

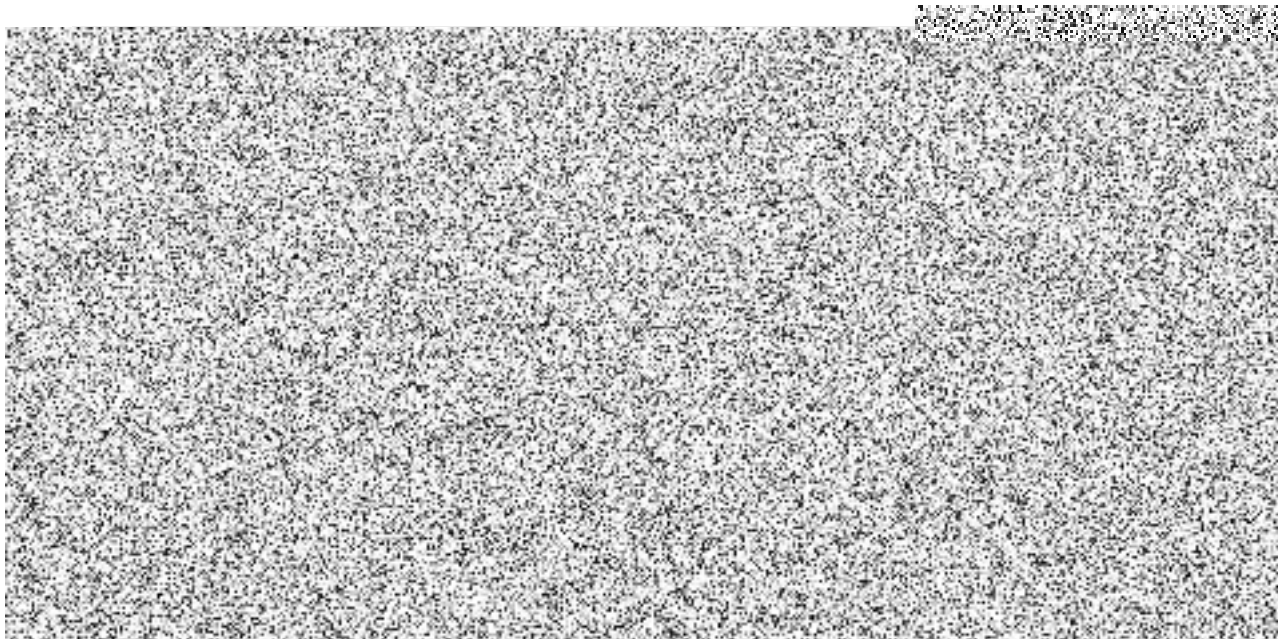
PŘÍLOHA Č. 8 SMLOUVY

Technická specifikace pro realizaci propojení do InterConnectu CMS

1) Podmínky propojení sítě Poskytovatele do InterConnectu CMS

Poskytovatel je povinen zřídit a provozovat propojení své sítě do InterConnectu CMS za následujících podmínek:

1. Redundantní připojení dvěma nezávislými optickými spoji do lokalit s instalovanými zařízeními InterConnect CMS – viz následující obrázek. Poskytovatel musí mít do obou lokalit InterConnectu CMS optickou trasu umožňující realizaci propojovacích služeb.



Lokality se směrovači InterConnect CMS.

Lokalita	Adresa
IC-1	Na Vápence 915/14, Praha 3
IC-2	Sazečská 598/7, Praha 10

2. Propojení mezi směrovačem InterConnectu CMS a směrovačem ASBR Poskytovatele bude realizováno spojem na bázi technologií Gigabit Ethernet (IEEE802.3z) nebo 10Gigabit Ethernet (IEEE802.3ae). Rozhraní musí podporovat tagování VLAN dle 802.1Q, jednotlivé VPN budou předávány formou jednotlivých VLAN. Poskytovatel musí být schopen zajistit do 1 kalendářního měsíce od odeslání požadavku Ministerstva upgrade na 10Gigabit Ethernet (IEEE802.3ae).
3. Fyzické rozhraní pro předání využívá optickou trasu Single Mode nebo Multimode s konektorem LC/PC na straně optického patch panelu.
4. Vlastní připojení k CMS a potřebné nastavení zajišťuje Poskytovatel. Poskytovatel předá provozovateli CMS, jímž je Národní agentura pro komunikační a informační technologie, s.p., (dále jen „**Provozovatel CMS**“) provozní řád včetně kontaktních údajů pro nahlašování poruch. Poskytovatel musí prokázat schopnost spolupráce se ServiceDeskem CMS; pro tyto účely může být pracovníky Provozovatele CMS požádán o test komunikace a test komunikace IP VPN MPLS.

