Príloha č. 2 - Podrobný popis riešenia

1. **Miesta koncových bodov pre poskytovanie služieb, spôsob a kapacita pripojenia**
   Koncové body VPN ÚDZS budú rozdelené do dvoch typov v závislosti od požadovaných parametrov na výkonnosť uzla a kapacitu pripojenia do VPN siete.
   Typ 1 – centrála a datacentrum
   Typ 2 – pobočky a Súdnolekárske a patologicko-anatomické pracoviská (ďalej len „SLaPA“)

2. **Spôsob a kapacita pripojenia koncových bodov VPN siete**
   VPN sieť bude vybudovaná na úrovni MPLS a pobočky budú komunikovať navzájom. Primárne pripojenia jednotlivých lokalít bude realizované buď:
   • prostredníctvom optickej prípojky
   • prostredníctvom metalického prenosového média
   • prostredníctvom rádiového pripojenia v licencovanom pásme

   Záložné pripojenie jednotlivých lokalít bude realizované geograficky nezávislou trasou a bude ukončené na inom fyzickom sieťovom prvku poskytovateľa. Záložné pripojenia budú realizované buď:
   • prostredníctvom optického prenosového média
   • prostredníctvom metalického prenosového média
   • prostredníctvom rádiového pripojenia v licencovanom pásme
   • prostredníctvom asymetrickým pripojením aDSL

   2.1 Koncový bod Typ 1 (centrála, datacentrum, MPLS a internet)
   Primárne pripojenie koncového bodu Typ 1 bude realizované cez optické prenosové médium (optický kábel). Prístupová kapacita primárneho pripojenia bude symetrická s minimálnou požadovanou kapacitou uvedenou v Tabuľke č. 1. Záložné pripojenie koncového bodu Typ 1 bude zrealizované prostredníctvom nezávislej fyzickej trasy iného optického prenosového média alebo rádiového pripojenia typu bod-bod v licencovanom pásme. Prístupová kapacita záložného pripojenia bude symetrická s minimálnou požadovanou kapacitou uvedenou v Tabuľke č. 1. Pripojenie koncového bodu Typ 1 bude realizované zdvojenými aktívnymi sieťovými prvkami v režime vysokej dostupnosti (high availability). Centrálne prepínače pre IKT zariadenia budú mať SFP prístupové a uplink porty, počty ktorých sú uvedené v Tabuľke č. 2, disponujúce s možnosťou doplniť network moduly s 10GE podporou a budú mať natívnu funkcionalitu stacku.

   2.2 Koncový bod Typ 2 (pobočky a pracoviská SLaPA)
   Primárne pripojenie koncového bodu Typ 2 bude realizované cez optické prenosové médium (optický kábel) alebo rádiové pripojenie typu bod-bod/bod-multibod. Prístupová kapacita primárneho pripojenia bude symetrická s minimálnou požadovanou kapacitou uvedenou v Tabuľke č. 1. Súčasťou služby pre koncový bod Typ 2 bude dodanie a správa koncových CPE zariadení – prepínačov pre zabezpečenie pripojenia koncových zariadení (počítače, notebooky, tlačiarne a pod) do LAN infraštruktúry. Prepínače pre koncové zariadenia budú mať PoE funkcionalitu, 10/100/1000Base-T porty,s SFP uplink portami s počtom uvedenom v Tabuľke č. 2. Súčasťou dodávky bude zálohový napájací zdroj UPS, ktorý zabezpečí napájanie sieťových prvkov v prípade výpadku elektrickej energie.

   2.3 Prístup do siete internet
   Pripojenie MPLS VPN siete do siete internet bude zabezpečené z lokality Želllova 2, Bratislava. Prístup do siete internet bude zabezpečený dvojúrovňovou ochranou (IPS a UTM ako samostatné služby). Obstarávateľovi bude pridelených minimálne 20 pevných verejných IP adries. Z dôvodu bezpečnosti bude vytvorených minimálne 4 DMZ zón.

2.4 L2 prepojenie centrály a datacentra

L2 prepojenie LAN sietí verejného obstarávateľa na úrovni 100Mbit/s bude zabezpečené medzi lokalitami Žellova 2, Bratislava a Ipeľská 1, Košice. Prepojenie bude ukončené na 10/100/1000Base-T rozhraní.

