Zakázkové číslo
332/103/2009
Toto číslo uvádějte při fakturaci

Smlouva o poskytování servisní podpory sítě FINet-ADIS Ministerstva financí

ev. č.: ANECT/MF/0905

uzavřená podle ustanovení § 536 a násl. zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů, (dále jen „obchodní zákoník")
v rámci veřejné zakázky na služby (evidenční číslo 60028673), která byla zadána v otevřeném zadávacím řízení podle zákona č.137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „zákon") ,
č.j. 232/49676/2009/BA

(dále jen „Smlouva")

Článek 1: Smluvní strany

1. Objednatel: **Česká republika – Ministerstvo financí**
se sídlem Letenská 15, 118 00 Praha 1
jejímž jménem jedná [redacted]
IČ: 00006947

DIČ: CZ 00006947
(dále v této Smlouvě označováno jen jako „Objednatel"nebo „zákazník")

2. Zhotovitel: **ANECT a.s.**
se sídlem Vídeňská 125, 619 00 Brno
jejímž jménem jednají [redacted]
a [redacted]
IČ: 25 31 30 29
DIČ: CZ25313029
zapsaná u rejstříkového soudu v Brně pod sp.zn. B 2113
(dále v této Smlouvě označována jen jako „Zhotovitel" nebo „ANECT" ")

Článek 2: Předmět Smlouvy

Předmětem této Smlouvy je závazek:

1. Zhotovitele spočívající v poskytování komplexní servisní podpory sítě FINet-ADIS, zahrnující zejména správu a údržbu provozu technických zařízení, správu konfigurace síťových služeb, provozní dohled, údržbu projektové dokumentace a dokumentace provozu, HelpDesk, v rozsahu specifikovaném v Příloze č.1.

Zhotovitel se zavazuje poskytnout plnění v souladu s „Nabídkou", kterou v rámci výše uvedené veřejné zakázky Objednateli předložil, pokud není touto Smlouvou upraveno jinak.

2. Objednatele
   a) v případě řádně poskytnutého plnění Smlouvy platit dohodnutou cenu a
   b) poskytovat Zhotoviteli při plnění předmětu Smlouvy nezbytnou součinnost.

Článek 3: Místo plnění předmětu Smlouvy

1. Místem plnění jsou sídla Objednatele v Praze a sídla územních finančních orgánů (dále jen „ÚFO"). Finanční ředitelství a finanční úřady byly zřízeny k 1.1.1991 na základě zákona č. 531/1990 Sb., o územních finančních orgánech a tvoří soustavu územních finančních orgánů na území ČR (jejich aktuální seznam je na www.mfcr.cz).
2. K jednání ve vzájemném styku smluvních stran ve věcech organizačních a technických podle této Smlouvy jsou oprávněnými zástupci:

za Zhotovitele: [redacted] tel.: [redacted]
za Objednatele: [redacted] tel.: [redacted]

Článek 4: Cena

1. **Celková cena plnění** dle této Smlouvy za období 48 měsíců je stanovena ve výši **bez DPH 11.521.680,- Kč** (slovy: jedenáct-milionů-pět-set-dvacet-jeden-tisíc-šest-set-osmdesát korun českých), DPH 2.189.119,20 (slovy: dva-miliony-sto-osmdesát-devět-tisíc-sto-devatenáct korun českých dvacet haléřů), **včetně DPH 13.710.799,20 Kč** (slovy: třináct-milionů-sedm-set-deset-tisíc-sedm-set-devadesát-devět korun českých dvacet haléřů) **a je nepřekročitelná**.
2. Výše měsíční platby je stanovena ve výši bez DPH 240.035,- Kč (slovy: dvě-stě-čtyřicet-tisíc-třicet-pět korun českých), DPH 45.606,65 (slovy: čtyřicet-pět-tisíc-šest-set-šest korun českých šedesát-pět haléřů), včetně DPH 285.641,65 Kč (slovy: dvě-stě-osmdesát-pět-tisíc-šest-set-čtyřicet-jedna korun českých šedesát-pět haléřů).
3. Cena obsahuje veškeré náklady Zhotovitele služeb nutné k realizaci předmětu Smlouvy.
4. Cenu díla je možné změnit pouze v případě, že dojde v průběhu realizace díla ke změnám daňových předpisů upravující výši DPH, o tomto jsou v tomto případě smluvní strany povinny uzavřít dodatek ke Smlouvě.
5. Platby budou probíhat výhradně v Kč a rovněž veškeré cenové údaje budou v této měně platit do doby přechodu ČR na měnu Euro.

Článek 5: Platební podmínky

1. Datum uskutečnění zdanitelného plnění dle této Smlouvy je vždy poslední den v měsíci, v němž bude zhotovitel plnit své závazky podle této Smlouvy. Fakturace za období prosince běžného roku mimořádně proběhne nejpozději do 15.12. téhož roku.
2. Daňový doklad (faktura) bude obsahovat náležitosti dle ustanovení § 28 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a náležitosti dle § 13a zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů. Zhotovitel se zavazuje vystavit daňový doklad a prokazatelným způsobem doručit Objednateli nejpozději do 15 kalendářních dnů od data uskutečnění zdanitelného plnění s výjimkou měsíce prosince daného roku, kdy daňový doklad bude vystaven nejpozději dne 15.12. Splatnost všech daňových dokladu činí 21 dnů od jejich doručení Objednateli. Peněžní závazek Objednatele se považuje za včas splněný dnem připsání příslušné částky ve prospěch účtu Zhotovitele.
3. Dokladem o plnění smlouvy, sloužícím současně jako podklad pro fakturaci služeb za uvedené období, bude protokol ***Měsíční výkaz vyhodnocení správy sítě***, který bude předán odpovědné osobě objednatele k ověření a podpisu do 3 pracovních dnů od posledního dne plnění příslušného období. Uvedený výkaz představuje měsíční hodnocení obsahující popis průběhu správy sítě FINet-ADIS za uplynulé období, včetně uvedení nastalých a přetrvávajících problémů a termínů jejich odstranění. Uvedené hodnocení se bude opírat o dokumentaci provozu sítě a o písemně doložené popisy kontaktů odpovědných osob obou smluvních stran.
4. Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit bez zaplacení daňový doklad - fakturu, obsahuje-li nesprávné údaje nebo náležitosti dle uvedených právních předpisů. Zhotovitel je povinen fakturu opravit nebo nově vyhotovit. Smluvní strany se dohodly na tom, že oprávněným vrácením faktury přestává běžet původní lhůta splatnosti a celá lhůta běží znovu ode dne doručení opravené faktury nebo nově vyhotovené faktury, to znamená, že nezaplacením oprávněně vrácené faktury není Objednatel v prodlení s její úhradou.

Článek 6: Předání a převzetí předmětu Smlouvy

Zhotovitel je povinen předmět Smlouvy předat Objednateli. Objednatel je povinen předmět Smlouvy převzít prostřednictvím svého oprávněného zástupce uvedeného v čl. 3 odst. 2 této Smlouvy a způsobem popsaným v čl.5 odst.3.

Článek 7: Sankce

1. V případě, že Zhotovitel nedodrží, aniž by k tomu objektivní důvod spočívající mimo jeho vůli, lhůty uvedené ve Smlouvě /dle článku 3 odst 2/, má Objednatel právo uplatnit vůči němu smluvní pokutu ve výši 0,05% z měsíční ceny díla/služeb za každý i započatý den prodlení. Zhotovitel je v takovém případě povinen smluvní pokutu zaplatit.
2. Pro případ prodlení Objednatele se zaplacením smluvené ceny na základě důvodně a řádně vystavené faktury ve lhůtě její splatnosti je Zhotovitel oprávněn požadovat úhradu úroku z prodlení. Výše úroku z prodlení se bude řídit nařízením vlády č.142/1994 Sb., kterým se stanoví výše úroků z prodlení a poplatku z prodlení podle občanského zákoníku, ve znění nařízení vlády č. 163/2005 Sb.

3. Ujednáním o smluvní pokutě, resp. úroku z prodlení není dotčeno právo té které smluvní strany na náhradu škody vzniklé v souvislosti s plněním předmětu Smlouvy.
4. Žádná ze smluvních stran není zodpovědná za prodlení způsobené prodlením s plněním závazků druhé smluvní strany.
5. Limitování sankcí se nepřipouští.