5. Propojení Poskytovatele a směrovačů InterConnect CMS předpokládá využití technologie MPLS VPN na straně Poskytovatele i CMS, propojení je pak realizováno dle RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs), sekce 10 Multi-AS Backbones, varianta A VRF-to-VRF connections at the AS (Autonomous System) border routers.
6. Směrovací informace protokolu IPv6 budou přenášeny samostatným BGP spojením v adresním prostoru IPv6 (dual-stack) dle RFC 4659.
7. Směrovací informace mezi propojovací sítí CMS a jednotlivými poskytovateli datové konektivity jsou předávány pomocí směrovacího protokolu eBGP dle RFC 4760 Multiprotocol Extensions for BGP-4.
8. Adresní rozsahy IPv4 spojnic KIVS spravuje, koordinuje a Poskytovateli přiděluje Provozovatel CMS.
9. Adresní rozsahy IPv6 spojnic KIVS spravuje, koordinuje a Poskytovateli přiděluje Provozovatel CMS.
10. Poskytovatel musí v případě potřeby zajistit, aby celá jím poskytovaná komunikační infrastruktura KIVS byla schopna jednotného řízení kvality služby (End-to-End QoS). Operátor zajistí přepis značek do DSCP PE-CE, tzv. " pipe" tunelovací režim MPLS, v němž je při průchodu MPLS páteří zachovávána původní hodnota DSCP transportovaných IP paketů (DSCP transparency).
11. Infrastruktura Poskytovatele musí v případě potřeby umožnit Provozovateli CMS sběr a vyhodnocování provozních statistik KIVS a poskytnout jeho dohledovému systému informace na bázi SNMP, syslog a Netflow.

2) Požadavky ASBR směrovače Poskytovatele

Směrovače Poskytovatele musí být vybaveny redundantním napájením v režimu minimálně N+1 a musí být vybaveny duální řídicí logikou v rámci jednoho šasi. Směrovače musí být vybaveny funkcí přepnutí řídicích jednotek bez ukončení sousedství směrovacích protokolů. Směrovače musí být postaveny na neblokující architektuře wire-speed portu. Směrovače musí směrovat bez dopadu na výkonost tzv. směrování v HW (směrování v ASIC). Poskytovatel zpřístupní přes protokol SNMP v2 nebo SNMP v3 přístup jen ke čtení s maximální periodicitou 1x za 10 Min pro účely diagnostiky.

3) Požadavky na koncové CPE

Z důvodů schopnosti monitorovat kvalitu linky a možnosti zabezpečení Služby pomocí IPSEC VPN je třeba zajistit následující požadavky na CPE zařízení. CPE musí umožnit zabezpečené připojení do CMS 2.0 přes Poskytovatele. CPE musí být bezpečnostní zařízení nabízející zónový firewall, překlad IP adres (NAT), IPsec VPN, IKEv2, podpora stavového firewallu pro IPv4 i IPv6. Musí umět možnost přepnutí do směrovacího režimu bez stavového firewallu na WAN portu. Pro VPN musí umět autentizaci pomocí Pre-shared klíče nebo Certifikátu vydaného kvalifikovanou certifikační autoritou. Požadovaná je podpora Route Base IPsec VPN. IPsec tunely musí podporovat minimálně sadu bezpečnostních funkcí. Všechny uvedené požadavky týkající se bezpečnosti vyplývají z právních předpisů (zejm. zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) a související právní předpisy),

Ze směrovacích protokolů je požadován minimálně protokol OSPFv2, OSPFv3, BGP, IS-IS s podporou pro IPv4 i IPv6, RIPv2, RIPv6. Zařízení CPE musí umět Real-time Network Monitoring na úrovni měření ztrátovosti, latence, stability.

Výkonnost prvku bude dle lokality a typu dle KL a to včetně IPSEC VPN.

4) Provozní podmínky zřízení služby přístupu k Interconnectu CMS

Poskytovatel na vlastní náklady zpracuje realizační projekt (dále jen „RP“) konektivity. RP musí být zpracován jak v případě zajištění konektivity vlastním kabelem Poskytovatele, tak i v případě pronájmu optických vlnových délek od jiných poskytovatelů služeb KIVS. RP musí obsahovat textovou a výkresovou část řešící konektivitu do Interconnectu CMS včetně souhlasu Ministerstva, případně i vlastníka objektu (v případě lokality Sazečská 598/7, Praha 10) s uložením v kabelovodu, průběhem trasy v objektu, i mimo objekt (až po ASBR Router Poskytovatele) zakončením optického kabelu v technologické místnosti – alokace místa ve stojanu pro zakončení optického kabelu případně umístění nového stojanu.

