

**Zmluva č. 23/2021/110 o pripojení do vládnej dátovej siete GOVNET
a o poskytnutí súvisiacich výkonov**

uzatvorená podľa § 51 zákona č. 40/1964 Zb. Občiansky zákonník
v znení neskorších predpisov

medzi zmluvnými stranami:

Národná agentúra pre sieťové a elektronické služby

Sídlo: Kollárova 8, 917 02 Trnava

IČO: 42 156 424

DIČ: 20 2273 6287

IČ DPH: SK20 2273 6287

Zastúpená: Ing. Pavel Karel

Bankové spojenie:

IBAN:

(ďalej len „*NASES*“)

a

Pôdohospodárska platobná agentúra

Sídlo: Hraničná 12, 815 26 Bratislava

IČO: 30 794 323

DIČ: 2021196210

Zastúpený: Ing. Jaroslav Jánoš, generálny riaditeľ

Bankové spojenie: Štátna pokladnica

IBAN:

(ďalej len „*PPA*“)

(*NASES* a *PPA* spoločne ďalej len „*Zmluvné strany*“)

Preambula

Keďže

predmetom činnosti *NASES* je správa, prevádzkovanie a rozvoj vládnej dátovej siete GOVNET (ďalej len „*GOVNET*“);

NASES nemá kryté náklady vzniknuté s pripojením *PPA* do *GOVNET* príspevkom z rozpočtu zriaďovateľa *NASES*;

PPA ako subjekt oprávnený na pripojenie do *GOVNET* prejavil záujem o pripojenie do *GOVNET* a o nahradenie nákladov s tým spojených;

sa *Zmluvné strany* rozhodli uzatvoriť túto Zmluvu o pripojení do vládnej dátovej siete GOVNET a o poskytnutí súvisiacich výkonov (ďalej len „Zmluva“) za nasledovných podmienok:

Čl. I

Predmet zmluvy

Predmetom tejto *Zmluvy* je:

- a) záväzok *NASES* zabezpečiť pripojenie *PPA* do *GOVNET* počas trvania tejto *Zmluvy*,
- b) záväzok *PPA* viazať prostriedky v rámci svojho rozpočtu v prospech *NASES* na náklady vzniknuté s plnením záväzku *NASES* podľa písm. a) tohto odseku, ktoré nie sú kryté príspevkom z rozpočtu zriaďovateľa *NASES*,
- c) úprava práv a povinností súvisiacich s plnením záväzkov *Zmluvných strán* podľa písm. a) a b) tohto odseku.

Čl. II

Podmienky pripojenia

1. *NASES* vytvorí pre *PPA* potrebné uzly na pripojenie do *GOVNET*.
2. *NASES* je povinná zabezpečiť pripojenie *PPA* do *GOVNET* najneskôr do siedmich dní od vytvorenia uzlov podľa ods. 1 tohto článku.
3. *NASES* je povinná zabezpečiť bezpečnosť a kyberbezpečnosť uzlov *GOVNET* pre *PPA*.
4. Zoznam zriaďovaných uzlov *GOVNET* pre *PPA* je uvedený v Prílohe č. 1 tejto *Zmluvy*.
5. Podrobná špecifikácia poskytovaných výkonov je uvedená v Prílohe č. 2 tejto *Zmluvy*.
6. Uzol *GOVNET* bude zriadený podľa technických požiadaviek k pripájaniu sa do siete *GOVNET* definovaných v dokumente „Informácie pre uzly - technické požiadavky k pripájaniu do siete Govnet“, ktorý tvorí prílohu č. 3 tejto *Zmluvy*.
7. O zriadenie nových uzlov *GOVNET* môže *PPA* požiadať *NASES* formou e-mailovej žiadosti so špecifikáciou prípojného miesta a to na adresu govnet@nases.gov. *NASES* sa zaväzuje do 30 dní odo dňa obdržania požiadavky pripraviť návrh dodatku k tejto *Zmluve* a poskytnúť ho *PPA* na pripomienkovanie. Po schválení požiadavky na pripojenie nových uzlov *GOVNET* pre *PPA* a uzatvorení dodatku k tejto *Zmluve* sa bude postupovať podľa ods. 2 tohto článku.
8. *NASES* bude zabezpečovať pripojenie *PPA* do *GOVNET* v režime 24 hodín x 7 dní v týždni a o všetkých výpadkoch a odstávkach systému bude informovať *PPA*. *NASES* je oprávnená v prípade hrozby kybernetického útoku alebo iného ohrozenia *GOVNET* na nevyhnutný čas blokovat' pripojenie *PPA* do *GOVNET*.
9. *PPA* sa zaväzuje nezasahovať do zariadení v správe *NASES* bez jej predchádzajúceho súhlasu. *PPA* sa zaväzuje informovať *NASES* o výpadkoch alebo chybách fungovania uzlov *GOVNET* a ich pripojenia, a to bezodkladne ako sa o tom dozvie.

Čl. III Náhrada za pripojenie

1. PPA je povinný viazať v rámci svojho rozpočtu rozpočtové prostriedky na náklady vzniknuté s pripojením do *GOVNET*, v prospech *NASES*, príspevkovej organizácie patriacej pod rozpočtovú kapitolu Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.

Celková výška týchto nákladov za dobu trvania tejto zmluvy je 561 960,00 Eur (slovom päťstošesťdesiatjedentisíc deväťstošesťdesiat eur).

2. Výška nákladov pre rok 2021 (t.j. 7 mesiacov poskytovania pripojenia podľa Čl. II Zmluvy a v súlade s bodmi 4. až 6. Čl. II Zmluvy) je 327 810,00 Eur (slovom trisťtisíc osemstodesať eur) a výška nákladov pre rok 2022 (t.j. 5 mesiacov poskytovanie pripojenia podľa čl. II Zmluvy a v súlade s bodmi 4. až 6. čl. II Zmluvy) je 234 150,00 Eur (slovom dvestotridsaťštyritisíc stopäťdesiat eur).