Článek 8: Součinnost Objednatele při plnění předmětu Smlouvy

1. Objednatel umožní zaměstnancům Zhotovitele nebo jejich subdodavatelům přístup:
    a) do objektů, místností a k zařízením v rozsahu nezbytném pro plnění této Smlouvy,
    b) k informacím nutným pro splnění předmětu Smlouvy.
2. Objednatel a Zhotovitel se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.
3. Objednatel se zavazuje vyvinout takovou součinnost, která může být Zhotovitelem oprávněně požadována k umožnění řádného plnění Smlouvy, a kromě závazků uvedených v předchozích odstavcích je zejména zavázán zajistit potřebnou účast odpovědných osob Objednatele a dostatečné pracovní prostředí pro zaměstnance Zhotovitele podílející se na plnění Smlouvy v objektech Objednatele. Brání-li Objednateli jakákoliv okolnost v plnění požadované součinnosti, oznámí to Zhotoviteli písemně a bez zbytečného odkladu.

Článek 9: Zvláštní ujednání

1. Zhotovitel se zavazuje, že jeho zaměstnanci budou při plnění této Smlouvy dodržovat veškeré obecně závazné české právní předpisy vztahující se k vykonávané činnosti, zejména předpisy o bezpečnosti práce a o požární bezpečnosti, dále interní předpisy Objednatele, předpisy o vstupu do objektů Objednatele a o bezpečnosti systémů, a budou se řídit organizačními pokyny odpovědných zaměstnanců Objednatele.
2. Zhotovitel se zavazuje, že informace ani jakékoliv technické nebo jiné podklady získané při plnění této Smlouvy nepoužije pro jiné než touto Smlouvou stanovené účely. Tento závazek se vztahuje na všechny zaměstnance Zhotovitele, kteří se seznámí s těmito informacemi nebo budou držiteli těchto podkladů. Tento závazek bude trvat i po ukončení účinnosti Smlouvy.
3. Obě smluvní strany se zavazují se, že zachovají jako důvěrné informace a zprávy týkající se vlastní spolupráce a vnitřních záležitostí smluvních stran a předmětu Smlouvy, pokud by jejich zveřejnění mohlo poškodit druhou stranu. Povinnosti poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ve znění pozdějších předpisů není tímto ustanovením dotčena.
4. Smluvní strany budou považovat za důvěrné informace a) jako důvěrné označené, b) informace, u kterých se z povahy věci dá předpokládat, že se jedná o informace podléhající závazku mlčenlivosti nebo informace o Objednateli či Zhotoviteli, které by mohly z povahy věci být považovány za důvěrné a které se dozvědí v souvislosti s plněním Smlouvy.

5. Smluvní strany se zavazují, že neuvolní třetí osobě informace druhé strany bez jejího souhlasu, a to v jakékoliv formě, a že podniknou všechny nezbytné kroky k zabezpečení těchto informací. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti po dobu 5 let po ukončení účinnosti Smlouvy.
6. Zhotovitel je povinen zabezpečit veškeré podklady, mající charakter důvěrné informace, poskytnuté mu Objednatelem proti odcizení nebo jinému zneužití.
7. Povinnost zachovávat mlčenlivost, o níž se hovoří v tomto článku, se nevztahují na informace:
    - které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením ustanovení tohoto článku ze strany Zhotovitele,
    - které jsou Zhotoviteli známy a byly mu volně k dispozici ještě před přijetím těchto informací od Objednatele,
    - které budou následně Zhotoviteli sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k ním nijak vázána,
    - jejichž sdělení se vyžaduje ze zákona.
8. Zhotovitel se zavazuje postupovat tak, aby jeho činností nedošlo k úmyslnému vzniku škody na zařízeních nebo datech Objednatele.
9. Za prokázané porušení ustanovení v tomto článku má druhá smluvní strana právo požadovat náhradu takto vzniklé škody.
10. V případě porušení povinností uložených smluvním stranám tímto článkem má druhá smluvní strana právo účtovat smluvní pokutu ve výši 100.000 Kč za každý případ porušení.

Článek 10: Odpovědnost za škodu

1. Zhotovitel odpovídá za řádné, kvalitní, bezvadné a včasné provádění svých závazků podle této Smlouvy a za to, že předmět těchto závazků bude proveden v souladu se souvisejícími platnými českými normami a právními předpisy podle této Smlouvy.
2. Zhotovitel odpovídá za veškerou způsobenou škodu a to porušením ustanovení Smlouvy, opomenutím nebo zásadně nekvalitním prováděním smluvní činnosti v plné výši. O náhradě škody platí obecná ustanovení Obchodního zákoníku v platném znění.
3. Objednatel odpovídá za škodu, kterou způsobí porušením svých smluvních povinností Zhotoviteli.
4. Žádná ze smluvních stran neodpovídá za škodu v případě okolností vylučujících její odpovědnost dle § 374 obchodního zákoníku.
5. Žádná ze smluvních stran není zodpovědná za škodu způsobenou prodlením s plněním závazků druhé smluvní strany.

Článek 11: Vyšší moc

1. Pro účely této Smlouvy „vyšší moc" znamená událost, která je mimo kontrolu smluvních stran, nastala po podpisu Smlouvy, ke které došlo bez zavinění Smluvních stran a která však nezahrnuje chybu či nedbalost jedné ze stran. Takovými událostmi se rozumí zejména bez omezení války a revoluce, přírodní katastrofy, epidemie, karanténní omezení, dopravní embarga, vyhlášené generální stávky v příslušných průmyslových odvětvích.

2. Jestliže vznikne situace zaviněná událostí vyšší moci, dotčená strana okamžitě uvědomí druhou smluvní stranu písemně o takových podmínkách a jejich příčině. Pokud není jinak stanoveno písemně ze strany dotčené, bude druhá smluvní strana pokračovat v realizaci svých závazků podle Smlouvy tak, jak je to možné a bude hledat veškeré rozumné alternativní prostředky pro realizaci části, kde nebrání vyšší moc.
3. Trvá-li vyšší moc déle než 3 měsíce, smluvní strany mohou odstoupit od Smlouvy okamžitě.

Článek 12: Ukončení smluvního vztahu

1. Smluvní strany jsou oprávněny odstoupit od této Smlouvy z důvodů uvedených v zákoně a dále z důvodu podstatného porušení této Smlouvy ve smyslu ustanovení § 345 obchodního zákoníku, pokud podstatné porušení této Smlouvy, které je důvodem pro odstoupení od smlouvy nebylo způsobeno okolnostmi vylučujícími odpovědnost dle ustanovení § 374 obchodního zákoníku.
   1.1.1. Za podstatné porušení Smlouvy ze strany Objednatele se považuje neplnění závazků spočívající zejména v neuhrazení dlužné částky po dobu 30 dnů po splatnosti daňového dokladu (faktury).
   1.1.2. Za podstatné porušení Smlouvy ze strany Zhotovitele se považuje neplnění závazků spočívající zejména v nedodržení termínů plnění delší než 30 dnů nebo realizace předmětu smlouvy v rozporu s ustanoveními Smlouvy a nebo jiných závazných dokumentů či předpisů.
   1.1.3. Toto odstoupení od Smlouvy nabývá právní účinnosti dnem doručení písemného oznámení o odstoupení od Smlouvy druhé smluvní straně.
2. Tuto Smlouvu může každá smluvní strana ukončit písemnou výpovědí podanou i bez udání důvodů s tím, že výpovědní lhůta činí 3 měsíce a počíná běžet od prvního dne měsíce následujícího po doručení výpovědi druhé smluvní straně.
3. V případě odstoupení od Smlouvy z výše uvedených důvodů má Objednatel v každém případě nárok na náhradu prokázaných nákladů, které vzniknou v souvislosti s náhradním řešením, zejm.nákladů, které mohou vzniknout v souvislosti s pověřením jiných obchodních společností.
4. Před uplynutím stanovené doby lze účinnost Smlouvy ukončit oboustrannou dohodou smluvních stran.
5. V případě, že se Objednateli s ohledem na financování ze státního rozpočtu nepodaří zajistit finanční prostředky na realizaci předmětu Smlouvy, má Objednatel právo jednostranně odstoupit od Smlouvy,a to bez nároku na náhradu škody nebo ušlého zisku pro kteroukoliv smluvní stranu.
6. Smluvní strany provedou finanční a věcné vypořádání nejpozději do 30 dnů po skončení platnosti Smlouvy v důsledku odstoupení.

Článek 13: Oddělitelnost

1. Stanou-li se některá ustanovení této Smlouvy zcela nebo zčásti neplatná nebo pokud by některá ustanovení chyběla, není tím dotčena platnost zbývajících ustanovení.

Článek 14: Záruka

1. Zhotovitel poskytuje Objednateli záruku na provedené práce dle této Smlouvy v délce 12 měsíců.
2. Zhotovitel neodpovídá za vady vzniklé neodborným zásahem Objednatele, mechanickým poškozením nebo nepřípustným zásahem do vnitřní struktury zařízení, na kterém dodávané řešení provozováno. Zhotovitel též neodpovídá za vady vzniklé provozem zařízení v prostředí s nevyhovujícími provozními podmínkami nebo za závady zapříčiněné vyšší mocí. Tyto závady Zhotovitel odstraní za úplatu.