RP se musí řídit následující osnovou:

Realizační projekt stavby

Název akce: Napojení objektu Na Vápence, Sazečská

Místo stavby: Praha

Investor:

Dodavatel:

Technická zpráva musí minimálně obsahovat:

- Profil a typ optického kabelu, optické konektory
- Instalace a montáž optického kabelu
- Optické spojky:
- Trasa a ukončení optického kabelu
- Způsob nakládání s odpady
- Vliv stavby na životní prostředí:
- Bezpečnost práce a protipožární ochrana
- Užívání veřejného prostranství
- Řešení autorského dozoru
- Dokumentace návrhu řešení

RP musí být schválen Ministerstvem; Provozovatel CMS zpracuje stanovisko k RP.

Ukončení kabelů zajistí na vlastní náklady Poskytovatel ve vlastních optických patch panelech maximálně 2U.

Poskytovatel dodá optické patch cordy dle konektorů v propojovací místnosti (na straně Ministerstva konektor LC/PC), stejně tak patch cord pro konektivitu do CMS (LC/PC-LC/PC).

Poskytovatel se dále zavazuje dodat SFP nebo XFP modul dle specifikace Provozovatele CMS.

Poskytovatel zajistí funkčnost celé trasy až po cílové optické moduly v Interconnectu CMS. Funkčnost trasy bude doložena provedením OTDR měření z lokality IC CMS až aktivním prvkům Poskytovatele, nebo v případě využití WDM technologie odpovídajícím měřením propustnosti využití vlnové délky. V případě použití transportní sítě, založené na technologii Ethernet, bude měření provedeno dle RFC2544.

Konfigurace IP connectivity a autonomního systému Poskytovatele na rozhraní k CMS; tj., BGP peering, bude prováděna dle specifikace Provozovatele CMS.

Poskytovatel se zavazuje do CMS šířit (propagovat) pouze routy specifikované Provozovatelem CMS a na své straně neprovádět jakoukoli manipulaci s adresami subjektů (NAT, Pat, apod.), kteří nejsou uživateli služeb CMS, tj. zabránit přístupu ke službám CMS neoprávněným osobám.

Požadavky na zřízení, změny a zrušení služeb spojených s konektivitou do CMS předkládá Pověřující zadavatel připojený přes Poskytovatele standardní cestou na Ministerstvo prostřednictvím technické specifikace, a to v rozsahu aktuálně platného katalogu služeb CMS.

Poskytovatel bere na vědomí a souhlasí, že služba InterConnect CMS se nepovažuje za nedostupnou, pokud je nedostupnost způsobena okolnostmi vylučujícími odpovědnost nebo z důvodu neplnění provozních podmínek ze strany Poskytovatele. Za okolnost vylučující odpovědnost se kromě okolností dle obecné právní úpravy považuje také vyhlášení mimořádného nebo výjimečného stavu nebo požadavek Ministerstva na omezení nebo dočasné zrušení přístupu k CMS z důvodu ohrožení bezpečnosti.

Poskytovatel se dále zavazuje provádět ochranu před útoky DDoS a ostatními známými hrozbami ze svých sítí (např. monitoringem poskytovaných služeb). V případě, že k takovému útoku dojde, je Provozovatel CMS oprávněn odpojit bez náhrady Poskytovatele od systému CMS do doby odstranění bezpečnostní hrozby, která vznikla na straně tohoto Poskytovatele. V takovémto případě je odpovědnost na straně Poskytovatele a případné smluvní pokuty za nedodržení SLA a vícenáklady na straně Provozovatele CMS i Pověřujících zadavatelů hradí Poskytovatel.

Požadavky na změnu operátorského rozhraní/prostředí předkládá Poskytovatel Provozovateli CMS současně s předběžným souhlasem Pověřujících zadavatelů, kteří jsou jeho přípojkami do CMS připojeni a souhlasu odpovědného zástupce Ministerstva. Požadavek je zadán 3 měsíce před požadovanou změnou.

Informace o plánovaném provozním výpadku poskytované služby musí Poskytovatel prokazatelně doručit na odpovědné pracoviště Ministerstva – DCEGOV (dále jen „**DCEGOV MV**“), a to minimálně 30 dní před plánovaným výpadkem.

Informace o závadách, výpadcích a chybovosti služby je Poskytovatel povinen neprodleně poskytnout DCEGOV MV spravovanému Provozovatelem CMS. Kontaktní údaje: mail  telefon



Poskytovatel musí poskytovat službu HelpDesk/ServiceDesk (dále jen „**HD/SD**“), a to s dostupností 24x7. Poskytovatel předloží detailní popis procesů jeho HD/SD.

Veškerá komunikace spojená s odstraňováním poruch, výpadky a chybovostí Služeb musí být realizována prostřednictvím DCEGOV MV a HD/SD Poskytovatele, a to dle stanovených procesů.

Poskytovatel musí definovat rozhraní loopback pro ověření konektivity na straně Poskytovatele, a to pro každou jednotlivou službu poskytovanou Pověřujícím zadavatelí.

Do prostředí CMS není Poskytovateli poskytován dálkový přístup, a to ani pro ověření konektivity