Čl. IV Trvanie zmluvy

1. Táto *Zmluva* sa uzatvára na dobu určitú do 31.05.2022.
2. V prípade, ak ktorákoľvek zo *Zmluvných strán* bude mať záujem o predĺženie trvania *Zmluvy*, sa zaväzuje do 15.03.2022 písomne požiadať druhú *Zmluvnú stranu* o predĺženie trvania *Zmluvy*. V takom prípade sa *Zmluvné strany* zaväzujú do 14 dní odo dňa doručenia žiadosti uskutočniť rokovanie o podmienkach predĺženia trvania *Zmluvy* a následne uzavrieť dodatok k tejto *Zmluve* v zmysle čl. V ods. 2 tejto *Zmluvy*.
3. V prípade, ak:
 - a) o predĺženie trvania *Zmluvy* požiadal *PPA*,
 - b) *Zmluvné strany* sa nedohodli na podmienkach predĺženia trvania tejto *Zmluvy* podľa ods. 2 tohto článku a
 - c) *PPA* písomne oznámila, že trvá na svojej žiadosti,trvanie *Zmluvy* sa predĺži o jeden rok. *NASES* je v takom prípade oprávnená jednostranne určiť výšku nákladov vzniknutých s pripojením *PPA* do *GOVNET* po dobu ďalšieho roka a *PPA* je povinný takto vyčíslené náklady uhradiť *NASES* v lehotách a spôsobom určeným v tejto *Zmluve*.
4. Túto *Zmluvu* je možné jednostranne písomne vypovedať aj bez uvedenia dôvodu. Výpovedná lehota je tri (3) mesiace a začína plynúť v prvý deň mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej *Zmluvnej strane*. Výpovedná lehota skončí však najneskôr v termíne uvedenom v ods. 1 tohto článku alebo v súlade s termínom uvedeným v dodatku k tejto *Zmluve* upravujúcim predĺženie trvania tejto *Zmluvy*.
5. Od tejto *Zmluvy* je možné písomne odstúpiť v prípade opakovaného alebo podstatného porušenia niektorej zmluvnej povinnosti. Na účely tejto *Zmluvy* je porušenie *Zmluvy* podstatné, ak strana porušujúca *Zmluvu* vedela v čase uzavretia *Zmluvy* alebo v tomto čase bolo rozumné predvídať s prihliadnutím na účel *Zmluvy*, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola *Zmluva* uzavretá, že druhá strana nebude mať záujem na plnení povinností

pri takom porušení *Zmluvy*. Pri pochybnostiach sa predpokladá, že porušenie *Zmluvy* nie je podstatné.

6. V prípade, ak dôjde k ukončeniu *Zmluvy* pred termínom uvedeným v bode 1. tohto čl.VI *Zmluvy*, PPA má nárok na vrátenie alikvotnej časti náhrady za pripojenie za obdobie po ukončení účinnosti tejto *Zmluvy*.

Čl. V **Záverečné ustanovenia**

1. Táto *Zmluva* nadobúda účinnosť dňom nasledujúcim po dni jej prvého zverejnenia v Centrálnom registri zmlúv.

2. Zmeny a dodatky k tejto *Zmluve* je možné vykonať len formou písomných číslovaných dodatkov, podpísaných štatutárnymi zástupcami *Zmluvných strán*.

3. Vzťahy *Zmluvných strán* súvisiace s touto *Zmluvou* a v tejto *Zmluve* bližšie neupravené, sa riadia príslušnými ustanoveniami Občianskeho zákonníka a ďalších všeobecne záväzných právnych predpisov.

4. Ak sú niektoré ustanovenia tejto *Zmluvy* neplatné alebo neúčinné alebo ak sa neplatnými stanú neskôr alebo svoju účinnosť stratia, nebude tým dotknutá platnosť a účinnosť ostatného obsahu tejto *Zmluvy*. Predmetné ustanovenie sa nahradí ustanovením, ktoré sa čo najviac blíži účelu, sledovanému *Zmluvnými stranami*.

5. Spory týkajúce sa tejto *Zmluvy* sa *Zmluvné strany* zaväzujú riešiť prednostne dohodou a vzájomným rokovaním. Ak dohoda nie je možná, pre riešenie sporov z tejto *Zmluvy* sú príslušné všeobecné súdy Slovenskej republiky.

6. Miestom pre doručovanie písomností sú adresy *Zmluvných strán* uvedené v záhlaví tejto *Zmluvy* alebo neskôr písomne oznámené. Každá zo *Zmluvných strán* je povinná písomne oznámiť druhej *Zmluvnej strane* akúkoľvek zmenu ohľadne doručovania, a to bezodkladne po tom, čo k takejto zmene dôjde. *Zmluvné strany* sa dohodli, že písomnosť doručovaná na miesto pre doručovanie písomností sa považuje za doručeníu v tretí (3.) pracovný deň nasledujúci po dni podania písomnosti na poštovú prepravu, ak písomnosť nebude doručená skôr.

7. Táto *Zmluva* je vyhotovená v štyroch rovnopisoch, z ktorých *NASES* dostane dva rovnopisy a *PPA* dva rovnopisy.

8. *Zmluvné strany* vyhlasujú, že ich vôľa vyjadrená v tejto *Zmluve* je slobodná a vážna, túto *Zmluvu* neuzatvárajú v tiesni, za nápadne nevýhodných podmienok a ich zmluvná voľnosť nie je inak obmedzená. Svoju vôľu byť viazané touto *Zmluvou* *Zmluvné strany* vyjadrujú svojimi podpismi tejto *Zmluvy*.

9. *Zmluvné strany* sa dohodli, že *NASES* nie je oprávnená postúpiť akékoľvek pohľadávky voči *PPA* podľa § 524 a nasl. zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov plynúce z tejto *Zmluvy* na tretí subjekt bez predchádzajúceho písomného súhlasu *PPA*. Právny úkon, ktorým by došlo k postúpeniu pohľadávky *NASES* v rozpore s touto zmluvou je podľa § 39 Občianskeho zákonníka neplatný.