3. Druh poskytovanej služby

Poskytované služby budú spĺňať nasledujúce požiadavky:

3.1 Umožňujú obojsmernú dátovú komunikáciu založenú na protokole IP medzi všetkými koncovými bodmi v sieťovej topológií typu každý s každým (any-to-any) s možnosťou nastavenia ľubovoľných obmedzení v smerovaní paketov podľa požiadaviek ÚDZS

3.2 Služba poskytuje virtuálnu privátnu sieť na prepojenie LAN sietí ÚDZS. VPN bude postavená na báze technológie IP MPLS.

3.3 Transport dát bude zabezpečený v minimálne dvoch kvalitatívnych triedach (mission critical data a best effort traffic) pričom priradenie jednotlivých zdrojov dát (aplikácií) do týchto tried bude realizované na základe požiadaviek ÚDZS

3.4 Hlavná chrbticová sieť Slovanetu je postavená v topológii dvojitého národného ringu medzi krajskými mestami s kapacitou n x 10Gbit, čím je zabezpečená vysoká dostupnosť a flexibilita siete. Okresné mestá tvoria regionálnu úroveň siete Slovanet, uzly regionálnej úrovne sú pripojené do jednotlivých miest v rámci národnej úrovne s kapacitou až n x1 Gbit/s. Všetky uzly siete Slovanet sú zálohované voči výpadku el. energie samostatnými zdrojmi UPS. IP/MPLS sieť Slovanet je hardvérovo postavená výlučne na smerovačoch a prepínačoch spoločnosti Cisco. MPLS VPN sieť bude obstarávateľovi umožňovať prenos informácií cez sieťovú infraštruktúru poskytovateľa služieb (Slovanet) spôsobom, ktorý podstatne zvyšuje mieru bezpečnosti a spoľahlivosti prenosu. Bude poskytovať kvalitatívne garancie pomocou definovania kvalitatívnych parametrov QoS. Prostredníctvom adresácie a manažmentu MPLS technológie a technológie BGP bude vytvorená oddelená privátna sieť s routovacou tabuľkou určenou výhradne pre obstarávateľa, do ktorej bude mať prístup iba definovaná skupina užívateľov. Takáto konfigurácia MPLS VPN zabezpečí, že celá sieťová prevádzka bude súčasťou iba obstarávateľovej VPN siete. Technológia IP/MPLS umožní uspokojiť odlišné nároky rozličných aplikácií používaných v sieti obstarávateľa.

3.5 Správa koncových CPE (v úlohe CPE zariadení bude riešenie od spoločnosti Cisco) zariadení bude predstavovať integrálnu súčasť služby v rozsahu:
• Nepretržitý 24x7x365 monitoring zariadení s možnosťou okamžitého prehľadu o stave všetkých CPE zariadení.
Monitorovací nástroj bude umiestnený vo VPN sieti a v architektúre budú použité nasledujúce monitorovacie aplikácie:

- Nagios
- Cacti
- Smokeping

Monitorovací nástroj Nagios
Nagios slúži pre monitorovanie počítačových sietí a systémov, kontroluje tzv. hosts (zariadenia – servery, routre a pod.) a services (služby na daných zariadeniach, ako ping, telnet, ssh a pod.), ktoré sú špecifikované používateľom. Pri zmene stavu monitorovaného zariadenia alebo služby, systém umožňuje notifikovať o tejto zmene.
Základné možností systému Nagios sú:

- Monitorovanie sieťových služieb (SMTP, POP3, HTTP, NNTP, PING atď.)
- Monitorovanie systémových zdrojov (záťaž procesora, počet prihlásených používateľov)
- Jednoduchý design plugin-ov umožňujúci vytváranie vlastných service checks
- Paralelné spúšťanie kontrol

- Možnosť implementácie hierarchie siete pomocou definovania parent host – rodičovského zariadenia, čím sa dajú určiť a rozlíšiť zariadenia ktoré sú down alebo unreachable
- Notifikácia definovaného kontaktu (napr. správca Mail serveru) pre zariadenie alebo službu pri zmene ich stavu (e-mailom, sms-kou, pagerom, alebo používateľom definovaným spôsobom)
- Možnosť definovať event handlers , čo môžu byť napr. skripty, ktoré sú spúšťané v nejakom stave zariadenia alebo služby pre aktívne riešenie problému.
- Automatická rotácia log súborov
- Podpora redundantného monitoringu
- Upraviteľné web rozhranie – prezentačná vrstva

Viac informácií o systéme Nagios je možné nájsť na http://www.nagios.org .

