MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

eGovernment Cloud

Bezpečnostní certifikace zapsané nabídky cloud computingu v katalogu cloud computingu pro jednotlivé bezpečnostní úrovně

Identifikace a popis kritéria ex-ante kontroly	Regulace/norma	Bezpečnostní úroveň, ve které je kritérium aplikováno			Způsob ověření	Realizace
		N (1)	S (2)	V (3)		
Sm1 - Součástí smluvních podmínek je SLA, zahrnující úroveň dostupnosti (vazba na SAZ, přílohu č. 5 *Minimální smluvní podmínky* a přílohu č. 4 *Metodika hodnocení bezpečnostních dopadů*)	ČSN ISO/IEC 27001 A.15	96,16%	99,45%	99,90%	Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele	Citace ze standardně nabízené SLA (která je součástí smluvní dokumentace), kde se poskytovatel zavazuje k úrovni dostupnosti, která je rovna nebo lepší než hodnoty v dané bezpečnostní úrovni, a to dle bližší specifikace v Příloze 5 SAZ, kap. 2.1. Dále citace ze smlouvy nebo citace a link na obecné podmínky o podpoře služby, a to minimálně s uvedením denní doby podpory, s úrovněmi nabízené podpory a s prioritizací incidentů dle Přílohy 5 SAZ, kap. 2.2.
Sm2 - Smlouva obsahuje závazek účinného zavedení bezpečnostních opatření v rozsahu dané bezpečnostní úrovně	ČSN ISO/IEC 27001 A.15; ZoISVS §5b; VKB Příloha 7 bod a).	X	X	X	Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele	Citace ze smluvních podmínek, uvádějící závazek zavedení bezp. opatření, která odpovídají rozsahu opatření dané bezp. úrovně. Pro BÚ 2 a 3: Účinnost těchto opatření musí být ověřena auditními zprávami podle mezinárodních standardů, uvedených dále v těchto kritériích.
Sm3 - Smlouva uvádí způsob poskytnutí informací o zavedených bezpečnostních opatřeních	ČSN ISO/IEC 27001 A.15, ZoISVS §5b	X	X	X	Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele	Citace smluvních podmínek poskytovatele, uvádějící informaci, resp. odkaz na podrobnější dokumentaci, jakým způsobem jsou bezpečnostní opatření realizována. Přístup k této informaci může být podmíněn uzavřením NDA.
Sm4 - Smluvní podmínky jsou v souladu s požadavky na zpracovatele dle čl. 28 Obecného nařízení GDPR, včetně pravidel pro zákaznický audit.	GDPR čl. 28 – Zpracovatel; zejména pak bod 3 h) a dále VKB Příloha 7 bod d).		X	X	Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele	Citace smluvních podmínek poskytovatele, která prokazuje soulad s požadavky na zpracovatele dle čl. 28 nařízení GDPR. Smluvní podmínky poskytovatele musí zahrnovat umožnění zákaznického auditu v souladu s čl. 28 bod 3 h), resp. VKB Příloha 7 bod d).
Sm5 - Smlouva obsahuje povinnost informovat zákazníka eGC o bezpečnostních incidentech, týkajících se daného zákazníka eGC, a spolupracovat při jejich zvládání	ČSN ISO/IEC 27001 A.16.1.2; VKB č. 82/2018 Sb. Příloha 7 odst. i) bod 1.	X	X	X	Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele	Citace smluvních podmínek poskytovatele, obsahující povinnost informovat správce ISVS – zákazníka dané služby eGC o bezpečnostních incidentech, týkajících se daného zákazníka eGC. Rozsah definice bezpečnostního incidentu musí obsahovat ztrátu, znečitelnění (zničení) nebo neautorizovanou změnu (ztrátu integrity), nebo únik (vyzrazení – ztrátu důvěrnosti) zákaznických dat, včetně ztráty přístupu k těmto datům (ztrátu dostupnosti). Smlouva též musí obsahovat závazek vyšetřit bezpečnostní incident, poskytnout zákazníkovi podrobné informace o incidentu, a spolupracovat při jejich zvládání za účelem zmírnění následků resp. minimalizace škod.