10. Neoddeliteľnou súčasťou tejto *Zmluvy* sú:

Príloha č. 1 – Zoznam uzlov GOVNET pre PPA,

Príloha č. 2 – Špecifikácia výkonov,

Príloha č. 3 – Informácie pre uzly - technické požiadavky k pripájaniu do siete Govnet.

Za Národnú agentúru
pre sieťové a elektronické služby:

Za Pôdohospodársku platobnú agentúru:

V Bratislave, dňa

V Bratislave, dňa

Ing. Pavel Karel
generálny riaditeľ

Ing. Jaroslav Jánoš
generálny riaditeľ

Príloha č. 1 – Zoznam uzlov -Pobočková sieť WAN PPA a pripojenie do siete GOVNET

	Koncový bod	Služba	Primárne pripojenie		Backup pripojenie		Koncové zariadenie	
			Technológia	Kapacita (Mbit)	Technológia	Kapacita (Mbit)		
GOVNET	Centrála Hraničná	Pripojenie do siete Govnet SECPORT_S+	optika	100	optika	100	██████████	██████████
Centrálné body PPA	DC Perpetuus - Hraničná	Prepojenie centrálnych bodov - DF jednovláknno	DF vlákno	4x DF jednovláknno	DF vlákno	4 x DF jednovláknno		
	DC Perpetuus	Centrálny bod - SECPORT_XL						
		MPLS VPN (B)	optika	1000				██████████
		Back up - Internet konektivita (B)	optika	500				
	Centrála Hraničná	MPLS VPN - centrála (A)	optika	1000				██████████
Back up - Internet konektivita (A)		optika	500					
Pobočky	Dobrovičova - HRANIČNA	L2	optika	500	optika	100	██████████	██████████
	Rimavská Sobota	MPLS VPN	RR	100	ST DO	4/4	██████████	██████████
	Dolný Kubín	MPLS VPN	FTP/POP	100	ADSL	15/1	██████████	██████████
	Michalovce	MPLS VPN	RR	100	ADSL	15/1	██████████	██████████
	Prešov	MPLS VPN	FTP/POP	200	VDSL	50/5	██████████	██████████
	Poprad	MPLS VPN	RR	100	ADSL	15/1	██████████	██████████
	Nové Zámky	MPLS VPN	RR	100	ADSL	15/1	██████████	██████████
	Dunajská Streda	MPLS VPN	RR	100	ADSL	15/1	██████████	██████████
	Levice	MPLS VPN	RR	100	ADSL	15/1	██████████	██████████
	Žilina	MPLS VPN	RR	200	VDSL	50/5	██████████	██████████
	Trenčín	MPLS VPN	RR	200	VDSL	30/5	██████████	██████████
	Trnava	MPLS VPN	optika	200	VDSL	50/5	██████████	██████████
	Nitra	MPLS VPN	RR	200	VDSL	50/5	██████████	██████████
	Košice	MPLS VPN	optika	200	ADSL	11/0.5	██████████	██████████
	Zvolen	MPLS VPN	RR	200	LTE	10/5	██████████	██████████
	Komárno - zrušené							



Príloha č. 2 – špecifikácia výkonov

Technického riešenia pripojenie do siete GOVNET a prevádzku WAN siete pre PPA

TECHNICKÉHO RIEŠENIA

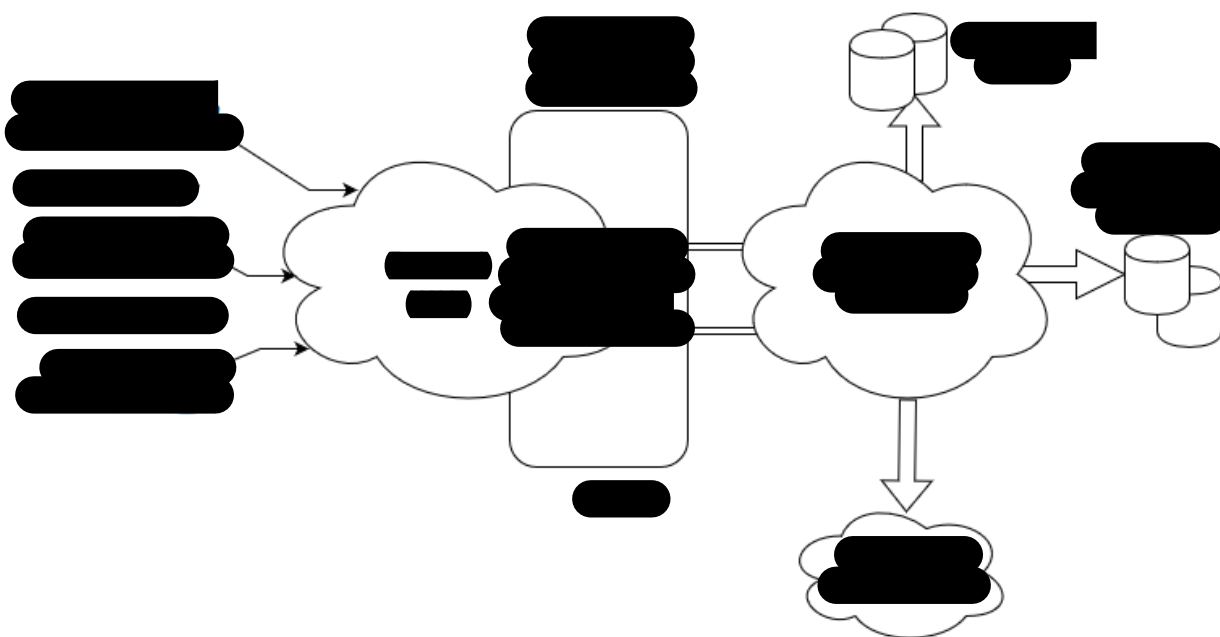
Jedná sa o správu a prevádzku počítačovej siete WAN - PPA pre organizáciu Pôdohospodárska platobná agentúra

Pripojenie je riešené ako pripojenie organizácie a jej regionálnych odborov do virtuálnej privátnej siete a pripojenie do infraštruktúry siete GOVNET, ktorá poskytuje služby pripojenia pre subjekty, ktoré potrebujú komunikovať elektronicky a pre svoj výkon potrebujú pristupovať do centralizovaných modulov verejnej správy.