Článek 15: Práva třetích osob

1. Zhotovitel prohlašuje, že předmět plnění dle této Smlouvy nebude zatížen právy třetích osob, ze kterých by pro Objednatele vyplynuly jakékoliv další finanční nebo jiné nároky ve prospěch třetích stran. V opačném případě Zhotovitel ponese veškeré důsledky takovéhoto porušení práv třetích osob.

Článek 16: Závěrečná ustanovení

1. Smlouva se uzavírá od 1.10.2009 na dobu neurčitou.
2. Součástí Smlouvy je:
   Příloha č.1 – Seznam spravovaných zařízení v rámci celé ČR (aktuální ke dni zpracování zadávací dokumentace)
   Příloha č.2 – Nabídka z 22.7.2009
3. Smlouvu lze měnit anebo doplňovat pouze písemnými dodatky, takto označovanými a číslovanými vzestupnou řadou, po dohodě obou smluvních stran a podepsanými oprávněnými zástupci smluvních stran uvedenými v záhlaví této Smlouvy. Jiná ujednání jsou neplatná.
4. Vzhledem k tomu, že se jedná o služby svěřené správy sítě, případná změna objemu poskytovaných služeb musí být předem projednána a následně sepsán a podepsán příslušný dodatek ke Smlouvě.
5. Zhotovitel se zavazuje upravit rozsah poskytovaných služeb v souvislosti se změnami organizačního uspořádání ÚFO, se změnami službou pokrytých technických zařízení či se změnami související legislativy.
6. V případě jednotlivých nutných úprav rozsahu poskytovaných služeb, vyplývajících z účinnosti změny organizační struktury ÚFO během účinnosti této Smlouvy, bude odpovídajícím způsobem modifikován rozsah služeb poskytovaných Zhotovitelem ve formě uzavření dohody o dodatku této Smlouvy nejpozději dva měsíce před účinností organizační změny ÚFO.
7. Tato Smlouva je vyhotovena ve dvou stejnopisech, každý s platností originálu, z nichž každá ze stran obdrží po jednom vyhotovení.
8. Tato Smlouva nabývá platnosti a účinnosti dnem podpisu obou smluvních stran.

9. Smluvní vztahy výslovně neupravené touto Smlouvou, nebo upravené pouze částečně, se budou řídit výlučně příslušnými ustanoveními zákona č. 513/1991 Sb., Obchodní zákoník, ve znění pozdějších předpisů a předpisy souvisejícími.

10. Smluvní strany prohlašují, že se s obsahem této Smlouvy před jejím podpisem seznámily, rozumějí mu a souhlasí se závaznosti jeho podmínek.

V Praze dne: 30 -09- 2009

Česká republika – Ministerstvo financí:

V Praze dne: 30.9.2009

ANECT a.s.:

MINISTERSTVO FINANCÍ 52

ANECT
ANECT
www.anect.com
10
10 mio
DIČCZ25313029

Příloha č. 1 - Seznam spravovaných zařízení v rámci celé ČR

(aktuální ke dni zpracování zadávací dokumentace)

Popis zařízení	Počet (ks)
Cisco 3660 – Voice	1
Cisco 2620 – Voice	5
Cisco 3725 – Voice	1
L3 přepínač Cisco Catalyst 3550	13
L3 přepínač Cisco Catalyst 3560	2
L3 přepínač Cisco Catalyst 3750	29
L3 přepínače Cisco Catalyst 4006	8
L3 přepínač Cisco Catalyst 4503	1
L3 přepínač Cisco Catalyst 4506	7
L3 přepínač Cisco Catalyst 4507	30
L3 přepínač Cisco Catalyst 6509	3
Cisco 2621XM přístupový router Uchazeče	1

Příloha č.2

Konkrétní nabídka služeb pokrývající požadavky definované v zadávací dokumentaci

1. Služby správy aktivních síťových prvků sítě FINet-ADIS

1.1. Seznam spravovaných zařízení

Seznam aktivních síťových prvků, pro které budou poskytovány služby správy, je uveden v Příloze č.1.

1.2. Služby správy systémových zdrojů

Uchazeč prohlašuje, že je připraven poskytovat služby správy softwarové konfigurace a operačního systému IOS na všech zařízeních dle seznamu spravovaných zařízení a v rozsahu požadovaném Zadavatelem.

Uchazeč se zavazuje provádět zásahy do konfigurace a změny v použitém software pouze po dohodě se Zadavatelem.

Uchazeč bere na vědomí a přijímá fakt, že nebude poskytovat servis technického vybavení.

1.2.1. Služby správy IOS

Uchazeč se zavazuje provádět správu operačních systémů IOS všech verzí, které jsou na zařízeních instalovány.

Uchazeč prohlašuje, že má rozsáhlé a dlouholeté zkušenosti se správou velkých komunikačních celků a tedy i s administrativní správou zařízení, s pohotovostními zásahy na zařízeních i se správou softwarového vybavení zařízení.

1.2.1.1. Administrativní správa všech verzí software

Uchazeč se zavazuje provádět administrativní správu verzí software použitého na všech zařízeních dle seznamu spravovaných zařízení.

Uchazeč disponuje vlastním pokročilým softwarovým vybavením pro automatické zpracování a vedení dokumentace síťových prvků. Jednou z funkcionalit je i správa verzí instalovaného software. Vypracování podkladů pro tvorbu dokumentace probíhá s využitím softwarové komponenty instalované na počítači v síti Zadavatele. Kontrolu správnosti získaných dat provádí lidská obsluha. Tak je zaručena aktuálnost a správnost sledovaných údajů.

1.2.1.2. Upgrade IOS v rámci verze a aplikace bezpečnostních záplat

Uchazeč se zavazuje provádět podle potřeby a požadavku Zadavatele aktualizaci softwarového vybavení na zařízeních dle seznamu spravovaných zařízení.

Uchazeč si je vědom důsledků vyplývajících z nasazení verze software s jinou funkční sadou, než byla k zařízení zakoupena. Uchazeč bude při standardní údržbě používat pouze verze software s funkční sadou odpovídající zakoupeným licencím.

Nad rámec běžné údržby poskytuje Uchazeč službu Aplikace bezpečnostních záplat, která spočívá v proaktivním odstraňování bezpečnostních rizik v návaznosti na informace od výrobce zařízení.

Uchazeč má přímé komunikační vazby na výrobce Cisco Systems a je odběratelem zpráv o zjištěných bezpečnostních rizicích a chybách v software, reakce na takové situace je proto bezodkladná. Uchazeč se zavazuje provést výběr vhodné verze software a po odsouhlasení Zadavatelem provést aktualizaci software v době, která neomezí provoz Zadavatele a to i mimo běžnou pracovní dobu.

V rámci pravidelné údržby se Uchazeč zavazuje k pravidelné aktualizaci software s periodicitou jeden rok, pokud nebude Zadavatelem požadováno jinak.

Upgrade IOS se Uchazeč zavazuje provádět na všech zařízeních, u kterých výrobce dosud vydává nové verze IOS. U zařízení, na která výrobce již nezajišťuje nové verze software, provede ANECT při výměně zařízení třetí stranou instalaci té verze IOS, která byla na zařízení nainstalována a funkční v době závady.

Uchazeč se tedy zavazuje provádět aktualizaci software ve všech následujících případech:

- na základě požadavku Zadavatele,
- periodicky, v rámci pravidelné údržby,
- po ohlášení závažné bezpečnostní chyby výrobcem – viz dále,
- po projevu závažného technického nedostatku software,
- po výměně zařízení – viz dále.