Sm6 – Smlouva obsahuje povinnost materiálního dodavatele informovat zákazníka eGC v případech, kdy o vydání zákaznických dat požádají orgány činné v trestním řízení, a to ve všech případech, kdy informování zákazníka není v rozporu se zákonem.		X	X	X	Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele	Citace smluvních podmínek poskytovatele, obsahující tento závazek.
Sm7 – Smlouva obsahuje povinnost poskytovatele dodržovat veškeré zákony a předpisy, které se vztahují k provozování služeb cloud computingu v segmentu zákazníků veřejné správy.		X	X	X	Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele	Citace smluvních podmínek poskytovatele, obsahující tento závazek.
Sm8 – Standardní smlouva prodejce není v rozporu s minimálními smluvními podmínkami - viz Příloha 4.	Příloha 4.	X	X	X	Akceptace podmínek poskytovatelem; smluvní povinnost pro zadavatele	
ID1 - Poskytovatel má sídlo nebo bydliště v členském státě EU/EHS nebo má určeného svého zástupce ve členském státě EU obdobně dle čl. 27 GDPR.		X	X	X	Předložení dokumentu	Výpis z obchodního rejstříku nebo obdobné zahraniční evidence, nebo písemné čestné prohlášení v rozsahu údajů obsažených v obchodním rejstříku v případě, že není v obchodním rejstříku zapsán
ID2 – Proti poskytovateli nebylo za posledních 5 let vydáno pravomocné rozhodnutí o spáchání přestupku dle zákona o kybernetické bezpečnosti.		X	X	X	Předložení dokumentu	Poskytovatel předloží čestné prohlášení statutárního zástupce organizace. Pro poskytovatele usazené v jiných zemích EU/EHS může být toto prohlášení vyhotoveno i statutárním zástupcem české dceřiné společnosti daného poskytovatele.

eGovernment Cloud

Identifikace a popis kritéria ex-ante kontroly	Regulace/norma	Bezpečnostní úroveň, ve které je kritérium aplikováno			Způsob ověření	Realizace
		N (1)	S (2)	V (3)		
ID3 – ČSN ISO/IEC 27001	Důvodová zpráva k VKB č. 82/2018 Sb., lze uvést i mapovací tabulku požadavků VKB na opatření ISO/IEC 27001. Schváleno rozhodnutím vlády v eGC SAZ kap. 6.2.2. Prošlo předběžnou tržní konzultací MV v červnu 2019.		X	X	Předložení dokumentu	1. Poskytovatel předloží certifikát ve formátu PDF, do jehož certifikovaného rozsahu náleží všechny posuzované služby cloud computingu. Rozsah certifikátu: certifikát se musí vztahovat na nabízené služby cloud computingu bez omezení; pokud certifikát obsahuje konkrétní výčet služeb cloud computingu, ale neobsahuje slovní spojení, které by výslovně omezovalo rozsah certifikace na přiložený výčet služeb, lze další služby cloud computingu stejné třídy, oblasti nebo typu, jako jsou uvedené na certifikátu doložit čestným prohlášením poskytovatele, že výčet služeb cloud computingu uvedený na certifikátu je vázán na datum provedení certifikace a další služby cloud computingu stejné třídy, oblasti nebo typu, které byly zavedeny a jsou poskytovány po datu vydání tohoto certifikátu, jsou podřazeny stejnému platnému systému řízení bezpečnosti informací poskytovatele, jehož soulad s mezinárodním standardem ISO/IEC 27001 byl vydaným certifikátem ověřen a jsou poskytovány z datových center poskytovatele, na které se vztahuje rozsah certifikátu. Pro poskytovatele usazené v jiných zemích EU/EHS může být toto čestné prohlášení vyhotoveno i statutárním zástupcem české dceřiné společnosti daného poskytovatele. Datum poslední revize na certifikátu nesmí být starší 15 měsíců (12 měsíců výročí plus 3 měsíce na dokončení auditních procesů). Po nouzových opatřeních (Covid-19) může tato doba poslední revize být výjimečně až 18 měsíců, pouze do 1/10/19, dále již standardně 15 měsíců. V případě vydání certifikátu s dobou platnosti delší než 12 měsíců předložit poslední auditní zprávu ne starší 15 měsíců (resp. 18 měsíců za podmínek výše) a jiným způsobem prokázat aktivní stav platnosti certifikátu dle podmínek příslušné certifikační organizace. Dále viz Poznámka 1 pod tabulkou (omezení rozsahu pro poskytovatele SaaS vyvíjeného na míru pro výkon veřejné správy. 2. Předložení SOA (Prohlášení o aplikovatelnosti) k certifikaci ČSN ISO/IEC 27001. 3. Předložení a auditní zprávy k certifikaci ČSN ISO/IEC 27001. Pro BÚ 2: předložit SOA a auditní zprávu k certifikaci, zahrnující všechny domény ISO/IEC 27001:2013 s výjimkou A10 a A14. Pro BÚ 3 a 4: předložit SOA a auditní zprávu k certifikaci, zahrnující všechny domény daného ISO standardu. Společnost provádějící certifikaci ISO/IEC 27001 musí mít akreditaci od akreditačního orgánu, který je členem IAF viz https://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4. Doložit výpisem z webu od koho má využitá certifikační společnost akreditaci, a zda je daný akreditační orgán uveden jako člen IAF.