Skladá sa z nasledujúcich funkčných celkov:

1. Pobočková VPN sieť WAN PPA
2. Pripojenie do siete GOVNET – koncový uzol siete na centrále – PPA
3. Poskytovanie centralizovaných služieb siete GOVNET
 - a. Poskytovanie centralizovaných služieb email, web a prislúchajúcich služieb typu DNS a centralizovanej sieťovej ochrany / proxy, fw a pod/
 - b. Pripojenie do centralizovaných modulov verejnej správy /UPVS a pod./
 - c. Pripojenie do ext. Sietí /Internet, Hlas a pod./

Logická schéma pripojenia pobočiek PPA a Centrálý do siete Govnet



Funkčné celky detailne

1. Pobočková sieť WAN PPA

Jedná sa o poskytovanie služieb komunikačnej infraštruktúry prepájajúcej jednotlivé pracoviská / Generálne Riaditeľstvo a Regionálne pracoviská / a ich integráciu na koncový uzol siete GOVNET v lokalite centrály PPA

Špecifikácia WAN pobočkový uzol

Pri WAN službe vzdialené lokality (pobočky) typicky okrem WAN prepojenia nemajú zriadenú žiadnu ďalšiu službu IP MPLS siete Govnet.

Ďalšie služby, ako napr. Govnet (zabezpečené prepojenie vládných organizácií alebo inštitúcií štátnej správy, bezpečné pripojenie do siete Internet), Untrusted Internet, Testa, IPTV alebo Voice sú zriadené iba na centrálnej lokalite zákazníka.

- _____
- _____

- _____
- _____
- _____

- _____
- _____
- _____
- _____

Služba zahŕňa:

- Služba prenájmu CPE routra
- Systémová a technická podpora siete WAN až po úroveň ethernet portu pripájajúceho LAN siete pracoviska
- Možnosť vytvorenia komunikačných profilov (QoS) podľa požiadaviek na kvalitu prenosových služieb v rôznych triedach podľa požiadaviek
- Podpora IPv6
- Monitoring siete WAN zákazníka v nepretržitej prevádzke 24/7 na zaručenie rýchleho riešenia incidentov
- Poskytovanie služieb dohľadového centra a helpdesku na nahlasovanie incidentov a výpadkov zákazníkom v elektronickom nástroji
- Zbieranie štatistických dát zo siete , ich vyhodnocovanie
- Voliteľne - Mesačné reporty dostupnosti, udalostí a prevádzky

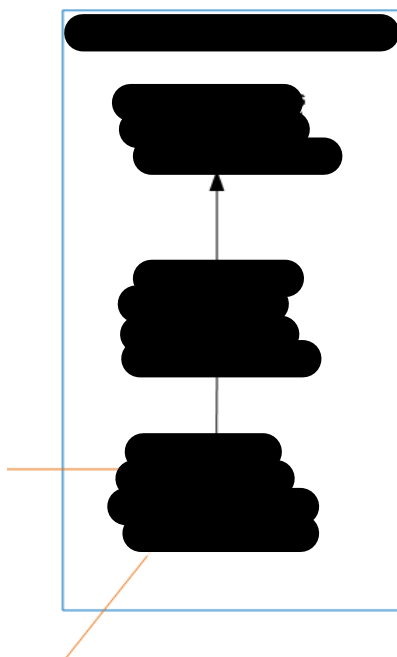
2. GOVNET SMALL uzol – 100 Mb , redundantný

Tento typ uzly sa zriaďujú u zákazníkov, ktorí majú stredné požiadavky na prenosovú rýchlosť.

Navrhované parametre pripojenia :

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Logická schéma pripojenia



SLA :

Druh SLA	Stratovosť počas 95% času merania	Oneskorenie počas 95% času merania	Variácia oneskorenia počas 95% času merania	Dostupnosť	Doba odstránenia poruchy	Backup *
SLA 3	Max. 1%	40ms	20ms	99,70%	4 hod	nie

Parametre služby a súhrn navrhovaných typov pripojenia

	Koncový bod	Služba	Primárne pripojenie		Backup pripojenie		Koncové zariadenie	
			Technológia	Kapacita (Mbit)	Technológia	Kapacita (Mbit)		
GOVNET	Centrála Hraničná	Pripojenie do siete Govnet SECPORT_S+	optika	100	optika	100	████████	████████
Centrálne body PPA	DC Perpetuus - Hraničná	Prepojenie centrálnych bodov - DF jednovlákno	DF vlákno	4x DF jednovlákno	DF vlákno	4 x DF jednovlákno		
	DC Perpetuus	Centrálny bod - SECPORT_XL						
		MPLS VPN (B)	optika	1000				████████
		Back up - Internet konektivita (B)	optika	500				
	Centrála Hraničná	MPLS VPN - centrála (A)	optika	1000				████████
Back up - Internet konektivita (A)		optika	500					
Pobočky	Dobrovičova - HRANIČNA	L2	optika	500	optika	100	████████	████████
	Rimavská Sobota	MPLS VPN	RR	100	ST DO	4/4	████████	████████
	Dolný Kubín	MPLS VPN	FTP/POP	100	ADSL	15/1	████████	████████
	Michalovce	MPLS VPN	RR	100	ADSL	15/1	████████	████████
	Prešov	MPLS VPN	FTP/POP	200	VDSL	50/5	████████	████████
	Poprad	MPLS VPN	RR	100	ADSL	15/1	████████	████████
	Nové Zámky	MPLS VPN	RR	100	ADSL	15/1	████████	████████
	Dunajská Streda	MPLS VPN	RR	100	ADSL	15/1	████████	████████
	Levice	MPLS VPN	RR	100	ADSL	15/1	████████	████████
	Žilina	MPLS VPN	RR	200	VDSL	50/5	████████	████████
	Trenčín	MPLS VPN	RR	200	VDSL	30/5	████████	████████
	Trnava	MPLS VPN	optika	200	VDSL	50/5	████████	████████
	Nitra	MPLS VPN	RR	200	VDSL	50/5	████████	████████
	Košice	MPLS VPN	optika	200	ADSL	11/0.5	████████	████████
	Zvolen	MPLS VPN	RR	200	LTE	10/5	████████	████████
	Komárno - zrušené							