Informace o službě Aplikace bezpečnostních záplat

Postupy zjišťování informací o bezpečnostních rizicích, jejich zpracování, testování nových verzí software, jednání se Zadavatelem o nasazení a postup nasazení je prováděn v souladu s interní směrnicí uchazeče, ze které uvádíme výňatek:

Příprava - zajištění informací

1. Přidělený pracovník Uchazeče bude zaregistrován pro odběr informačních bulletinů ve fórech výrobců a dodavatelů SW.
2. Přidělený pracovník Uchazeče bude zaregistrován na informačních serverech, kde využívá zkušeností ostatních IT profesionálů (oddělení předprodejní podpory eviduje informační zdroje našich partnerských výrobců a dodavatelů).
3. Přidělený pracovník Uchazeče bude sledovat vydávání bezpečnostních oprav pro jemu svěřenou oblast technologií. Bude porovnávat informace s provozní dokumentací poskytovanou zadavateli (v případě její nedostatečnosti nebo neúplnosti bude věc konzultovat s příslušným projektantem určeným k práci pro Zadavatele).
4. Přidělený pracovník Uchazeče bude pravidelně informovat emailem o svých zjištěních pracovníky zaregistrované do distribučních skupin (min.1x měsíčně). Bude-li objeven zásadní bezpečnostní problém, informuje je okamžitě. Všechny odeslané informace budou archivovány minimálně po dobu jednoho roku ve veřejných složkách.
5. Členové distribuční skupiny budou sledovat a vyhodnocovat přijaté emaily, dle uvážení pak vybírají bezpečnostní opravy vhodné pro nasazení v systémech Zadavatele, ke kterým jsou přiděleni. To platí i v případě, že člen distribuční skupiny obdrží upozornění na bezpečnostní chybu z jiných zdrojů. Pak bude neprodleně informovat příslušného pracovníka Uchazeče, který zajistí distribuci dalším členům skupiny.

Rozhodnutí o nasazení

1. Přidělený projektant Uchazeče zváží nutnost nasazení bezpečnostní opravy a projedná možné dopady a rizika s ostatními projektanty dalších systémů u Zadavatele.
2. Pracovník, který rozhodl o nutnosti nasazení bezpečnostní opravy, má možnost v této etapě provést její předtestování v labu ANECT. Testování by mělo poskytnout důležité informace pro jednání se Zadavatelem a může zkrátit dobu vlastního testování před nasazením u Zadavatele.

Jednání o nasazení se zadavatelem

1. Přidělený projektant Uchazeče bude informovat Zadavatele o nejvhodnějším postupu a způsobu nasazení bezpečnostní opravy, o možných rizicích, o časové a kapacitní náročnosti otestování.

2. Zadavatel potvrdí svůj souhlas s nasazením bezpečnostní opravy ve své síti prostřednictvím registrace požadavku na Service Desk ANECT.

Testování

1. Testování bude provádět příslušný projektant Uchazeče s podporou projektanta specializovaného na danou technologickou oblast. U méně rizikových nasazení neohrožujících chod ostatních systémů bude testování provádět příslušný technický pracovník Uchazeče s podporou projektanta specializovaného na danou technologickou oblast, který na závěr odsouhlasí výsledek testování.
2. V průběhu testování bude brán ohled na všechny ostatní běžící systémy, služby a aplikace a budou zohledněna všechna rizika nasazení.
3. Pracovník uchazeče provádějící testování zaznamená výsledky průběhu testování do příslušného tiketu v Service Desk ANECT. Výsledek testování bude vždy obsahovat i popis plánu návratu – „recovery plan", který bude v souladu se zvoleným postupem nasazení opravy nebo doporučením daným distributorem bezpečnostní opravy.
4. Výsledek testování bude odsouhlasen Zadavatelem formou zápisu komentáře do tiketu v Service Desk.
5. Pracovník, který bude provádět testování, informuje o výsledku skončeného testování manažera projektu a account manažera. Ti poté dohodnou se Zadavatelem přesný termín nasazení.

Nasazení

1. Příslušný pracovník ANECT provede nasazení bezpečnostní opravy v systému Zadavatele.
2. Ten pak informuje o postupu, výsledcích a problémech vzniklých v rámci nasazení bezpečnostní opravy příslušného projektanta a account manažera.
3. Příslušný technický pracovník uchazeče společně s projektantem, manažerem projektu a account manažerem, pak bude řešit se Zadavatelem případné nežádoucí dopady nasazení bezpečnostní opravy.

Zaznamenané výsledky nasazení bezpečnostní opravy budou při uzavření příslušného tiketu zaneseny v systému Service Desk.

1.2.1.3. Instalace aktuální verze IOS na zařízení v případě, kdy dojde k výměně HW třetí stranou

Uchazeč je připraven spolupracovat s třetí stranou při výměně zařízení. Uchazeč bude zajišťovat instalaci softwarového vybavení po výměně zařízení třetí stranou. Uchazeč předpokládá, že třetí strana uvede zařízení do stavu, kdy bude vzdáleně dosažitelné. Uchazeč prohlašuje, že je schopen poskytnout potřebnou podporu i na místě instalace v případě, že se třetí straně nepodaří uvést zařízení do stavu, kdy bude vzdáleně dostupné.

1.2.2. Služby správy konfigurací

Diagnostika a řešení konfiguračních závad

Uchazeč prohlašuje, že disponuje pracovníky, schopnými posoudit funkční stav provozovaných zařízení. Pracovníci Uchazeče mají rozsáhlé a dlouholeté zkušenosti se zajišťováním provozu síťových zařízení. Identifikaci závad provádí v první řadě v nepřetržitém režimu (7 dnů v týdnu, 24 hodin denně) pracovníci Dohledového centra Uchazeče, k faktickému zahájení prací na řešení závad tedy dochází velmi rychle po jejich zjištění. Pracovníci Dohledového centra mají přímé napojení na první a druhou úroveň technické podpory Uchazeče a je tak zajištěna dostatečná personální i odborná základna pro řešení incidentů libovolného rozsahu.

Uchazeč společně se Zadavatelem zpracuje popis funkčních testů jednotlivých zařízení, které budou prováděny jako první úkon pro zjištění plné funkcionality zařízení v případě podezření na jeho závadu.

1.2.2.1. Správa aktivních prvků

Uchazeč se zavazuje provádět správu konfigurací zařízení v rozsahu požadovaném Zadavatelem, tedy:

- nastavení základních parametrů zařízení,
- konfigurace všech rozhraní,
- konfigurace směrování,
- konfigurace komplexu bezpečnostních opatření,
- konfigurace systému správy uživatelů a řízení jejich přístupů,
- konfigurace synchronizace času,
- konfigurace tvorby provozních záznamů.

Uchazeč navíc nabízí využití svých hlubokých zkušeností s návrhem a správou rozsáhlých komunikačních celků a je připraven přinášet Zadavateli návrhy na změny konfigurací s cílem vyšší funkční efektivity i úrovně zabezpečení komunikačních zařízení.

Uchazeč se zavazuje provádět změny konfigurací spravovaných zařízení, které budou požadovány a odsouhlaseny Zadavatelem na základě nových nároků aplikací v síti provozovaných nebo nároků na nová bezpečnostní opatření.

Uchazeč bude provádět konfigurační úkony na základě požadavku v systému Service Desk Uchazeče. Zahájení prací proběhne v době podle požadavku Zadavatele, v souladu s dohodnutým SLA. Pracovníci Uchazeče vynaloží maximální úsilí k tomu, aby požadavek byl splněn řádně a včas. O průběhu realizace požadavků a jejich dokončení budou vedeny záznamy v systému Service Desk Uchazeče. Před uzavřením požadavku požádá pracovník Uchazeče o souhlas určeného pracovníka Zadavatele.

Pokud bude Zadavatel požadovat po Uchazeči činnosti, které by mohly vést ke snížení bezpečnosti sítě, nebo by byly nebezpečné pro zájmy Zadavatele, zavazuje se Uchazeč Zadavatele na tento fakt upozornit a provádět činnosti až po potvrzení ze strany Zadavatele.

1.2.2.2. Ochrana proti neoprávněnému přístupu na zařízení

Uchazeč se zavazuje udržovat konfigurace AAA ve stavu, kdy každý pracovník Uchazeče i Zadavatele bude mít přiřazeno osobní uživatelské jméno a heslo. Přístupové informace budou předávány proti podpisu v zapečetěných obálkách. V konfiguracích AAA budou zohledněna autorizační pravidla.

Uchazeč bude udržovat konfigurace spravovaných zařízení ve stavu, kdy se jednotliví pracovníci budou autentizovat osobním jménem a heslem a bude jim umožněno provádění pouze těch činností, ke kterým jsou serverem AAA autorizováni. Anonymní přístup na zařízení nebude umožněn, výjimkou bude pohotovostní přístup, který bude použitelný pouze v případě výpadku všech AAA serverů.

Uchazeč se zavazuje udržovat takovou strukturu oprávnění, kdy Zadavatel bude mít trvale nejvyšší úroveň oprávnění. Uchazeč nebude manipulovat s účty Zadavatele bez přímého požadavku ze strany Zadavatele.