Monitorovací nástroj Cacti

Cacti je úplný frontend k RRDTool nástroju, ktorý ukladá všetky potrebné informácie pre vytváranie grafov a napĺňa ich údajmi v MySQL databáze. Cacti je celé naprogramované v PHP, okrem možnosti spravovania grafov, zdrojov dát a Round Robin archívov umožňuje zbieranie dát samozrejme s SNMP podporou.
Zbieranie dát môže byť realizované aj prostredníctvom externých skriptov a tak je možné naplniť akékoľvek dáta do Cacti následne do MySQL/RRD.
Akonáhle sú zadefinované zdroje dát, RRDTool vytvorí grafy. Cacti umožňuje vytváranie komplexných grafov použitím štandardných RRDTool typov grafov a konsolidačných funkcií. Cacti umožňuje nielen vytvárať ale aj mnohými spôsobmi zobrazovať a prezentovať vytvorené grafy. Okrem pohľadov typu „listview“ a „preview“ umožňuje aj zobrazenie v stromovej štruktúre.
Užívateľská administrácia, ktorú poskytuje Cacti, umožňuje pridávať používateľov a prideľovať im práva na prezeranie a editovanie určených častí Cacti.
Cacti je škálovateľné pre použitie s veľkým počtom zdrojov dát a grafov, použitím šablón.

Monitorovací nástroj Smokeping

SmokePing je nástroj na meranie latencie a stratovosti v sieti. Umožňuje merať, zaznamenávať, zobrazovať latenciu a stratovosť v časovom rade. Smokeping používa RRDTool nástroj pre ukladanie dlhodobých výsledkov meraní a tiež pre vykresľovanie grafov v časovom rozlíšení až do 1 minúty.
Smokeping používa systém externých pluginov pre ľahkú rozšíriteľnosť.
Smokeping používa smart alarm systém, na rozdiel od jednoduchých alarmov definovaných medznými hodnotami, smokeping umožňuje definovania vzorov latencie a stratovosti a ich zasielanie na email.
Skriptovacie nástroje slúžia na zálohovanie konfigurácií aktívnych prvkov zákazníka. Konfigurácie sú automaticky zálohované po každej zmene, alebo na pokyn administrátora, čo umožňuje mať aktuálny stav v ľubovoľnom čase a v prípade havárie je možné tieto nahradiť v pôvodnom stave.

Monitorovací nástroj SPECTRUM (v sieti poskytovateľa)

Monitorovacie nástroje umiestnené vo VPN ÚDZS budú doplnené centrálnym monnitorovacím nástrojom SPECTRUM Network Fault Manager spoločnosti Computer Associates, ktorý zabezpečuje monitorovanie a manažment udalostí, chybových stavov, dostupnosti, využitia a výkonu sledovaných zariadení, sieťových prvkov a definovaných funkcií. Je to hlavný nástroj monitorovania telekomunikačnej infraštruktúry spoločnosti a jej zákazníkov.

Implementovaním vybranej sady nástrojov:

- Data Manager with Report Gateway Toolkit;
- MPLS VPN Manager;
- QoS Manager;
- Report Manager;
- Service Manager;
- Service Performance Manager;

zo širokého portfólia SPECTRUM nástrojov, umožňuje operátorom siete podstatne zrýchliť nájdenie príčin porúch, úplnej alebo čiastočnej nefunkčnosti alebo zmene sledovaných parametrov a okamžite iniciovať ich odstránenie. Tieto činnosti podporujú integrované unikátne vlastnosti SPECTRA, ako hľadanie prvotnej príčiny pri komplexnejších poruchách (Root Cause Management), vzťahy medzi udalosťami a stavmi (Event Correlation). Zároveň umožňuje nastaviť a plne automatizovať report manažment.

• Riešenie poruchových stavov v súčinnosti so zodpovednými pracovníkmi ÚDZS. Centrum monitorovania siete 24 hodín denne zabezpečuje dohľad nad všetkými zariadeniami a prenosovými časťami. Kontrolné mechanizmy siete dokážu do určitej miery samostatne rozpoznávať poruchy a netypické situácie a následne informovať technickú podporu signálom o stupni závažnosti podľa typu poruchy. V prípade potreby okamžitého zásahu je o probléme informovaný odborný technický tím, ktorý je pripravený okamžite vzniknutú situáciu riešiť.
Duálny princíp technickej podpory zaručuje, že nikdy nenastane situácia, aby nebol o každom zákazníkovi informovaný aspoň jeden pracovník, ktorý je členom aktuálneho technického tímu.
Náplňou práce technických tímov je preventívna údržba siete, administrácia a konfigurácia siete, výstavba sieťovej infraštruktúry, inštalácia a konfigurácia sieťových prvkov v zákazníckych priestoroch, inštalácia a konfigurácia koncových telekomunikačných zariadení, odstraňovanie poruchových stavov v sieti a na zákazníckych sieťových uzloch, odstraňovanie porúch koncových telekomunikačných zariadení. Alokácia tímov na celom území Slovenska umožňuje rýchly prístup na miesto poruchy a znižuje tak čas potrebný na odstránenie poruchy.