CENOVÁ PONUKA - Pobočková sieť WAN PPA a pripojenie do siete GOVNET

	Koncový bod	Služba	Primárne pripojenie		Backup pripojenie		Koncové zariadenie		PONUKA (EUR bez DPH)	
			Technológia	Kapacita (Mbit)	Technológia	Kapacita (Mbit)			Mesačný poplatok	Inštalčný poplatok
GOVNET	Centrála Hraničná	Pripojenie do siete Govnet SECPort_S+	optika	100	optika	100	████████	████████	990 €	- €
Centrálna body PPA	DC Perpetuus - Hraničná	Prepojenie centrálnych bodov - DF jednovláknovo	DF vlákno	4x DF jednovláknovo	DF vlákno	4 x DF jednovláknovo			11 640 €	- €
	DC Perpetuus	Centrálny bod - SECPort_XL							3 500 €	- €
		MPLS VPN (B)	optika	1000				████████	1 500 €	- €
		Back up - Internet konektivita (B)	optika	500					990 €	- €
	Centrála Hraničná	MPLS VPN - centrála (A)	optika	1000					1 500 €	- €
Back up - Internet konektivita (A)		optika	500				████████	990 €	- €	
Pobočky	Dobrovičova - HRANIČNA	L2	optika	500	optika	100		████████	1 500 €	- €
	Rimavská Sobota	MPLS VPN	RR	100	ST DO	4/4	████████	████████	1 045 €	- €
	Dolný Kubín	MPLS VPN	FTP/POP	100	ADSL	15/1	████████	████████	1 045 €	- €
	Michalovce	MPLS VPN	RR	100	ADSL	15/1	████████	████████	1 045 €	- €
	Prešov	MPLS VPN	FTP/POP	200	VDSL	50/5	████████	████████	1 300 €	- €
	Poprad	MPLS VPN	RR	100	ADSL	15/1	████████	████████	1 045 €	- €
	Nové Zámky	MPLS VPN	RR	100	ADSL	15/1	████████	████████	1 045 €	- €
	Dunajská Streda	MPLS VPN	RR	100	ADSL	15/1	████████	████████	1 045 €	- €
	Levice	MPLS VPN	RR	100	ADSL	15/1	████████	████████	1 045 €	- €
	Žilina	MPLS VPN	RR	200	VDSL	50/5	████████	████████	1 300 €	- €
	Trenčín	MPLS VPN	RR	200	VDSL	30/5	████████	████████	1 300 €	- €
	Trnava	MPLS VPN	optika	200	VDSL	50/5	████████	████████	1 300 €	- €
	Nitra	MPLS VPN	RR	200	VDSL	50/5	████████	████████	1 300 €	- €
	Košice	MPLS VPN	optika	200	ADSL	11/0,5	████████	████████	1 300 €	- €
	Zvolen	MPLS VPN	RR	200	LTE	10/5	████████	████████	1 300 €	- €
	Komárno - zrušené								- €	- €
								39 025 €	- €	

Ceny sú kalkulované v EUR bez DPH.

Sieť Govnet – informácia pre uzly

Upozornenie: Dokument obsahuje aktuálne informácie ku dňu vydania. Pravidlá a informácie môže prevádzkovateľ siete Govnet kedykoľvek jednostranne zmeniť. Aktuálne znenie dokumentu je dostupné v sieti Govnet na adrese <https://govnet.gov.sk/>. Táto adresa nie je publikovaná do Internetu.

verzia	dátum	popis
9.6	5.5. 2020	aktualizované adresy serverov , všeobecné požiadavky na uzol a doplnené sieťové služby
9.5	24.9. 2018	odmazané odkazy na sieť 172.16.0.0/12, pridaná informácia o novom proxy serveri newproxy.gov.sk, doplnené bezpečnostné požiadavky na uzol
9.4	8.3. 2017	doplnené verzionovanie, čísla strán, drobné upresnenia
9.3	20.2. 2017	zmenená IP adresa na SPAM karanténu (prístup je sprostredkovaný cez WAF)

Obsah

Obsah	1
Technické požiadavky na uzol.....	1
Všeobecné požiadavky	2
Pravidlá pre IPv4 adresáciu.....	2
Pravidlá pre IPv6 adresáciu.....	2
Konfigurácia proxy	2
Konfigurácia mailov	2
Konfigurácia DNS.....	3
Integrácia do UPVS, e-kolkov	3
Bezpečnostné požiadavky na uzol	3
Kontakty	5
Úvod do siete Govnet - informácia pre uzly.....	5
Typický spôsob využitia siete Govnet	7
Štandardné nastavenia.....	7
Webová stránka	8
Iná komunikácia mimo siete Govnet.....	8

Technické požiadavky na uzol

Uzlu siete Govnet pri pripájaní prideliť IP adresy z rôznych rozsahov, najmä z rozsahu Govnet-internet (/25 IPv4 adresy a typicky /48 IPv6 adresy)

Všeobecné požiadavky

- Pre zriadenie nového Govnet uzla je potrebné zo strany žiadateľa o pripojenie zabezpečiť housing vo svojej technologickej miestnosti. Presná špecifikácia parametrov housingu závisí od požiadaviek žiadateľa. Jedná sa predovšetkým o zabezpečenie:
 - asistovaného vstupu do technologickej miestnosti s dostatočným voľným miestom v RACKu
 - zálohovaného napájania s potrebným príkonom
 - vykáblovanie pripojenia smerom na infraštruktúru žiadateľa
- uzol musí mať vlastný e-mailový server
- uzol musí používať DNS servery, proxy servery, e-mailové servery siete Govnet
- Uzol musí mať vlastný DNS server pre Govnet
- webové sídlo uzla musí patriť do domény .gov.sk
- uzol musí mať zriadenú e-mailovú adresu govnet@menouzla.gov.sk, nasmerovanú na relevantný technický kontakt
- uzol musí NASES-u oznámiť aktuálne technické, administratívne a bezpečnostné kontakty a priebežne ich aktualizovať