Uchazeč prohlašuje, že jeho zaměstnanci jsou si vědomi, že jsou odpovědni za všechny činnosti, které jsou uskutečněny pod přidělenými uživatelskými účty a hesly. Pracovníci Uchazeče přijmou taková bezpečnostní opatření, která zabrání přístupu neautorizovaných osob k důvěrným informacím Zadavatele a k jejich zneužití prostřednictvím počítače / terminálu, kterým se přihlásili do sítě Zadavatele. Uchazeč se zavazuje bez zbytečného odkladu oznámit Zadavateli všechny zjištěné bezpečnostní incidenty nebo nedostatky v síti, včetně podezření, že taková situace nastala. Zaměstnanci Uchazeče zajistí, aby přístupová hesla byla změněna okamžitě po zjištění, že hesla byla prozrazena, nebo pokud vznikla pochybnost, že by jiná osoba mohla identifikovat a zjistit hesla. Zadavatel je oprávněn plně monitorovat konfigurační činnosti Uchazeče na zařízeních.

1.2.2.3. Správa záloh konfigurací

Uchazeč se zavazuje provádět archivaci konfiguračních souborů všech spravovaných zařízení, jejich pravidelnou aktualizaci a údržbu verzí tak, aby byly trvale k dispozici aktuální verze pro všechna spravovaná zařízení.

Uchazeč se zavazuje v případě nutné výměny HW vybavení poskytnout součinnost pracovníkům třetích stran tak, aby bylo možné uvést nový HW do provozu s patřičnou aktuální konfigurací. Uchazeč se zavazuje při předávání konfigurace nebo jejích částí dodržovat maximální přiměřenou úroveň zabezpečení předávaných dat.

Uchazeč má dlouholeté zkušenosti s provozem dohledového centra zákaznických sítí a používá dobře propracované a zaběhnuté postupy pro zálohování a uchovávání konfigurací síťových zařízení. Dohledové centrum Uchazeče pracuje se standardním komerčním softwarovým vybavením pro inteligentní automatické zálohování konfigurací síťových zařízení. Správná funkce zálohování konfigurací je pravidelně kontrolována kvalifikovanou lidskou obsluhou, která řeší případné závady archivace. Uchazeč udržuje také archiv historických konfigurací síťových zařízení. Konfigurace spravovaných zařízení jsou v podobě ochuzené o hesla a jiné citlivé údaje součástí Elektronické provozní dokumentace, vedené Uchazečem. Aktuální konfigurace budou oprávněným pracovníkům Zadavatele přístupné prostřednictvím WWW portálu.

1.2.3. Služba správy matričního souboru

Uchazeč se zavazuje k údržbě a aktualizaci centrálního matričního souboru (masterfile), který obsahuje v definované struktuře veškeré informace, nutné pro vytváření konfigurací aktivních síťových prvků a síťových služeb aplikačních serverů (určené pro IS ADIS) tak, aby byla zajištěna konzistence síťových služeb na úrovni LAN sítí ÚFO (územní finanční orgány).

Uchazeč bude provádět správu masterfile podle používaných a zaběhnutých postupů.

1.2.4. Výstup služeb

Uchazeč se zavazuje Zadavateli umožnit v nepřetržitém režimu (24 hodin denně, 7 dnů v týdnu) hlášení poruchy funkcionality systémových zdrojů a průběžné sledování stavu řešených požadavků. K zajištění této služby bude využíván dispečink technické podpory Uchazeče, jehož služby jsou popsány níže.

Souhrnné informace o ICT Zadavatele

Uchazeč se zavazuje Zadavateli poskytovat souhrnné informace, které mohou pomoci při plánování dalšího rozvoje sítě, funkcionality služeb, ochrany proti bezpečnostním incidentům apod.

Pro potřeby strategického řízení ICT zákazníka ANECT nabízí službu „Vyhodnocení technické podpory", která představuje prezentaci výsledků a průběhu poskytované technické podpory zákazníkovi společnosti ANECT. Vyhodnocení vychází z údajů ze systému Service Desk nebo management systémů a z praktických poznatků specialistů ANECT s provozem IS zákazníka a zaměřuje se především na analýzu silných a slabých stránek provozu ICT zákazníka a na shrnutí příležitostí ke zlepšení jeho provozu v těch oblastech, pro které ANECT zajišťuje technickou podporu.

Prezentovány jsou též dosahované výsledky poskytovaných služeb (plnění SLA).

Prezentace obsahuje přehled poruch v provozu IS, jejich vyhodnocení, trendy, návrhy na opatření jak je odstranit a návrhy na další zvýšení spolehlivosti IS zákazníka.

V případě požadavku zákazníka je ANECT schopen upravit interval nebo formu poskytování této služby tak, aby přinášela zákazníkovi potřebné informace častěji, například formou automaticky generovaných reportů do webového prostředí.

ANECT tuto službu standardně nabízí formu prezentace s periodicitou jednoho (uplynulého) roku.

Reporting archivace konfigurací

Uchazeč se zavazuje Zadavateli umožnit průběžnou kontrolu provádění archivací konfiguračních souborů. Pro účely reportingu bude Uchazeč provozovat webový portál, který bude obsahovat mimo jiné informace o průběhu zálohování konfiguračních souborů. Uchazeč umožní přístup na tento portál oprávněným osobám Zadavatele. Dále Uchazeč Zadavateli umožní příjem e-mailových hlášení o výsledcích posledního běhu zálohování konfigurací.

1.2.5. Četnost služeb

Dostupnost služeb

Služby budou poskytovány průběžně.

Přímý kontakt se Zadavatelem není omezen žádným časovým intervalem, bude poskytován nepřetržitě 7 dnů v týdnu, 24 hodin denně, přičemž pro všechny způsoby komunikace (prostřednictvím internetu, emailu, telefonu včetně zelené linky i faxu) mezi Zadavatelem a poskytovatelem technické podpory **bude zajištěna nepřetržitá (7 dnů v týdnu, 24 hodin denně), fyzická přítomnost pracovníků technické podpory ANECT.**

Veškeré požadavky na poskytování technické podpory jsou vyhodnocovány a zpracovávány průběžně.

Archivace konfiguračních souborů

Uchazeč bude provádět archivaci konfiguračních souborů ze všech prvků denně v čase podle dohody se Zadavatelem. Záznamy o provedení archivace bude Uchazeč zpracovávat a uchovávat. V případě, že budou zjištěny problémy v procesu archivace, podniknou pracovníci Uchazeče bez zbytečného odkladu kroky k jejich nápravě.

Reporting archivace konfigurací je popsán v kapitole Výstup služeb.

SLA

Uchazeč se zavazuje poskytovat servisní službu „Servis" v následujících režimech:

- závada, která ohrožuje základní funkcionalitu sítě,
- závada s nižší prioritou a požadavky, které nesouvisí s odstraňováním závad,
- ostatní požadavky.

V následujících odstavcích jsou jednotlivé případy podrobně rozepsány.

V případě závady, která ohrožuje základní funkcionalitu sítě v oblastech:

- poruchy IP konektivity,
- chyby ve směrování,
- chyby v bezpečnostních opatřeních,

se Uchazeč zavazuje odstranit závadu do 8 hodin od nahlášení.

Servis Do8 – 7x24 (zaručená doba opravy do 8 hodin, režim 7x24)

Servisní služba poskytovaná 7 dnů v týdnu, 24 hodin denně, s povinností oznámit Zadavateli jméno řešitele požadavku nejpozději do 1 hodiny a odstranit závadu nejpozději do 8 hodin po elektronickém nebo faxovém potvrzení požadavku na servisní zásah.

V případech, kdy bude k vyřešení závady nutná spolupráce s třetí stranou (např. v případě HW závady a nutnosti výměny zařízení) nebo pokud nebude poskytnuta v daný okamžik nezbytná součinnost Zadavatele (např. umožnění přístupu k zařízení), se o tento čas prodlužuje garantovaná doba opravy.

Pro závady s nižší prioritou (které neohrožují základní funkcionalitu sítě) a pro požadavky které nesouvisí s odstraňováním závad (např. změny konfigurací aktivních prvků, VLAN, aktualizace AL atd.) se Uchazeč zavazuje zahájit práce na jejich řešení do 8 hodin v režimu 5x9.

Dz8 - 5x9 (zaručená doba zásahu do 8 hodin, režim 5x9)

Servisní služba poskytovaná 5 pracovních dní v týdnu, 9 hodin denně v pracovní době od 07:30 do 16:30 hodin, s povinností oznámit zadavateli jméno řešitele požadavku nejpozději do 1 hodiny a zahájit činnosti spojené s jeho řešením nejpozději do 8 hodin po elektronickém nebo faxovém potvrzení požadavku na servisní zásah.

Ostatní požadavky Zadavatele budou řešeny formou služby odborná podpora v režimu 5x8.

Odborná podpora v režimu OpNPD – 5x8

Odborná podpora bude zadavateli poskytována 5 pracovních dnů v týdnu, 8 hodin denně v době od 08:00 do 16:00 hodin, s povinností oznámit zadavateli jméno řešitele problému do 1 hodiny a zahájit činnosti spojené s řešením problému nejpozději do konce následujícího pracovního dne po elektronickém nebo faxovém potvrzení požadavku.

