps
Forwading Rate	Min 90 Mbps
Počet MAC adries	Min 10k
Oneskorenie (64-byte)	<6 micros
Výška	1RU
Maximálna hĺbka	30 cm
Maximálna spotreba	650W
Minimálny PoE rozpočet	350W
Technické vlastnosti riadenie prístupu k sieti	Technické vlastnosti riadenie prístupu k sieti
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Certifikácia Wi-Fi CERTIFIED, Súlad s lokálnymi štandardmi pre bezdrôtovú komunikáciu
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora IEEE Standard 802.11h – DFS2
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora súčasného, dual-band prístupu technológií 802.1 a/n/ac (5GHz) a 802.1 b/g/n (2m4 GHz)
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Plug and Play inštalácia prístupových bodov
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Bezpečná vzdialené správa pomocou protokolov HTTPS a SSH
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Centrálna konfigurácia a aktualizácia SW vybavenia
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Autentizačné a šifrovacie štandardy WEP, WPA (TKIP), WPA2 (AES), 802.1x, 802.11i
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Automatický výber kanálu a vysielacieho výkonu podľa stavu RF priestoru a vyťaženia kanálu
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Riadenie vysielacieho výkonu po 12 a viac úrovniach
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Možnosť automatického presmerovania klienta medzi rádiami – band steering
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Automatická redistribúcia klientov medzi prístupovými bodmi podľa vyťaženia prístupového bodu
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora rýchleho a bezpečného roamingu (pre authentication, OKC)
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Terminovanie klientskej prevádzky pri prístupovom bode, pri radiči (L2) alebo na radiči (L3)
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Distribuovaný RF manažment medzi prístupovými bodmi aj v prípade výpadku radiča
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora Air Time Fairness pre rôzne typy prístupových zariadení
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora hlasových, videových a dátových aplikácií na rovnakom SSID
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Prioritizovanie hlasových tokov pred dátovými pri označených aj neoznačených tokoch
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora IEEE 802.11e, vrátane WMM, TSPEC a U-APSD

Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	V prípade výpadku radiča, prístupové body musia vedieť naďalej pracovať samostatne – terminovanie klientskej prevádzky pri prístupovom bode,
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	šifrovanie, BlackList, L3 a L4 filtrovanie, asymetrický rate limit, QoS, RF manažment pre lokálne prepínanú prevádzku
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora QoS (DiffServ, IP ToS, IP Precedence) pri pevnom a aj bezdrôtovom prístupe
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Možnosť priradenia rôznych prístupových a bezpečnostných profilov (ACL, QoS, Rate Limit, atď.) na klienta bez nutnosti používania inej SSID
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Možnosť konverzie multicastov do unicastov
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora multicastov Bonjour/LLMNR/UPnP – identifikácia, obmedzenie, riadenie
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora 8 SSID na rádio
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora dynamickej autorizácie – RFC 3576, podpora RADIUS AAA
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Podpora WDS s možnosťou vyčlenenia rádia pre chrbticový spoj a aj s možnosťou používania rovnakého rádia pre chrbticový spoj a aj pre klientsku prevádzku
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Možnosť používania interného aj externého Captive Portalu pre autentizáciu klientov
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Možnosť editácie interného Captive Portálu
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Možnosť definície lokálnych účtov pre návštevy bez podpory IT personálu
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Softvérový radič kompatibilný s platformov VmWare, s plnou integrovateľnosťou zapojenia vo vysokej dostupnosti s hardvérovým radičom ,
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	pričom primárny radič je hardvérové zariadenie Extreme networks WS-C35. Sekundárny kontrolér musí automaticky prevziat kompletnú funkčnosť v prípade výpadku primárneho kontróleru Extreme WS - C35.
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	API pre location-based aplikácie tretích strán
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Rozšírenie licencií existujúceho NAC na 3000. Súčasné implementované riešenie pokrýva 1000licencií. Požadované rozšírenie o 2000 licencií.
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	Rozšírenie existujúcej licencie NMS-50 na NMS-50-A50.
Bezdrôtový prístup – kontroler Extreme networks WS-V2110-9-ROW	1 ročná podpora od výrobcu pre kontroler Extreme networks WS-V2110-9-ROW.
Bezdrôtový prístup - Všeobecné požiadavky – Integrácia	Inštalácia WS-V2110 v sídle obstarávateľa. Integrácia do existujúcej infraštruktúry a nakonfigurovanie zariadenia podľa súčasnej konfigurácie obstarávateľa.
Bezdrôtový prístup - Všeobecné požiadavky – Integrácia	Plná konfigurácia zariadenia ako slave zariadenia k WS - C35
Bezdrôtový prístup - Všeobecné požiadavky – Integrácia	Inštalácia dodaných AP v sídle obstarávateľa. Integrácia do existujúcej infraštruktúry a nakonfigurovanie zariadenia podľa súčasnej konfigurácie obstarávateľa.
1 Year solution services - Všeobecné požiadavky	zabezpečenie prevádzky a funkčnosti systému v sídle obstarávateľa, pravidelná denná kontrola a rutinná administrácia systémových nastavení, riešenie kolíznych stavov
1 Year solution services - Všeobecné požiadavky	pravidelné aktualizácie zariadení, aktualizácie threat a URL filtering signatúr, oprava, výmeny chybného HW, zmena konfigurácii podľa požiadaviek na zmenu, diagnostika chybových stavov
1 Year solution services - Všeobecné požiadavky	odborné technické konzultačné činnosti pri zmenových konaniach (nové požiadavky na funkčnosť, zmeny existujúcich riešení, nové projekty, konzultačné činnosti v oblasti informačnej , personálnej,
1 Year solution services - Všeobecné požiadavky	sieťovej a fyzickej bezpečnosti