Prípadné poruchy súvisiace s prevádzkou VPN ÚDZS, oznamuje poverený pracovník zákazníka telefonicky alebo písomne (e-mailom alebo faxom) na kontakty:

Centrum monitorovania siete a služba hotline Slovanet
tel. číslo: 02 / 208 28 120,
fax. číslo: 02 / 208 28 222,
e-mail adresa: operator@slovanet.net.
Ohlásenie poruchy musí obsahovať opis poruchy, čas vzniku a identifikáciu volajúceho s kontaktnými údajmi pre informácie o riešení poruchy.

• Implementácia access listov a ďalších IOS možností bude na základe požiadavky ÚDZS

• Prípadné zmeny v konfigurácií CPE alebo VPN siete budú vykonávané výlučne na základe písomnej objednávky ÚDZS

3.6 Poskytovanie služieb expertnej technickej podpory počas realizácie procesu prechodu služieb od súčasného poskytovateľa podľa bodu 5 dokumentu „Príloha č. 1 – Technická špecifikácia – Opis predmetu zákazky“.

3.7 Jednotková cena (hodinová sadzba) za poskytovanie služieb expertnej technickej podpory počas prevádzkovania služieb bude podľa bodu 5 dokumentu „Príloha č. 1 – Technická špecifikácia – Opis predmetu zákazky“.

3.8 Prístup do siete internet bude zabezpečený:
IPS (Intrusion Prevention System) – technológia aktívne chráni sieť pred neoprávneným zásahom kybernetických útokov prostredníctvom aktívneho hľadania a blokovania externých hrozieb ešte predtým, než sa dostanú k potenciálne zraniteľným zariadeniam v sieti. IPS disponuje množstvom funkcií na ochranu citlivých dát, aplikácii a užívateľov ako sú, komplexná ochrana poskytovaná IPS založená na signatúrach, skenovanie anomálií protokolov, zmiernenie DDOS. Po Integrácií IPS do siete zabezpečí nízku latenciu a vysokú mieru zabezpečenia pre citlivé aplikácie, ktoré nie sú ovplyvnené prevádzkou IPS systému. Chráni kritické systémové zdroje proti internému zneužitiu a externými počítačovými zločincami, aj v prípade sofistikovaných útokov. Udržiava aktuálnu a proaktívnu ochranu pred najnovšími známymi hrozbami a novo objavených techník hackovania čo dáva organizáciám čas pre zabezpečenie zraniteľných systémov.

• IPS systémom (v úlohe IPS systému bude riešenie od spoločnosti Fortinet) s parametrami:
• 1 RU prevedenie
• kontrolovaná priepustnosť 1,5Gb/s
• 2x GE manažment interface
• 12x GE monitoring interface
• možnosť vytvoriť 6 ochranných segmentov
• Zero-day ochrana
• kontrola sieťovej aktivity vrátane šifrovanej prevádzky
• granulárna kontrola webových a newebových aplikácií podľa užívateľov alebo skupín užívateľov
• mesačne 4 hodinová bezplatná systémová podpora expertami na konfiguráciu a vyhodnocovanie incidentov
• 36mes podpora výrobcu vrátane prístupu k aktualizáciám

UTM (Unified Threat Management) - konsoliduje viacero funkcií zabezpečenia a vytvárania sietí na jednom zariadení s cieľom chrániť sieťovú infraštruktúru zároveň znižovať riziká, ktoré predstavuje ransomware, phishing a iné vyvíjajúce sa hrozby. UTM zahŕňa u next generation firewall funkcionalitu ako „application control“ (kontrola aplikácii a udržanie škodlivých, rizikových a nežiadúcich aplikácii mimo siete, perimetra siete a dátových centrier), „funkcia antivirus“ (chraniaca e-mailovú komunikáciu klienta pred vírusmi vďaka kvalitnému antivírusovému programu, ktorý umožňuje sledovanie podozrivých súborov na protokoloch http, ftp, imap, pop3, smtp, im, nntp.), IPS “Intrusion Prevention System”, ”Web Filtering” (slúži na obmedzenie a správu prístupu k webovým stránkam z vnútra siete s možnosťou definovať viac druhov filtrov - URL webfilter/content webfilter/webfilter na základe kategórií) a “Antispam Services” (Antispam poskytuje dokonalú kontrolu a ochranu pošty proti nevyžiadaným správam vo všetkých štandardných protokoloch).