O plnění této služby je ANECTem pravidelně zpracováván report, z něhož jsou zákazníkovi v přehledné formě dostupné informace o:

- celkovém měsíčním rozsahu poskytované odborné podpory,
- rozsahu odborné podpory v jednotlivých oblastech, které si sám vydefinuje,
- délce trvání řešení jednotlivých požadavků na odbornou podporu.

1.2.6. Technické a organizační prostředky pro zajištění služeb

Uchazeč bude při poskytování uvedených služeb respektovat stávající koncepci sítě – adresní plán, způsob směrování, bezpečnostní opatření, řízení přístupů apod. Uchazeč se přímo podílel na tvorbě koncepce celoresortní sítě a je tedy přirozené, že bude její současnou podobu respektovat. Uchazeč nabízí Zadavateli svoje dlouholeté a rozsáhlé zkušenosti s návrhem a správou rozsáhlých komunikačních systémů a je připraven dále spolupracovat se Zadavatelem na rozvoji sítě.

Uchazeč souhlasí s tím, že většinu požadovaných úkonů bude vykonávat vzdáleně – podle povahy prací. Dále Uchazeč prohlašuje, že disponuje skupinou pohotovostních techniků, kteří jsou nepřetržitě ve službě a v případě potřeby mohou zasáhnout na libovolném místě.

Pro výkon svěřené správy bude Uchazeč používat zabezpečený přístup do sítě FINet-ADIS pomocí dedikované WAN spojnice.

Uchazeč se zavazuje poskytovat dodavatelům třetích stran potřebné informace (verze IOS apod.) a aktuální konfigurace, které jim umožní uvést nová zařízení do požadovaného provozního stavu. Uchazeč ve spolupráci se Zadavatelem zpracuje popis funkčních testů jednotlivých zařízení, které budou prováděny pro ověření plné funkcionality zařízení po jejich zprovoznění. Pracovníci Uchazeče budou provádět kontrolu funkcionality spravovaných zařízení po zásahu třetí strany v rozsahu takto dohodnuté správy.

Uchazeč se zavazuje udržovat všechny potřebné administrativní informace, centrální konfigurační soubor, aktuální verze IOSu a konfigurace na serverech v majetku Zadavatele, nacházející se v prostorách ICT MF a jednotlivých FŘ.

1.3. Služby řízení přístupu

Uchazeč zajistí poskytování AAA služeb na devíti instancích způsobem, který je administrátory sítě dlouhodobě využíván a který respektuje hierarchii odpovědnosti administrátorů v síti FINet-ADIS (příslušnost FÚ k FŘ).

Uchazeč zajistí, aby byly splněny následující požadavky:

- redundance provozu AAA služeb tak, aby každý síťový prvek mohl mít nakonfigurovány dva nezávislé AAA servery, na které se může obracet s požadavky,
- zajištění konzistence informací o řízení přístupů se síťovými parametry udržovanými v maticním souboru tak, aby se promítaly včas případné změny v síťové infrastruktuře,
- možnost vytvářet skupiny zařízení s jednotnou správou (uživatelé, autorizační pravidla) podle IP adresy,
- možnost používat odlišné sdílené klíče pro jednotlivá zařízení,
- zajištění průběžného ukládání všech informací o systému služeb AAA do záznamových souborů, logování i neúspěšných pokusů o autentizaci včetně IP adresy přistupujícího klienta.

Uchazeč se zavazuje zajistit správu konfiguračních souborů pro AAA servery, tj.:

- aktualizaci při změnách podle požadavků Zadavatele (zavádění a rušení uživatelů nebo skupin, změna parametrů jako jsou hesla, přístupová práva apod.),
- zabezpečení proti zneužití,
- archivaci.

Uchazeč bude provádět správu záznamových souborů generovaných systémem řízení přístupu AAA, tj. jejich vytváření, zpřístupnění, zabezpečení, archivaci a likvidaci.

1.3.1. Výstup služeb

Uchazeč zajistí Zadavateli možnost hlášení poruchy funkcionality služeb řízení přístupů a průběžného sledování stavu řešení problému stejným způsobem, jako v případě řešení jiných požadavků na technickou podporu – Zadavatel bude v těchto případech kontaktovat Dispečink technické podpory Uchazeče.

Zadavatel bude mít možnost přístupu (bez možnosti modifikace) ke konfiguračním a záznamovým souborům, bude informován o změnách v konfiguracích, průběhu archivací a případných bezpečnostních incidentech.

1.3.2. Četnost služeb

Dostupnost služeb

Služby budou poskytovány průběžně.

Přímý kontakt se Zadavatelem není omezen žádným časovým intervalem, bude poskytován nepřetržitě 7 dnů v týdnu, 24 hodin denně, přičemž pro všechny způsoby komunikace (prostřednictvím internetu, emailu, telefonu včetně zelené linky i faxu) mezi Zadavatelem a poskytovatelem technické podpory **bude zajištěna nepřetržitá (7 dnů v týdnu, 24 hodin denně), fyzická přítomnost pracovníků technické podpory ANECT.**

Veškeré požadavky na poskytování technické podpory jsou vyhodnocovány a zpracovávány průběžně.

Archivace konfiguračních souborů

Uchazeč se zavazuje zajistit po každé provedené změně na AAA serveru provést zálohu konfiguračního souboru. Uchazeč pořídí po každé provedené archivaci konfigurace záznam o výsledku archivace.

SLA

Uchazeč akceptuje postoj Zadavatele, že AAA služby neohrožují základní funkcionalitu sítě a zavazuje se poskytovat správu AAA služeb v režimu Do2D – 7x24 = dodržovat dobu opravy na závadu AAA služeb 48 hodin od nahlášení.

Do2D – 7x24 (zaručená doba opravy do 48 hodin)

Servisní služba poskytovaná 7 dnů v týdnu, 24 hodin denně, s povinností oznámit zadavateli jméno řešitele požadavku nejpozději do 1 hodiny a odstranit závadu nejpozději do 48 hodin po elektronickém nebo faxovém potvrzení požadavku na servisní zásah.

V případech, kdy bude k vyřešení závady nutná spolupráce s třetí stranou (např. v případě HW závady a nutnosti výměny zařízení) nebo pokud nebude poskytnuta v daný okamžik nezbytná součinnost zadavatele (např. umožnění přístupu k zařízení), se o tento čas prodlužuje garantovaná doba opravy.

V oblasti služeb řízení přístupu bude zadavateli stejně jako v oblasti služeb správy systémových zdrojů (a stejně tak i v oblasti služeb dohledu) poskytována odborná podpora v režimu OpNPD – 5x8.

Odborná podpora v režimu OpNPD – 5x8

Odborná podpora bude zadavateli poskytována 5 pracovních dnů v týdnu, 8 hodin denně v době od 08:00 do 16:00 hodin, s povinností oznámit zadavateli jméno řešitele problému do 1 hodiny a zahájit činnosti spojené s řešením problému nejpozději do konce následujícího pracovního dne po elektronickém nebo faxovém potvrzení požadavku.

Požadavky na služby řízení přístupu lze uplatňovat 7 dnů v týdnu, 24 hodin denně.

1.3.2.1. Technické a organizační prostředky pro zajištění služeb

Uchazeč převezme a bude respektovat stávající koncepci řízení přístupů.

Uchazeč se zavazuje udržovat dostupnost služeb dostatečnou k tomu, aby neohrožovala běžný provoz.

Uchazeč převezme a bude udržovat stávající programové vybavení (OS a aplikace) pro poskytování služeb AAA.

Uchazeč bude poskytovat služby s využitím serverů v majetku Zadavatele, nacházejících se v prostorách ICT MF a jednotlivých finančních ředitelstvích.

1.3.3. Služby dohledu provozu, sběru provozních údajů a bezpečnosti

Služby Proaktivního dohledu funkcionality prvků sítě Zadavatele, sběru provozních údajů a bezpečnosti jsou provozní činnosti, jejichž obsahem je monitorování, vyhodnocování, detekce a řešení mezních a poruchových stavů na infrastruktuře Zadavatele.

Služba Proaktivní dohled je soubor řízených činností zaměřených na zjišťování provozních změn v informačním a komunikačním systému Zadavatele, které by mohly vést k chybovým stavům a dokonce i ke ztrátě provozuschopnosti jeho infrastruktury.