Pravidlá pre IPv4 adresáciu

- 0-7 infraštruktúra (routr Govnet, routr uzol)
- 8-15 DNS servery
- 16-23 mail servery
- 24-31 VPN koncentrátoary

- uzol musí do siete Govnet routovať celý rozsah 100.64.0.0/10
- uzlu odporúčame udržiavať informácie o pridelených IP adresách v aplikácii <https://ipv6.gov.sk>

Pravidlá pre IPv6 adresáciu

- uzol musí do siete Govnet routovať celý IPv6 adresný rozsah, ktorý je pridelený pre sieť Govnet
- uzlu odporúčame udržiavať pridelené sieťové alokácie v aplikácii <https://ipv6.gov.sk>

Konfigurácia proxy

- Povolit' komunikáciu:
 - wsa.gov.sk port 3128 - použiť doménové meno, súčasná adresa 100.64.16.190:3128 sa môže v budúcnosti zmeniť
 - newproxy.gov.sk port 3128 - použiť doménové meno, súčasná adresa 100.64.16.55:3128 sa môže v budúcnosti zmeniť

Konfigurácia mailov

- Povolit' prijímanie mailov z centrálnych mailových severov v sieti Govnet 2
 - ng2inmail.gov.sk - 100.64.16.30
 - 100.112.0.16 s bitovou maskou (nie sieťová maska) 0.15.255.7 - mailové servery uzlov v Govnet 2

- Povolit' odosielanie mailov na poštové servery podľa individuálneho plánu pre uzol - niektoré z uvedených:
 - ng2inmail.gov.sk (mail.gov.sk) - 100.64.16.30
 - 100.112.0.16 s bitovou maskou (nie sieťová maska) 0.15.255.7 - mailové servery uzlov v Govnet 2
- Povolit' HTTPS komunikáciu cez port 443 do SPAM karantény:
 - ng2karantena1.gov.sk, ng2karantena2.gov.sk - 100.112.0.126

Konfigurácia DNS

- DNS server na uzle musí robiť iteratívny lookup v rámci siete Govnet a rekurzívny lookup do internetu cez nadradené DNS servery Govnetu:
 - g2nsg1.gov.sk - 100.64.16.8
 - g2nsg2.gov.sk - 100.64.16.9
- MX záznamy pre uzol:
 - s vyššou prioritou - uzlový mailový server
 - s nižšou prioritou - g2inmail.gov.sk, ako záložná cesta v prípade nedostupnosti niektorého uzlového servera

Integrácia do UPVS, e-kolkov

- nevyhnutné podmienky:
 - IPsec VPN tunel do UPVS, e-kolkov
 - uzol používa na komunikáciu VPN koncentrátor z rozsahu 100.112.X.0/25. Tento rozsah sa nepoužíva na priamy prístup k poskytovaným službám.
 - každá organizácia má vyhradený tunelový koordinovaný adresný rozsah, ktorý sa používa iba vo VPN tuneloch a nie je v Govnet-e routovaný. Tento rozsah sa používa na prístup k poskytovaným službám.

Bezpečnostné požiadavky na uzol

- Webové aplikácie v sieti Govnet
 - Webové aplikácie by mali byť realizované rovnakým spôsobom, ako v prípade nasadenia webovej stránky do serverovej farmy NASES - statickým exportom hostovaným v NASES, typicky štruktúrovaným pomocou dynamického webu aj s manažmentom a statickou kópiou webu.
 - ***Dynamický web*** je preferované hostované na samotnom uzle, ale voliteľne tiež v NASES vedľa statického webu. Je hostovaný na samostatnom URL, odlišnom od publikovaného verejného URL.
 - Dynamický web generuje stránku obvyklým "dynamickým spôsobom"
 - Všetky lokálne URL sú "SEO friendly" a relatívne. Nikdy nie absolútne. URL neobsahuje otázniky.
 - Jazyk je kódovaný v URL.
 - Vyhľadávanie je vyriešené cez browser-side knižnicu a JSON index stránky (dynamicky generovaný podľa aktuálneho obsahu redakčného systému na statickom URL).

- Štatistika je riešená cez externú službu.
 - Dynamický web je prístupný len z vybraných IP adries, hostovaný buď u zákazníka na Govnet uzle (preferované), alebo v NASES. Dynamický web nie je viditeľný z Internetu.
 - ***Statický web*** je vytvorený automaticky rekurzívnym sťahovaním z dynamického webu, napríklad každých 15 minút. Táto statická kópia je prekopírovaná na webhosting NASES.
 - Statický web neobsahuje manažment a ani žiadne dynamické skripty.
 - V prípade, že je potrebné riešiť kontaktný formulár, rieši sa buď vnorením externej služby, alebo pridaním jedného dobre zauditovaného dynamického skriptu, na ktorý sa odkazuje web.
- Pre obmedzenie a zníženie rizika je potrebné vykonávať penetračné testy na webové aplikácie v sieti Govnet. Tieto penetračné testy môžu byť vykonávané:
 - Treťou stranou - v tomto prípade je potrebné dodržiavať formát oznamovania penetračných testov.
 - Službu penetračných testov vykonáva aj GOV CERT SK (<https://www.cert.gov.sk>)
 - V oboch prípadoch je potrebné zaslať požiadavku oficiálnou cestou na GOV CERT SK.
 - V záujme najrýchlejšej reakcie na bezpečnostný incident si GOV CERT SK vyhradzuje právo na testovanie zraniteľností zo zachytených incidentov na cieľi v sieti Govnet. Týmto spôsobom zabezpečuje GOV CERT SK aktívnu kontrolu nad cieľom a jeho potenciálnou kompromitáciou.
 - Uzol je povinný nahlasovať bezpečnostné incidenty a proaktívne kooperovať pri jeho riešení na nasledujúce kontakty:
 - web: **cert.gov.sk**
 - email: **incident@cert.gov.sk**
 - tel.číslo: **+421 2 3278 0780**