ID4 - Deklarace minimálních bezpečnostních opatření pro BÚ 1		X			Předložení dokumentu	Předložení deklarace poskytovatele o zavedených bezpečnostních opatřeních a popis těchto bezpečnostních opatření minimálně v doménách ISO/IEC 27001:2013 A7, A9, A12, A13, A15, A16, A18 a to na úrovni požadavku tohoto standardu.
ID5 – ČSN ISO/IEC 27017	Schváleno rozhodnutím vlády v eGC SAZ kap. 6.2.2. Prošlo předběžnou tržní konzultací MV v červnu 2019.		X	X	Předložení dokumentu	1. Poskytovatel předloží certifikát ve formátu PDF (může být také rozšířením certifikátu ISO/IEC 27001), do jehož certifikovaného rozsahu náleží všechny posuzované služby cloud computingu. Pro Rozsah certifikátu platí totéž, co je uvedeno u ID-3. Datum poslední revize na certifikátu nesmí být starší 15 měsíců (12 měsíců výročí plus 3 měsíce na dokončení auditních procesů). Po nouzových opatřeních (Covid-19) může tato doba poslední revize být výjimečně až 18 měsíců, pouze do 1/10/19, dále již standardně 15 měsíců. V případě vydání certifikátu s dobou platnosti delší než 12 měsíců předložit poslední auditní zprávu ne starší 15 měsíců (resp. 18 měsíců za podmínek výše) a jiným způsobem prokázat aktivní stav platnosti certifikátu dle podmínek příslušné certifikační organizace. Dále viz Poznámka 1 pod tabulkou (omezení rozsahu pro poskytovatele SaaS vyvíjeného na míru pro výkon veřejné správy.) 2. Předložení SOA (Prohlášení o aplikovatelnosti) k certifikaci ČSN ISO/IEC 27001, zahrnující nebo uvádějící samostatně i rozsah dle ČSN ISO/IEC 27017. 3. Předložení auditní zprávy k certifikaci ČSN ISO/IEC 27001, zahrnující nebo uvádějící samostatně i rozsah dle ČSN ISO/IEC 27017.

eGovernment Cloud

Identifikace a popis kritéria ex-ante kontroly	Regulace/norma	Bezpečnostní úroveň, ve které je kritérium aplikováno			Způsob ověření	Realizace
		N (1)	S (2)	V (3)		
						Společnost provádějící certifikaci ISO/IEC 27017 musí mít akreditaci od akreditačního orgánu, který je členem IAF viz https://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4. Doložit výpisem z webu od koho má využitá certifikační společnost akreditaci, a zda je daný akreditační orgán uveden jako člen IAF.