Dohled umožňuje:

- předcházet chybovým stavům,
- zkrátit čas potřebný na lokalizaci a odstranění závady v informačním systému,
- podporovat servisní činnosti,

- vytvářet reporty o funkčnosti a provozních parametrech dohlížených systémů,
- získávat výstupy použitelné k objektivnímu měření kvality poskytovaných služeb,
- zpracovávat analýzy předpokládaného vývoje klíčových provozních komponent, které mohou zákazníkovi sloužit jako rozhodovací základna při plánování investic do ICT,
- plánovat kapacity ICT,
- ochránit investice do drahých ICT zařízení,
- přispívat k maximálnímu využití prostředků ICT,
- nahradit vlastní dohledové centrum Zadavatele nebo souběžnou činnost s dohledovým centrem Zadavatele.
- naprostou kontrolu nad průběhem řešení chybového stavu - veškeré informace od vzniku až po vyřešení incidentu / problému jsou vkládány do extranetové aplikace ServiceDesk, která je nonstop přístupná Zadavateli,
- přinést úsporu nákladů Zadavatele jak na implementaci vlastních management nástrojů, tak na provoz dohledového centra a v neposlední řadě i v souvislosti se získáváním a udržením vlastních specializovaných pracovníků,
- snadné a rychlé získání cenného know-how společnosti ANECT získaného dlouholetými zkušenostmi při provozu DCA a poskytování služby dohledu mnoha zákazníkům,
- rozsáhlé přizpůsobení dle potřeb zákazníka, produkt lze poměrně rychle implementovat a začít provozovat.

Službu zajišťuje Dohledové centrum Uchazeče (DCA) v nepřetržitém režimu 7x24 (7 dnů v týdnu, 24 hodin denně, 365 dnů v roce). Společně s plněním své základní funkce sehrává DCA nezastupitelnou roli při spolupráci se servisním oddělením (zajišťujícím službu správy) a **přináší zkrácení průměrné doby opravy zařízení nebo systému.** DCA provádí také komplexní testy IP konektivity po provedení servisního zásahu a je v bezprostředním kontaktu s dispečinkem technické podpory.

Služba je personálně zajištěna operátory DCA, kteří se střídají ve směnném, denním a nočním provozu, jsou **trvale přítomni na pracovišti, dostupní v kteroukoliv denní či noční hodinu** prostřednictvím Service Desku, emailu a telefonu. Operátoři DCA jsou síťoví specialisté schopni samostatného řešení servisních zásahů vzdáleným přístupem. Toto spojení operativní pohotovosti s odbornými znalostmi přináší pro Zadavatele ve většině případů výrazné zkrácení doby řešení doby opravy zařízení.

Dohled sítí je prvním krokem k zajištění vysoké dostupnosti, spolehlivosti, důvěryhodnosti a bezpečnosti dat a informací poskytovaných informačními a komunikačními systémy Zadavatele. Společně s dalšími službami jako je „Servis", „Správa ICT" a „Odborná podpora" vytváří komplexní systém garantující vysokou dostupnost informačního a komunikačního systému Zadavatele.

Uchazeč má dlouhodobé praktické zkušenosti s poskytováním služeb dohledu komunikační infrastruktury a dokáže využít svých bohatých zkušeností s implementací management systémů k tomu, aby jeho tato služba byla komplexní.

Kvalita služeb dohledového centra je potvrzena dlouhodobou spokojeností zákazníků podobné velikosti jako Zadavatel.

Principy fungování dohledu

- Dohledové centrum ANECT je vybaveno dohledovými systémy, které umožňují zpracovávat informace z mnoha různých zdrojů a různých sítí. Je založeno na systému Netcool Omnibus, který umožňuje velmi flexibilně nastavovat požadavky, které jsou specifické pro dohled specifických potřeb různých zákazníků. Centrální řešení automaticky třídí události podle priorit, zobrazuje je operátorovi a upozorňuje jej na nově příchozí události s kritickou prioritou.
- V případě, že je určitý prvek systému nedostupný, nebo je zaznamenán nestandardní/mezní stav, management aplikace pošle tuto informaci do centrálního dohledového systému systému Netcool Omnibus umístěného v DCA.

- Události jsou označeny prioritou systémem, ze kterého přicházejí a jsou k nim přidané další informace o zákazníkovi, potřebné pro rychlou reakci operátora DCA. Operátor DCA může priority také měnit.
- Incident je automaticky nebo manuálně založen operátorem DCA formou tiketu do systému Service Desk na základě potvrzení mezního stavu.
- Následně jsou do tiketu vloženy informace zjištěné od vzniku mezního stavu a které pomohou k dalšímu řešení.
- V DCA jsou vytvořena pravidla, která odpovídají kritičnosti dohlížených zařízení a systémů pro zákazníky a operátoři dohledového centra postupně zpracovávají incidenty od incidentů s nejvyšší prioritou až po incidenty s nejnižší prioritou. DCA provádí:
    - detekci incidentů/problému a mezních stavů,
    - primární lokalizaci a kategorizaci s následným předání incidentů a problémů příslušným řešitelům technické podpory,
    - nahlášení zaregistrovaného mezního stavu zákazníkovi do 30minut, s předáním doporučení pro následná rozhodnutí,
    - komunikaci se zákazníkem o provozních parametrech a událostech, a to prostřednictvím telefonu (zelená linka), e-mailu, extranetové aplikace Service Desk),
    - ověření u kontaktních osob Zadavatele, zda se nejedná o plánovanou akci,
    - nahlášení poruchy linky poskytovateli komunikačních tras,
    - nahlášení incidentu/problému Zadavateli, který se poté rozhodne o způsobu jeho vyřešení, DCA zajistí předání informace o výskytu incidentu/problému nebo mezního stavu Zadavateli už do 30 minut s tím, že do této doby provede úvodní analýzu závady a předá tak úplné vstupní informace pro následná rozhodnutí,
    - operátoři DCA se aktivně účastní řešení incidentu/problému.

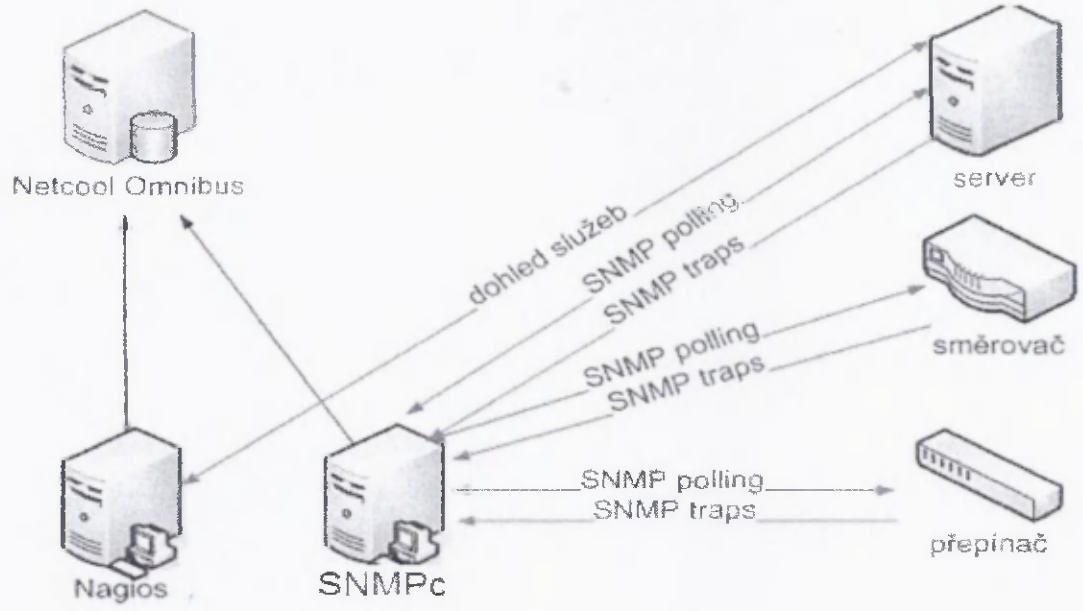
Technická specifikace systému dohledu

Služba Proaktivní dohled využívá pro zjišťování informací o zařízeních (pollingu) a příjmu událostí (eventů) protokol SNMP. Dále umožňuje zpracovávat syslog zprávy a to jak z aktivních síťových zařízení, tak ze serverů. Veškeré tyto informace se následně korelují a zpracovávají v centrálním nástroji IBM NetCool. Informace se vyhodnocují v dohledovém centru v operátorském rozhraní Netcool Webtop.

SNMP polling je iniciačně nastaven s těmito časovými hodnotami (po dohodě se Zadavatelem je možné tyto hodnoty přizpůsobit individuálním požadavkům): poll interval 60s, poll timeout 4s, poll retries 5. V konečném důsledku to znamená, že pokud zařízení neodpoví do 240 sekund, je prohlášeno za nedostupné.