1 Year solution services - Všeobecné požiadavky	monitoring funkčnosti LAN, pravidelná denná kontrola a rutinná administrácia systémových nastavení, podpora pri riešení bezpečnostných incidentov, j) vzdialená podpora a údržba systému
1 Year solution services - Všeobecné požiadavky	rýchle riešenie bezpečnostných incidentov a odstránenie chýb (L2 support) a spolupráca s výrobcom pri riešení problémových stavov, zber a pravidelné vyhodnocovanie logov,
1 Year solution services - Všeobecné požiadavky	celkový minimálny rozsah služieb v rámci 1 Year solution services je 144 človekodní (mandays)
Bezdrôtový prístup – kontroler Extreme networks WS-35	1 ročná hardvérova a softvérová podpora od výrobcu pre kontroler Extreme networks WS-35.
Bezdrôtový prístup – kontroler Extreme networks WS-35	Pre túto podporu nie je možná alternatíva. Obstarávateľ požaduje dodanie HW podpory pre už implementované zariadenia.
Bezdrôtový prístup – kontroler Extreme networks NMS 50	1 ročná WP Software Subscription NAC s 1000 licenciami n. Pre túto podporu nie je možná alternatíva. Obstarávateľ požaduje dodanie HW podpory pre už implementované zariadenia.
Bezdrôtový prístup – kontroler Extreme networks NMS-50-A50-UG	1 ročná PWP Software Subscription podpora od výrobcu pre NMS-50-A50-UG.
Bezdrôtový prístup – kontroler Extreme networks NMS-50-A50-UG	1 ročná PWP Software Subscription podpora od výrobcu pre Extreme networks Identity and Access pre 3000 licencií.

2.4 Osobitné požiadavky na plnenie:

Názov
V cene je dovoz, rozbalenie, inštalácia dodávaného tovaru na pracoviska podľa požiadaviek verejného obstarávateľa.
Verejný obstarávateľ si vyhradil právo na poskytnutie bezplatnej vzorky Plnenia predmetu zákazky, resp. do 48 hodín dodať popis a technickú špecifikáciu obstarávaných zariadení v zákazke z dôvodu odkontrolovania požadovaných parametrov zariadení.
Záručná doba 12 mesiacov v mieste inštalácie s odozvou nasledujúci pracovný deň.
Nedodržanie uvedených osobitných požiadaviek na plnenie bude objednávateľ považovať za závažné porušenie zmluvných podmienok zákazky.
Pokuta za nedodržanie uvedených osobitných požiadaviek na plnenie, nedodanie tovaru podľa popisu, špecifikácií a termínoch dodania v objednávkovom formulári je 10% z predpokladanej hodnoty zákazky na účet verejného obstarávateľa do 10 pracovných dní.
Uchádzač predloží do 48 hodín od uzavretia zmluvy úplnú špecifikáciu a cenovú kalkuláciu jednotlivých položiek predmetu zákazky v členení: jednotková cena položky bez DPH, cena za jednotlivé položky spolu (bez DPH, výška DPH, spolu s DPH).
Uchádzač predloží do 48 hodín od uzavretia zmluvy vyhlásenia o zhode a doplňujúce podklady k nim, resp. certifikáty vydané autorizovanými osobami alebo notifikovanými osobami pre všetky položky predmetu zákazky.
Uchádzač dodá predmet zákazky, ktorý je certifikovaný a schválený na dovoz a predaj v Slovenskej republike, resp. v rámci Európskej únie a bude vyhovovať platným medzinárodným normám, STN a všeobecne záväzným právnym predpisom.
Splatnosť faktúr 30 dní.
Objednávateľ je oprávnený pri dodávke skontrolovať predmet zákazky a v prípade dodávky iného tovaru tento tovar neprevziať.
Víťazný uchádzač predloží do 24 hodín od uzavretia zmluvy: certifikáty min. 3 expertov pre správu FW - Certified Network Security Engineer CNSE 5.1, prípadne rovnocenný ekvivalent tohto certifikátu.
Víťazný uchádzač predloží do 24 hodín od uzavretia zmluvy: certifikáty min. 3 expertov pre správu FW - Certified Network Security, Professional pre FortiOS v.5, prípadne rovnocenný ekvivalent tohto certifikátu.
Víťazný uchádzač predloží do 24 hodín od uzavretia zmluvy: certifikáty min. 2 expertov pre správu Extreme prepínačov - Extreme Networks Switching & Routing - XOS Specialist, prípadne rovnocenný ekvivalent tohto certifikátu.
Víťazný uchádzač predloží do 24 hodín od uzavretia zmluvy: certifikáty min. 1 experta pre informačnú bezpečnosť - platný doklad odbornej a technickej spôsobilosti v oblasti zabezpečenia siete, identifikácie zraniteľností v sieti analýzy škodlivého kódu platný certifikát CISM prípadne ekvivalent tohto certifikátu.
Maximálna lehota dodania predmetu zákazky je 14 pracovných dní odo dňa nadobudnutia účinnosti zmluvy.
Úspešný uchádzač je zodpovedný v plnom rozsahu za akúkoľvek škodu vrátane skutočnej škody, ušlého zisku a iných priamo alebo nepriamo súvisiacich škôd, ktorá vznikne v dôsledku porušenia akýchkoľvek jeho záväzkov zo Zmluvy, právnych predpisov alebo iných pravidiel, ktoré sú pre neho záväzné.
Nedodržanie uvedených osobitných požiadaviek na plnenie bude objednávateľ považovať za závažné porušenie zmluvných podmienok zákazky. Nedodržaním uvedených osobitných požiadaviek na plnenie objednávateľ zákazku neprijme a odstúpi od zmluvy.