• *UTM systémom* (v úlohe UTM firewallu bude riešenie od spoločnosti Fortinet) v režime vysokej dostupnosti s parametrami:
• HA konfigurácia active-active, active-passive, cluster
• 1 RU prevedenie
• 2x GE manažment interface
• 4x GE monitoring interface
• 4x SFP monitoring porty osadené 4x GE RJ45 modulmi
• 120GB vnútorné dátové úložisko

• Real-time aktualizácia signatúr
• Next Generation Firewall s priepustnosťou 1,7Gb/s
• SSL kontrola s priepustnosťou 1,9Gb/s (pri TLS v1.2 s AES256-SHA šifrovaní)
• aplikačná kontrola s priepustnosťou 2,5Gb/s
• počet konkurentných spojení 6mil
• 500 konkurentných SSL-VPN užívateľov
• Zero-day ochrana
• 48 mes podpora výrobcu vrátane prístupu k aktualizáciám

• *Emailovou bránou* (v úlohe E-mail brány bude riešenie od spoločnosti Fortinet) s parametrami
• Konektivita minimálne 4x GE
• Priepustnosť (správ za hodinu):
• email routing ≥3600
• antispam ≥3100
• antispam a antivír ≥2700
• transparentný mód (mail-relay)
• antivírus, antispam, antispyware, antiphising v reálnom čase
• analýzy podľa správania sa odosielateľa
• podpora SPF, DKIM, DMARC štandardov
• podpora minimálne 2 domén
• správa exchange servera

3.9 Riešenie bude umožňovať VPN prístupy interných užívateľov a tretích strán do siete UDZS. Riešenie bude disponovať vysokým stupňom ochrany zabezpečenia služby vzdialeného prístupu:
• Bezpečnosť – na základe dvojfaktorovej autentifikácie zaručí vysokú úroveň zabezpečenia VPN prístupu
• Dostupnosť – riešenie bude škálovateľné, redundantné, odolné voči výpadkom jednej VPN brány
• Manažovateľnosť – riešenie bude poskytovať prehľadný manažment používateľov, asociovaných tokenov a autentifikátorov.
Integrálnou súčasťou riešenia budú špecializované OTP tokeny a taktiež ich voliteľná softvérová varianta pre bežné operačné systémy. Doplnkovými prvkami budú alternatívne tokeny (USB token, smart karta, mobilný telefón). Pre defaultnú dvojfaktorovú autentifikáciu bude poskytnutý, okrem názvu VPN účtu a špecializovaného OTP token-u, ktorý vygeneruje pri prihlasovaní sa používateľa jednorazový číselný kód. Namiesto uvedeného tokenu je možné v niektorých prípadoch použiť softvérový token. Správa VPN používateľov bude oddelená od vnútornej infraštruktúry na samostatnom autentizačnom serveri, vrátane pravidiel, ktoré vymedzujú prístup používateľov na konkrétne zariadenia vo vnútornej sieti. Pre potreby obstarávateľa bude poskytnutý prehľadný webový interfejs pre provisioning vzdialených používateľov (zriadenie nového používateľa, priradenie tokenu používateľovi, zriadenie skupiny používateľov, definovanie politík pre vzdialený prístup,…). Autorizačný server bude umožňovať reporting o udalostiach tykajúcich sa prihlasovania do VPN a kontrolu logov za účelom zisťovania bezpečnostných incidentov. Na strane VPN klienta podávaný systém bude podporovať vzdialene spôsoby prístupu: IPSec a SSL VPN.