ID6 – ČSN ISO/IEC 27018	Schváleno rozhodnutím vlády v eGC SAZ kap. 6.2.2. Prošlo předběžnou tržní konzultací MV v červnu 2019.		X	X	Předložení dokumentu	1. Poskytovatel předloží certifikát ve formátu PDF (může být také rozšířením certifikátu ISO/IEC 27001), do jehož certifikovaného rozsahu náleží všechny posuzované služby cloud computingu. Pro Rozsah certifikátu platí totéž, co je uvedeno u ID-3. Datum poslední revize na certifikátu nesmí být starší 15 měsíců (12 měsíců výročí plus 3 měsíce na dokončení auditních procesů). Po nouzových opatřeních (Covid-19) může tato doba poslední revize být výjimečně až 18 měsíců, pouze do 1/10/19, dále již standardně 15 měsíců. V případě vydání certifikátu s dobou platnosti delší než 12 měsíců předložit poslední auditní zprávu ne starší 15 měsíců (resp. 18 měsíců za podmínek výše) a jiným způsobem prokázat aktivní stav platnosti certifikátu dle podmínek příslušné certifikační organizace. Dále viz Poznámka 1 pod tabulkou (omezení rozsahu pro poskytovatele SaaS vyvíjeného na míru pro výkon veřejné správy.) 2. Předložení SOA (Prohlášení o aplikovatelnosti) k certifikaci ČSN ISO/IEC 27001, zahrnující nebo uvádějící samostatně i rozsah dle ČSN ISO/IEC 27018. 3. Předložení auditní zprávy k certifikaci ČSN ISO/IEC 27001, zahrnující nebo uvádějící samostatně i rozsah dle ČSN ISO/IEC 27018. Společnost provádějící certifikaci ISO/IEC 27018 musí mít akreditaci od akreditačního orgánu, který je členem IAF viz https://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4. Doložit výpisem z webu od koho má využitá certifikační společnost akreditaci, a zda je daný akreditační orgán uveden jako člen IAF.
ID7 – Auditní zpráva SSAE18 SOC 2 Type II (sledování po dobu min. 6 měsíců z roku, viz www.ssae-18.org)	Schváleno rozhodnutím vlády v eGC SAZ kap. 6.2.2. Prošlo předběžnou tržní konzultací MV v červnu 2019. Dále VKB §16			X	Předložení dokumentu	ODLOŽENÁ ÚČINNOST: toto kritérium bude účinné (tedy bude aplikováno) až od uplynutí 3 let od nabytí účinnosti probíhající novelizace ZoISVS projednávané v PS PČR (sněmovní tisk 756): Poskytovatel předloží celou auditní zprávu ve formátu PDF, v doménách Security, Availability, Processing Integrity, Confidentiality, Privacy. Pokud se jedná o službu typu SaaS vyvíjeného na míru jako ISVS (viz definice v ZoISVS § 2 písm. b)) využívající vrstvy IaaS nebo PaaS, které již tuto auditní zprávu mají, pak stačí doložit pouze auditní zprávu SSAE18 SOC 2 Type II na tyto podkladové vrstvy IaaS/PaaS (auditní zpráva SSAE 18 SOC 2 Type II se pro vrstvu aplikačního SW vyvíjeného na míru pro potřeby veřejné správy nevyžaduje).
ID8 – Zpráva o provedených penetračních testech (ne starší 3 let)	ČSN ISO/IEC 27001 A.18, A.12, VKB § 25			X	Předložení dokumentu	Poskytovatel předloží zprávu o penetračních testech: 1) v případě IaaS/PaaS dle standardu NIST SP 800-115, nebo dle standardu OSSTMM https://www.isecom.org/OSSTMM.3.pdf. 2) v případě SaaS se zahrnutím OWASP Top Ten zranitelností: https://owasp.org/www-project-top-ten/.
ID9 - Deklarace místa uložení zákaznických dat v rámci jurisdikce EU a ošetření případného předávání údajů do třetích zemí		X	X	X	Předložení dokumentu	Citace smluvních podmínek poskytovatele, uvádějící závazek místa trvalého uložení zákaznického obsahu (jako jsou databáze, dokumenty, obsahy emailů atd. včetně jejich záloh) v rámci jurisdikce EU/EHS. Pokud mohou nastat případy zpracování zákaznických dat mimo EU nebo EHS, poskytovatel tuto možnost deklaruje a doloží způsob zajištění bezpečnosti předávaných údajů do třetích zemí. Poskytovatel v Katalogu označí jako „globální CC“ takové služby CC, které kromě uložení zákaznických dat v jurisdikci EU/EHS mohou z funkčních důvodů ukládat a zpracovávat části zákaznického obsahu vícenásobně, a to i mimo jurisdikci EU/EHS (pozn. může se jednat např. o služby vyhledávání, jazykového překladu, nebo o služby pokročilého zabezpečení s korelací dat ze senzorů v globálním měřítku).