Verejný obstarávateľ požaduje bez vyzvania do 24 hodín od uzavretia zmluvy a od doručenia oznámenia z EKS predložiťod víťazného uchádzača zápis v Registri konečných užívateľov výhod podľa platného právneho poriadku.	
Názov	**Upresnenie**

2.5 Prílohy opisného formulára Zmluvy:

Popis	**Názov súboru**

III. Zmluvné podmienky

3.1 Miesto plnenia Zmluvy:

Štát:	Slovenská republika
Kraj:	Bratislavský
Okres:	Bratislava I
Obec:	Bratislava - mestská časť Staré Mesto
Ulica a číslo:	

3.2 Čas / lehota plnenia zmluvy:

22.3.2016 9:00:00 - 5.4.2016 15:00:00

3.3 Dodávané množstvo/ rozsah zmluvného plnenia:

Jednotka:	ks
Požadované množstvo:	1,0000

3.4 Práva a povinnosti zmluvných strán podľa tejto Zmluvy sa spravujú Obchodnými podmienkami elektronického trhoviska verzia 2.1, účinná zo dňa 1.12.2015 , ktoré tvoria neoddeliteľnú prílohu tejto Zmluvy.

IV. Zmluvná cena

4.1 Celková cena predmetu Zmluvy bez DPH: 204 549,92 EUR

4.2 Sadzba DPH: 20,00

4.3 Celková cena predmetu Zmluvy vrátane DPH: 245 459,90 EUR

V. Záverečné ustanovenia

5.1 Táto Zmluva bola uzavretá automatizovaným spôsobom v rámci Elektronického kontraktačného systému a v zmysle Obchodných podmienok elektronického trhoviska verzia 2.1, účinná zo dňa 1.12.2015, ktoré tvoria jej prílohu č. 1.

5.2 Táto Zmluva nadobúda platnosť dňom jej uzavretia a účinnosť za podmienok definovaných v Obchodných podmienkach elektronického trhoviska uvedených v bode 5.1 tejto zmluvy.

5.3 Táto Zmluva vrátane jej príloh predstavuje úplnú dohodu zmluvných strán o jej predmete. Vedľajšie dohody k tejto zmluve neexistujú.

5.4 Táto Zmluva je vyhotovená v elektronickej podobe v štyroch vyhotoveniach, po jednom pre každú zmluvnú stranu, jedno vyhotovenie bude zaslané na zverejnenie v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky a jedno bude zverejnené v Centrálnom registri zmlúv trhoviska.

5.5 Túto Zmluvu bude možné meniť a dopĺňať za podmienok stanovených príslušnými všeobecne záväznými právnymi predpismi len vo forme písomného a číslovaného dodatku podpísaného oboma zmluvnými stranami.

5.6 Táto Zmluva má nasledovné prílohy:

Príloha č.1 Obchodné podmienky elektronického trhoviska verzia 2.1, účinná zo dňa 1.12.2015, https://portal.eks.sk/SpravaOpet/Opet/VerejnyDetail/

V Bratislave, dňa 10.3.2016 16:00:01

Objednávateľ:
Hlavné mesto Slovenskej republiky Bratislava
konajúci prostredníctvom osoby poverenej zastupovať Objednávateľa v rámci elektronického trhoviska

Dodávateľ:
TooNet, s.r.o.
konajúci prostredníctvom osoby poverenej zastupovať Dodávateľa v rámci elektronického trhoviska