3.10 Monitoring a vyhodnocovanie neštandardného správania sa siete s parametrami
• Monitorovanie až na aplikačnú vrstvu OSI modelu s možnosťou výberu protokolov
• Bude umožnená klasifikácia služby/aplikácie, ktoré používajú užívatelia a to aj v prípade, že sú neštandardné (napr. http, ktorá štandardne používa port 80 bude používať iný port a pod.)
• Systém umožní vyhodnocovanie bezpečnostných hrozieb sieťovej infraštruktúry (SIEM), ktorého úlohou bude zhromažďovať, analyzovať a prezentovať údaje zo siete a bezpečnostných zariadení (agregácia dát a ich následná korelácia, vyhodnotenie, alerting, dashboarding a reporting, ukladanie logov). Vyhodnocované zdroje budú

firewally, antivírové servre, aplikačné servre, databázové servre (6HW NODov, 43 virtuálnych serverov)
• Systém umožní upozorniť na bezpečnostné hrozby databázových systémov (databázový firewall) – identifikácia a reporting prístupu k databázam, určovanie pravidiel prístupu a operácií nad dátami vrátane blokovania podozrivých transakcií, posilnenie integrity dát. Služba umožní vytvoriť model správania sa užívateľov (štandardné a neštandardné) a na základe vytvoreného pravidla notifikovať o podozrivých transakciách
• Systém umožní zasielanie dohodnutých reportov a na vyžiadanie prístup do monitoringu pre zamestnancov ÚDZS

3.11 Prenájom a prevádzka systému IP telefónie, ktorý bude pozostávať z IPPBX od spoločnosti XORCOM v režime vysokej dostupnosti (HA) umiestnenej na centrále. Systém IP telefónie bude zabezpečovať:
• Lokálny prestup volaní do VTS s vlastnými geografickými DDI číslami
• Automatické smerovanie hovorov
• Volania v rámci vlastnej siete bezplatne
• Možnosť presmerovania hovorov v celej sieti
• 420 klapiek
• Zachovanie súčasne platného číslovacieho plánu
• Súčasťou ponuky bude prenájom priechodných IP telefónnych aparátov s portami 10/100/1000Base-T s PoE funkcionalitou registrujúcich sa na IPPBX na centrále
• Riešenie umožňuje čiastočnú vlastnú správu užívateľov

Tabuľka č. 1 – Zoznam koncových bodov a požadovaných parametrov

Typ	Adresa	Primárne pripojenie (Mb/s)	Záložné pripojenie (Mb/s)	Odovzdávajúce rozhranie
1-centrála	Žellova 2, Bratislava	100	---	1000Base-T
1-MPLS	Žellova 2, Bratislava	300	60	1000Base-T
1-internet	Žellova 2, Bratislava	150	40	1000Base-T
1- datacentrum	Ipeľská 1, Košice	50	10	1000Base-T
2	Trojičné nám. 10, Trnava	30	5	1000Base-T
2	Legionárska 17, Trenčín	30	5	1000Base-T
2	Coboriho 2, Nitra	30	5	1000Base-T
2	Wolkerova 34, Banská Bystrica	30	5	1000Base-T
2	Kuzmányho 27/B, Martin	30	5	1000Base-T
2	Ipeľská 1, Košice	30	5	1000Base-T
2	Kúpeľná 3, Prešov	30	5	1000Base-T
2	Antolská 11, Bratislava	30	5	1000Base-T
2	Sasinkova 4, Bratislava	30	5	1000Base-T
2	Špitálska 6, Nitra	30	5	1000Base-T
2	Nám. L. Svobodu 1, Banská Bystrica	30	5	1000Base-T
2	V. Spanyola 43, Žilina	30	5	1000Base-T
2	Zdravotnícka 3253/3, Poprad	30	5	1000Base-T
2	Hollého 14, Prešov	30	5	1000Base-T

Tabuľka č. 2 – Zoznam koncových bodov a požadovaných parametrov

Typ	Adresa	Počet LAN portov	Počet uplink portov
1	Žellova 2, Bratislava	240	36
1	Žellova 2, Bratislava, centrálne prepínače	96	8
1	Ipeľská 1, Košice, centrálny prepínač	96	8
2	Trojičné nám. 10, Trnava	48	4
2	Legionárska 17, Trenčín	48	4
2	Coboriho 2, Nitra	48	4
2	Wolkerova 34, Banská Bystrica	48	4
2	Kuzmányho 27/B, Martin	96	8
2	Ipeľská 1, Košice	48	4
2	Kúpeľná 3, Prešov	48	4
2	Antolská 11, Bratislava	96	8
2	Sasinkova 4, Bratislava	48	4
2	Špitálska 6, Nitra	48	4
2	Nám. L. Svobodu 1, Banská Bystrica	48	4
2	V. Spanyola 43, Žilina	48	4
2	Zdravotnícka 3253/3, Poprad	48	4
2	Hollého 14, Prešov	48	4