ID10 - Poskytovatel musí umožňovat synchronní replikaci dat alespoň do jednoho (jiného) záložního datového centra, které je z hlediska kapacity a zajištěné konektivity dostatečné k převzetí všech služeb, poskytovaných z primárního datového centra.	ČSN ISO/IEC 27001 A.11.1.4, A.12.3.1 VKB § 15, § 17			X	Předložení dokumentu	**Pro IaaS:** Poskytovatel doloží citací z auditní zprávy ISO 27001 nebo ISO 22301 nebo SSAE 18 SOC 2 Type II připravenost záložního datového centra, které je kapacitně dostatečné k převzetí všech služeb poskytovaných z primárního datového centra. **Pro PaaS:** deklarovat totéž pro ty služby PaaS, pro které je tento požadavek relevantní. Pro **SaaS**: Odkaz na technickou dokumentaci služby, která tuto schopnost popisuje.
ID11 - Primární i záložní datacentrum, které jsou využívány pro asynchronně udržované zálohy poskytované	ČSN ISO/IEC 27001 A.17.1.2, A.17.2.1 VKB § 15, § 17; Vzdálenost 50km: Zák. č. 499/2004 Sb.		X	X	Předložení dokumentu	Poskytovatel doloží citací z auditní zprávy ISO 27001 nebo ISO 22301 nebo SSAE 18 SOC 2 Type II, ze kterých musí být zřejmé umístění primárního a záložního datového

Identifikace a popis kritéria ex-ante kontroly	Regulace/norma	Bezpečnostní úroveň, ve které je kritérium aplikováno			Způsob ověření	Realizace
		N (1)	S (2)	V (3)		
služby, jsou umístěny nejméně 50 km od sebe.	§ 61 bod (2); Dále viz doporučení Advisera ISO 27001 Academy					centra (minimálně s uvedením katastrálního území či obce a země).
ID12 - Primární i záložní datové centrum se nacházejí buď obě v České republice nebo ve dvou různých státech EU (EHS).	Viz zdůvodnění v předchozím ID12.			X	Předložení dokumentu	Poskytovatel doloží citací z auditní zprávy ISO 27001 nebo ISO 22301 nebo SSAE 18 SOC 2 Type II, ze kterých musí být zřejmé umístění primárního a záložního datového centra (minimálně s uvedením katastrálního území či obce a země).
ID13 - Poskytovatel má vyhotoven plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu pro zajištění dostupnosti uvedené v bodě ID1	ČSN ISO/IEC 27001 A.17, VKB §15			X	Předložení dokumentu	Poskytovatel doloží svým Plánem zajištění kontinuity provozu a obnovy po havárii, který byl součástí certifikace ISO/IEC 27001 domény A.17 nebo certifikace ISO/IEC 22301, obojí s citací z příslušné auditní zprávy. Alternativně může doložit citací příslušných opatření ze zprávy SSAE 18 SOC 2 Type II. Každá taková auditní zpráva musí obsahovat kontrolní bod, podle kterého se provádí pravidelné testy výpadku provozního systému s přechodem zátěže do záložního nebo standby systému (tzv. Failover exercise).
ID14 – Poskytovatel má zaveden v rámci cloudových služeb systém sledování a vyhodnocování bezpečnostních událostí (např. SIEM) a umožní zpřístupnění prioritních událostí zákazníkovi	Umožnit správcům ISVS sběr a vyhodnocování kybernetických bezpečnostních událostí dle VKB § 24; Viz kontrolní bod A.12.4.1, lze doložit citací ze SSAE 18 SOC 2		X	X	Předložení dokumentu	Poskytovatel prokáže některou auditní zprávou ISO/IEC 270XX, SSAE 18 SOC 2 Type II, nebo jinou nezávislou auditní zprávou, že má zaveden systém sledování a vyhodnocování bezpečnostních událostí služby (např. SIEM), a poskytne technickou dokumentaci (nebo URL link), prokazující zpřístupnění prioritních událostí zákazníkovi služby.