Kontakty

Uzol môže kontaktovať prevádzkovateľa siete Govnet niektorým z týchto spôsobov:

- tiketovým systémom na adrese <https://servicedesk.gov.sk/> (povinný spôsob pre zadávanie nových požiadaviek a change requestov)
- e-mailom na govnet@nases.gov.sk (všeobecné informácie, havarijné stavy a podobne)
- telefonicky na čísle je +421 (0)2 3278 0780 (urgentné hlásenie havarijných stavov)

Úvod do siete Govnet - informácia pre uzly

Sieť Govnet, ktorá je budovaná už od roku 1993, prepája desiatky uzlov štátnej správy (medzi inými ministerstvá, Úrad Vlády, Kanceláriu Prezidenta a ďalšie) a poskytuje im širokú škálu služieb vrátane privátneho - od internetu nezávislého - vzájomného prepojenia, verejného pripojenia k internetu, služieb web hostingu, server housingu, antivírusovú a antispamovú ochranu.

Jedným z hlavných dizajnových motívov siete Govnet je umožniť využitie sieťových služieb bez závislosti od akejkoľvek externej infraštruktúry, čo umožňuje garantovať spojenie v akejkoľvek situácii a nastoľuje jednoduchý spôsob identifikácie a odstraňovania problémov. Z tohto pohľadu sa Govnet nechápe ako poskytovateľ pripojenia do Internetu, ale ako poskytovateľ prepojovacej sieťovej infraštruktúry, ktorý:

- definuje jednotný adresný plán (evidovaný v aplikácii <https://ipv6.gov.sk/>),
- definuje pravidlá využívania častí adresného plánu jednotlivými uzlami a sprostredkúva ich vzájomné prepojenie,
- prevádzkuje technické zariadenia nevyhnutné pre plnohodnotné fungovanie, ako napr. vnútorné servery DNS (g2nsg1, g2nsg2),
- prevádzkuje pridané služby siete Govnet,
- vykonáva pokročilý prevádzkový a bezpečnostný monitoring siete, jej údržbu. Spolupracuje s uzlami pri využívaní a rozvoji siete a pri riešení bezpečnostných incidentov

Ďalším z dizajnových motívov siete Govnet je bezpečnosť a spoľahlivosť, ktorá je zahrnutá v návrhu siete, a tiež v procesoch a postupoch jej využívania. Za časť týchto procesov je zodpovedný prevádzkovateľ siete Govnet, za ďalšiu časť sú zodpovedné jednotlivé uzly. Za tým účelom uzly môžu využívať a/alebo musia dodržiavať:

- tiketový a dohľadový systém
- telefonické a e-mailové kontakty
- pravidlá pre správne využitie komunikačnej siete, z ktorých časť je formalizovaná v priebežne aktualizovanom verejnom dokumente "Požiadavky na uzol" (napr. rozdelenie rozsahu pre routre, VPN koncentrátory, mail servery, ostatné servery, kvôli jednotným firewallovým pravidlám naprieč sieťou Govnet), časť je súčasťou interných postupov a s uzlom sa komunikujú v rámci riešenia jednotlivých tiketov (napr. nepovoľujú sa priame spojenia zo siete Internet a podobne)
- komunikácia medzi uzlami musí byť realizovaná prostredníctvom siete Govnet

Sieť Govnet poskytuje tiež centrálné služby s pridanou hodnotou ako napríklad:

- bezpečnú e-mailovú komunikáciu
- bezpečný prístup na web
- IP telefóniu
- prepojenie do Internetu
- NTP
- Vytváranie Virtual Private Network

Keďže sieť govnet „G2“ je stavaná už s ohľadom na podporu MPLS, je možné pri požiadavke zákazníka o vytvorenie VPN siete v rámci prostredia Govnet tuto požiadavku zrealizovať. V súčasnosti je celá produkčná komunikácia vygenerovaná Govnet uzlami smerovaná do týchto VPN: govnet, inet, iptv, voice, testa, wifi. Každá jedna požiadavka govnet uzla o vytvorenie VPN bude samostatne posudzovaná.

- Poskytnutie IPv6 adresného rozsahu
Prevádzkovateľovi siete Govnet - NASES-u boli spoločnosťou RIPE prenajaté IPv6 adresne rozsahy, z ktorých je možné poskytnúť Govnet uzlu ucelený adresný rozsah.
- Služby IPTV
Pri poskytovaní služieb IPTV je NASES len v pozícii sprostredkovateľa IP konektivity medzi koncovými stanicami (Set-top Box) a poskytovateľom programovej ponuky (kontentu) spoločnosti SWAN.
- Host'ovský internet
Pri potrebe Govnet uzla mať k dispozícii (napr. pre svojich zamestnancov a klientov v priestoroch uzla) prístup čisto len do internetu, ktorý je oddelený od produkčných privátnych dát, je možné poskytnúť takúto konektivitu do internetu. Jedna sa o neobmedzenú konektivitu čo do objemu sťahovaných dát i čo do rýchlosti (tá však závisí od rýchlosti Govnet linky, ktorou je uzol pripojený do Govnet-u).
- Vzdialené pripojenie do siete Govnet cez FortiVPN pripojenie:
Vzhľadom k prísnej bezpečnostnej politike v prostredí siete Govnet, jediným riešením zabezpečenia prístupu pre externých dodávateľov a správcov k informačným systémom na jednotlivých OVM je zriadiť VPN pripojenie. Prístup je generovaný na konkrétneho človeka. Nie je možný súčasný viacnásobný prístup cez jeden účet.
- Sledovanie štatistík vyťaženia Govnet linky
Pre potreby mať informácie o vyťažení pripojenia do govnetu je možné zriadiť prístup do monitorovacieho systému. Štatistiky je možné prezerať v takmer ľubovoľne zvolenom časovom rozsahu.

Služby sú poskytované centrálné. To výrazne zvyšuje efektivitu prevádzky týchto služieb v prostredí verejnej správy. Napríklad prevádzkovaním jedného AV/AS riešenia namiesto viacerých, prípadne jednotným obstaraním spoločného pripojenia do siete Internet.