4. Dohoda o úrovni poskytovanej služby SLA

4.1 Definície a úroveň požadovanej SLA

Dostupnosť služby (ďalej tiež „SA“, t.j. Service Availability) je garantovaná dostupnosť služby vyjadrená ako podiel času, počas ktorého môže užívateľ používať službu v dohodnutom rozsahu a kvalite, k dĺžke celého sledovaného obdobia. Sledované obdobie je kalendárny mesiac (vyjadrený v minútach) a výsledná hodnota dostupnosti služby sa vyjadruje v percentách so zaokrúhlením na dve desatinné miesta smerom nahor.
Dostupnosť bude počítaná podľa nasledovného vzorca:

$$\textbf{Dostupnosť služby [\%]} = \frac{(\sum \text{minút/mesiac} - \sum \text{minút nedostupnosti/mesiac})}{\sum \text{minút / mesiac}} \text{ x } 100\%$$

Doba nedostupnosti služby (vyjadrená v minútach) je doba, počas ktorej nemohla byť služba používaná v dohodnutej kvalite.

Dĺžka sledovaného obdobia:

Počet dní v mesiaci	Počet minút v mesiaci
28	40 320
29	41 760
30	43 200
31	44 640

Maximálna doba na odstránenie poruchy (ďalej tiež „TTR“, t.j. Time To Repair) je garantovaná doba na odstránenie poruchy v pracovnom a/alebo mimopracovnom bloku, ktorá sa počíta ako doba medzi ohlásením poruchy autorizovaným zástupcom užívateľa a okamihom obnovenia poskytovania služby. Do celkového času trvania poruchy sa nezapočítavajú a za poruchu sa nepovažujú všetky nasledovné dôvody a doby:

a) prerušenie poskytovania služby z dôvodu dohodnutej plánovanej údržby;
b) prerušenie poskytovania služby z dôvodu neplánovanej údržby odsúhlasenej užívateľom;
c) dočasné prerušenie poskytovania služby na žiadosť užívateľa;
d) prerušenie poskytovania služby spôsobené užívateľom spôsobené zásahom do zariadení poskytovateľa služby, resp. ich odpojením;
e) prerušenie poskytovania služby spôsobené prerušením elektrického napájania zariadení určených na poskytovanie služby v priestoroch užívateľa;
f) prerušenie poskytovania služby spôsobené poruchou na vnútorných rozvodoch vo vlastníctve užívateľa, resp. vo vlastníctve tretej strany;
g) doba, počas ktorej nebol umožnený prístup pracovníkom poskytovateľa služby do priestorov užívateľa, za účelom analýzy a zistenia príčin poruchy, ako aj opravy poruchy na zariadeniach a príslušnej infraštruktúre, prostredníctvom ktorých je služba poskytovaná;
h) doba, počas ktorej nebola poskytnutá potrebná súčinnosť zo strany užívateľa;
i) doba prerušenia poskytovania služby z dôvodov okolností vyššej moci.

Garantované maximálne oneskorenie (ďalej tiež „RTD“, t.j. Round Trip Delay) je maximálna hodnota oneskorenia paketov pri prenose elektronickou komunikačnou sieťou. Je meraná ako oneskorenie paketu s referenčnou dĺžkou 64 bajtov medzi definovanými prípojnými bodmi alebo kostrovými uzlami elektronickej komunikačnej siete.

Strata paketov (ďalej tiež „PLR“, t.j. Packet Loss Ratio) udáva percento paketov prenášaných cez elektronickú komunikačnú sieť, ktoré sa nedostali do cieľa. Je to pomer celkového počtu paketov stratených medzi definovanými prípojnými bodmi alebo kostrovými uzlami elektronickej komunikačnej siete vztiahnutý k celkovému počtu odoslaných paketov.
„Nulová“ strata paketov indikuje, že žiadny paket sa nestratil počas prenosu.

Tabuľka č. 3 - Parametre SLA

Koncový bod	Parameter a hodnota
Typ 1	Dostupnosť 99,99% Maximálne oneskorenie – do 30 ms Chybovosť (strata paketov) – max. 0,5% TTR – do 2 hodín
Typ 2	Dostupnosť 99,70% Maximálne oneskorenie – do 60ms Chybovosť (strata paketov) – max. 1% TTR – do 6 hodín

Poznámka: TTR sa viaže na primárny prístup, SA je viazaný na celkovú dostupnosť lokality (koncového bodu služby) za mesiac.