ID15 – Služby centra bezpečnostního dohledu 24x7x365 pro sledování, vyhodnocování a řešení bezpečnostních událostí (může představovat volitelnou službu za příplatek nebo může být splněno službou třetí strany)	ČSN ISO/IEC 27001 subdoména A.12.4., lze doložit citací ze SSAE 18 SOC 2			X	Předložení dokumentu	Poskytovatel prokáže některou auditní zprávou ISO/IEC 270XX, SSAE 18 SOC 2 Type II, nebo jinou nezávislou auditní zprávou, že využívá služby centra bezpečnostního dohledu 24x7x365 pro sledování, vyhodnocování a řešení bezpečnostních událostí (může představovat volitelnou službu za příplatek nebo může být splněno službou třetí strany).
ID16 - Šifrování při přenosech dat po externí datové síti (přes Internet)	ČSN ISO/IEC 27001 A.10.1.1; VKB § 18 c)	X	X	X	Předložení dokumentu	BÚ2 a BÚ3: Poskytovatel prokáže technickou dokumentací k certifikaci ČSN ISO/IEC 27001 nebo auditní zprávou SSAE 18 SOC 2 Type II, že má zavedeno vynucení šifrování protokolem TLS při externích přenosech dat s vyloučením možnosti fall-backu na protokol HTTP (bez šifrování). BÚ1: Poskytovatel předloží čestné prohlášení statutárního zástupce organizace, že má zavedeno vynucení šifrování protokolem TLS při externích přenosech dat s vyloučením možnosti fall-backu na protokol HTTP (bez šifrování). Pro všechny: Použité šifry a hašovací algoritmy musí splňovat Minimální požadavky na kryptografické algoritmy publikované na webu NÚKIB GovCERT.
ID17 – Ochrana dat šifrováním v úložištích v cloudové službě algoritmem uvedeným v doporučení v oblasti kryptografických prostředků, které je zveřejněno na internetových stránkách NÚKIB; v případě uložení šifrovacích klíčů mimo perimetr zákazníka umožní poskytovatel uložení klíčů v certifikovaném Hardware security modulu (HSM) úrovně ochrany FIPS 140-2 level 2 (nebo vyšší) nebo certifikaci dle Common Criteria minimálně na EAL 4 a vyšší, který je pod virtuální správou orgánu veřejné moci. (Využití HSM modulu může představovat volitelnou službu za příplatek)	ČSN ISO/IEC 27001 A.10.1.2; Odvozeno od požadavku VKB Příloha 4 – Likvidace dat pro úroveň aktiv „Vysoká“.			X	Předložení dokumentu	1) Poskytovatel předloží technickou dokumentaci k bodu A.10.1.2 ISO/IEC 27001 nebo prokáže auditní zprávou SSAE 18 SOC 2, že v případě uložení šifrovacích klíčů mimo perimetr zákazníka, má zákazník možnost uložit šifrovací klíče pod svojí virtuální správou v HSM modulu definované úrovně ochrany. Dokumentace musí ukázat, že použité šifry a hašovací algoritmy musí splňovat Minimální požadavky na kryptografické algoritmy publikované na webu NÚKIB GovCERT. 2) Poskytovatel deklaruje, že tímto bodem je možné splnit požadavky na bezpečnou likvidaci dat pro úroveň důvěrnosti aktiv „vysoká“ v souladu s VKB Příloha 4.
ID18 – Definovaná dostupnost služby CC prostřednictvím NIX.CZ nebo jiného peeringového uzlu v ČR		X	X	X	Předložení výpisu	Dodavatel služby eGC deklaruje svoje možnosti peeringu v ČR, a to výpisem z www.peeringdb.com nebo jiným srovnatelným způsobem. Deklarovat šířku pásma [Gb/s], kterou má daný poskytovatel služby z datového centra (nebo center) do peeringového bodu k dispozici.