Pripojenie siete Govnet do Internetu a do iných sietí je redundantne realizované v prepojavacích bodoch prostredníctvom sady DMZ sietí GOVNET Edge, ktoré obsahujú perimetrové ochranné prvky, aplikačné firewally a aplikačné proxy pre jednotlivé protokoly:

- webový proxy cluster: wsa.gov.sk, newproxy.gov.sk
- edge DNS sever: g2ns1.gov.sk, g2ns2.gov.sk (uzly ich využívajú sprostredkované pomocou vnútorných DNS serverov g2nsg1.gov.sk a g2nsg2.gov.sk)
- webový aplikačný firewall F5 - ASM na spojenia z internetu do Govnet-u, ak uzol využíva službu ochrany prichádzajúcich spojení
- mailovú farmu: mail.gov.sk (uzly ju využívajú pomocou vnútorných adres)

Sieť Govnet má centrálny prevádzkový a bezpečnostný dohľad v podobe dohľadového pracoviska a ďalšieho automatizovaného softvéru.

Všetky prvky Govnet Edge, vrátane upstream liniek do SIX a do Internetu a tiež väčšina pripojení uzlov (podľa typu uzlu), sú budované redundantne s vylúčením single point of failure na fyzickej, sieťovej aj aplikačnej úrovni.

Typický spôsob využitia siete Govnet

Typické využitie siete Govnet uzlom je nasledovné (príklad je len pre ilustráciu, konkrétne a aktuálne pravidlá je možné nájsť v dokumente "Požiadavky na uzol"):

Štandardné nastavenia

- uzol dostane od Govnet-u adresný rozsah napr. 100.112.500.0/25 a subdoménu .gov.sk, typicky ministerstvoXYZ.gov.sk.
- uzol si na tomto rozsahu nastaví jednotlivé zariadenia, najmä DNS server a mail server
- DNS server poskytuje informácie o doméne ministerstvoXYZ.gov.sk pre ostatné uzly siete Govnet. Tento DNS server bude vždy oznamovať **adresy z Govnetového rozsahu 100.112.500.0/25**, napr.:
 - mail.ministerstvoXYZ.gov.sk IN A 100.112.500.16 ,
 - vpn1.ministerstvoXYZ.gov.sk IN A 100.112.500.24,
 - www.ministerstvoXYZ.gov.sk IN A 100.112.500.32.

TENTO DNS SERVER NIKDY NEPOSKYTUJE VEREJNÉ INTERNETOVÉ ADRESY.

- uzol nastaví svoj DNS resolver tak, aby resolvoval domény v .gov.sk priamo a všetky ostatné dopyty posielal na nadradený server g2nsg1.gov.sk, g2nsg2.gov.sk. Až tieto DNS servery spracujú rekurzívny lookup do Internetu prostredníctvom dopytov na ďalšie servery v Govnet Edge.
- odchádzajúce webové spojenia z uzla sú sprostredkované cez proxy servery wsa.gov.sk alebo newproxy.gov.sk

Webová stránka

- uzol si môže vytvoriť webovú stránku www.ministerstvoXYZ.gov.sk. Táto stránka **nemôže byť prevádzkovaná mimo siete Govnet**. Musí byť prevádzkovaná v rámci interného IP adresného rozsahu siete Govnet. Napríklad na IP adrese 100.112.500.32. Dôvodom je, aby bola vždy dostupná pre ostatné uzly siete Govnet.
- Ak má byť stránka dostupná z verejného Internetu, uzol požiada o NAT cez tiketový systém. Zároveň prevádzkovateľ siete Govnet zavedie záznamy s verejnými adresami do verejného DNS pre doménu .gov.sk. Tento DNS spravuje prevádzkovateľ siete Govnet.
- Uzol si voliteľne vyžiada od prevádzkovateľa siete Govnet, aby dohľadové centrum siete Govnet zabezpečilo bezpečnostnú kontrolu prichádzajúcich spojení na uzlový web server prostredníctvom webového aplikačného firewallu (WAF), umiestneného v Govnet Edge. Táto ochrana vyžaduje, aby v sieti Govnet bol nainštalovaný TLS certifikát uzlovej webovej stránky (TLS certifikát LetsEncrypt na požiadanie zabezpečí NASES). To umožňuje bezpečnostnému prvku WAF nahliadnuť do obsahu komunikácie. Očistená komunikácia je na vnútorný server opäť smerovaná šifrovaným protokolom TLS.

Iná komunikácia mimo siete Govnet

- Ak chce uzol komunikovať s iným uzlom, alebo s adresou v Internete, požiada prevádzkovateľa siete Govnet cez tiketový systém o povolenie firewallových pravidiel s uvedením protokolu, konkrétnych zdrojových a cieľových IP adries a portov.
- Tieto žiadosti sa akceptujú len od poverených kontaktných osôb na uzloch, nie od ich subdodávateľov.
- Žiadosti podliehajú schvaľovaniu podľa internej metodiky. Typicky sú zamietnuté žiadosti o povolenie prichádzajúcej komunikácie z Internetu na port 25=smtp (pretože je potrebné využívať AV/AS farmu v Govnet Edge), 22=ssh (pretože uzol má pre svojich dodávateľov vybudovať VPN prístup), žiadosti s príliš širokými neopodstatnenými pravidlami, žiadosti podané za iný uzol (komunikácia medzi uzlami musí byť odsúhlasená kontaktnými osobami oboch strán).
- Prevádzkovateľ siete Govnet, ak to situácia vyžaduje, môže požiadať uzly o revíziu starých pravidiel a potvrdenie, že majú naďalej platiť. Ak uzol na požiadanie nedodá potvrdenie o platnosti pravidiel, NASES si vyhradzuje právo na ich zrušenie.
- Domény iné ako .gov.sk:
Uzol môže mať voliteľne aj doménu ministerstvoXYZ.sk hostovanú v sieti Govnet. Môže ju prevádzkovať buď u seba, alebo využívať komplexné služby prevádzkovateľa siete Govnet vrátane registrácie domény.