4.2 Služby v rámci SLA

Pod pojmom „pracovná doba“ sa chápe čas od 8:00 hod. do 17:00 hod. v rámci bežných pracovných dní. Pokiaľ nie je uvedené inak, týkajú sa garantované kvalitatívne parametre služieb, ako aj servisné a záručné podmienky (ďalej SLA) výhradne iba tých softvérových a hardvérových komponentov, ktoré poskytol alebo spravuje dodávateľ. SLA bude dodávateľ poskytovať počas celej doby poskytovania služieb a to nasledovne:

• Proaktívny dohľad a monitorovanie funkčnosti jednotlivých hardvérových a softvérových komponentov VPN a VPN ako celku, je poskytované 365 dní v roku, 7 dní v týždni, 24 hodín (ďalej aj 7dx24h). Dodávateľ bude zároveň monitorovať komponenty IT a IS infraštruktúry, ktoré ÚDZS požiada o zaradenie do sledovania.
• Dodávateľ zabezpečí pre ÚDZS bezplatný online prístup na monitorovací systém a to v režime „read only“ 24x7x365
• Podpora komponentov VPN je poskytovaná v pracovnej dobe (5dx8h)
• Update a upgrade SW komponentov VPN bude vykonávaný dodávateľom podľa potrieb ÚDZS so zreteľom na minimalizáciu výpadkov a dodržania dohodnutých parametrov VPN
• Analýza záznamov a pravidelné správy - reporty o výpadkoch a bezpečnostných incidentoch vo VPN bude dodávateľom poskytovaná v pracovnej dobe

4.3 Reporty

SLA reporty bude dodávateľ poskytovať počas celej doby poskytovania služieb a to nasledovné:

• Reporty budú aj v grafickej podobe
• Agregované reporty vyťaženia linky - link performance (rozlíšenie hodina, deň, mesiac), história uchovania min. 3 mesiace
• Real time detailné reporty vyťaženie linky s rozlíšením maximálne 5 min, história uchovania minimálne 24 hod.
• Dostupnosť dátovej linky – service availability
• Reporty per QoS, vyťaženie linky real time pre každú triedu služieb samostatne
• Pre každú triedu merať a reportovať jitter, delay, packet loss
• Reporty budú poskytované pre všetky kategórie koncových bodov
• Prístup na www stránku poskytovateľa poskytujúcu informácie o vyťažení a poruchovosti,
• Notifikácie ÚDZS o výpadkoch a bezpečnostných incidentoch vo VPN bude dodávateľom poskytovaná 7dx24h a to okamžite po ich zistení
• Dodávateľ bude sledovať jednotlivé parametre VPN a bude podávať návrhy na prípadné zmeny v nastaveniach VPN tak, aby bola dosiahnutá efektívna optimalizácia využívania poskytovaných služieb. Toto bude poskytované v pracovnej dobe
• Dodávateľ bude poskytovať konzultácie k problematike poskytovaných služieb v rozsahu do 20 hodín v rámci 1 kalendárneho mesiaca, konzultácie budú poskytované na žiadosť ÚDZS

4.4 Sankcie

Vrátenie časti už zaplatenej ceny za poskytovanie služby za nedodržanie dohodnutej úrovne služby:

Typ 1 - Hodnota SLA	Výška časti ceny
SA > 99,99 %	Bez vrátenia
99,89 % > SA > 99,58 %	5% z ceny za používanie príslušného prístupu s SLA
99,58 % > SA > 99,31 %	10% z ceny za používanie príslušného prístupu s SLA
99,30% > SA	15% z ceny za používanie príslušného prístupu s SLA

Hodnota SLA	Výška časti ceny
TTR > 2 hodiny	Za každú ďalšiu začatú hodinu omeškania 1% z mesačného poplatku, max. do výšky 30%

Typ 2 - Hodnota SLA	Výška časti ceny
SA > 99,70 %	Bez vrátenia
99,69 % > SA > 99,44 %	5% z ceny za používanie príslušného prístupu s SLA
99,43 % > SA > 98,91 %	10% z ceny za používanie príslušného prístupu s SLA
98,90% > SA	15% z ceny za používanie príslušného prístupu s SLA

Hodnota SLA	Výška časti ceny
TTR > 6 hodiny	Za každú ďalšiu začatú hodinu omeškania 1% z mesačného poplatku, max. do výšky 30%