Pojmy:

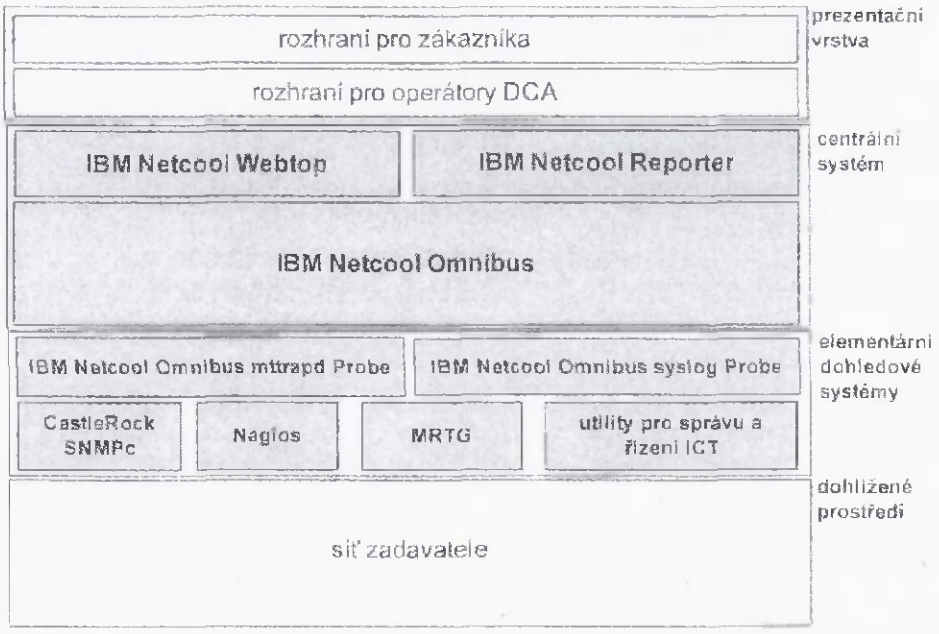
- poll interval – v jakém intervalu je iniciován SNMP polling
- poll timeout – maximální doba čekání na odezvu z pollovaného zařízení
- poll retries – počet opakování, kolikrát musí test selhat aby mohlo být zařízení vyhodnoceno jako nedostupné



Obrázek 1 Obecné schéma SNMP komunikace mezi pollovacím serverem SNMPc, centrálním management nástrojem Netcool Omnibus a dohlíženými entitami sítě

Podmínkou je umožnění přístupu na aktivní prvky protokoly ICMP Ping, SNMP, SNMP trap, případně Telnet, Syslog a dalšími podle charakteru monitorovaného systému.

Dohledový systém Uchazeče je postaven na nástrojích a postupech, které mohou být přizpůsobeny konkrétnímu prostředí a požadavkům Zadavatele. Dohledový systém uchazeče tvoří následující nástroje a řešení: IBM Netcool Omnibus, IBM Netcool mttrapd Probe, IBM Netcool syslog Probe, CastleRock SNMPc, Nagios, MRTG, Netcool WebTop, specializované utility pro správu a řízení ICT infrastruktury.



Obrázek 2 Komponenty dohledového systému Uchazeče

Elementární dohledové systémy uchazeče zabezpečují:

- dohled SNMP zařízení pomocí protokolů ICMP a SNMP (informace o zjištěném stavu jsou posílány ve formě události do centrálního systému),
- přijímání SNMP trapů a syslogů z dohlížených zařízení a následné přiřazování priorit těmto informacím,
- přijímání událostí z jiných systémů určených pro správu,
- dotazování parametrů zařízení (tzv. polling).

Centrální systém sdružuje všechny informace ze zařízení (ve formě SNMP trapů i ve formě syslogových zpráv) a také informace z jednotlivých elementárních dohledových nástrojů. Centrální systém provádí vzájemné korelace jednotlivých událostí a doplňuje je o informace z databáze dohlížených zařízení.

Prezentační vrstvu tvoří rozhraní pro operátory DCA a rozhraní pro Zadavatele - webový portál.

Služby poskytované dohledovým centrem Uchazeče

DCA pomocí výše uvedených nástrojů zabezpečuje tyto služby:

- Vzdálený proaktivní monitoring nad technickým vybavením Zadavatele nejen jako celku, ale i jejích jednotlivých rozhraní, segmentů, částí, modulů a komponent:
  - stav zařízení,
  - stav rozhraní,
  - stav IP konektivity.
- Detekci incidentů/problémů a mezních stavů.
- Dohled síťové infrastruktury s využitím umělých transakcí na úrovni sítě (využití tzv. IP SLA agentů na Cisco směrovačích Zadavatele) – tímto bude zajištěn dohled nad funkčností systémových zdrojů a jejich konfigurací, který umožní rozpoznat korektní stav dohlížených systémových zdrojů nejen z pohledu poruchy/chyby vybavení.
- Primární lokalizaci a kategorizaci incidentů/problémů na základě přijatých událostí (např. SNMP trapů, syslogů nebo informací z podpůrných management nástrojů):
  - restarty,
  - informace o interaktivních přístupech a pokusech o neoprávněný přístup na zařízení (včetně login jména a IP adresy přistupujícího klienta),
  - nedostatek paměti pro buffery (zjištěný systémem dotazováním stavu bufferů),
  - přetečení input a output queue (zjištěný systémem dotazováním vstupních a výstupních front na rozhraních),
  - stav CPU busy (dotazování využití CPU),
  - stav synchronizace času,
  - průběh pravidelných archivací (informace z podpůrného nástroje pro správu – informace o zařízeních, na kterých nebyla provedena archivace konfigurace).
- Kontrola správné konfigurace statického i dynamického směrování ve spravovaných zařízeních (systém upozorní na změny ve směrování dotazováním na směrovací tabulky a porovnáváním proti stavu během předchozího dotazování). Nalezená nesrovnalost ve směrovacích tabulkách bude řešena jako incident.
- Dohled na správnou výměnu směrovacích informací se směrovači, které nejsou předmětem správy – zpracováním trapů od zařízení (SNMP trapy o směrovacích protokolech).
- Vytvoření incidentu/problému v Service Desku.
- Pravidelný reporting Zadavateli, poskytování reportů o zaznamenaných incidentech/problémech ze nástroje Service Desk.

1.3.4. Výstup služeb

Reportování služeb dohledovým centrem uchazeče

Forma reportů a systém jejich předávání uchazeči je předmětem vzájemné dohody, obvykle je kombinací následujících možností:

- Okamžité reporty:
  - e-mail vyplněný operátorem,
  - telefonicky.
- Pravidelné reporty zasílané elektronickou poštou:
  - měsíční zpráva o zásadních řešených incidentech, shrnující stav komunikační infrastruktury,
  - denní zprávy o chybném průběhu archivace.
- Přístup ke statistikám výpadků na webovém portále:
  - přehled aktuálně nedostupných zařízení,
  - denní, týdenní, měsíční přehled aktuálně nedostupných zařízení,
  - statistiky dostupnosti jednotlivých zařízení.

Webový portál pro Zadavatele

V dohledovém systému DCA bude vytvořeno pro Zadavatele přizpůsobené rozhraní – webový portál, který bude obsahovat:

- Aktuální stav prvků sítě (včetně stavů AAA serverů) – zde budou informace nejen o dostupnosti, ale budou zde i významné události od těchto zařízení. Informace budou organizované tak, aby logicky odpovídaly současné hierarchii ÚFO (report přehledu aktuálně nedostupných zařízení).
- Rozcestník pro přístup k záznamovým souborům z aktivních síťových prvků – vytvářené mechanismem syslog, mechanismem používaným pro automatizovanou archivaci konfigurací a vytvářené systémem řízení přístupů (rozcestník bude organizovaný tak, aby logicky odpovídal současné hierarchii ÚFO).
- Přístup k historickým reportům o stavu prvků sítě:
  - týdenní přehled krátkodobých výpadků,
  - týdenní přehled závažných, řešených výpadků,
  - statistiky dostupnosti jednotlivých zařízení,
  - pravidelné měsíční výstupy ze zpracování záznamových souborů.
- Odkazy na reporty ze Service Desku:
  - v Service Desku bude přehled řešených tiketů – přizpůsobené výstupy a reporty ze Service Desku budou sloužit jako základ provozního deníku.
- Odkazy na písemné zprávy:
  - písemné zprávy pracovníků provádějících dohled o mimořádných událostech bezpečnostního nebo provozního charakteru – písemné zprávy bude vypracovávat jednou měsíčně dedikovaný pracovník Uchazeče.

Prostřednictvím webového portálu budou mít pracovníci Zadavatele zajištěn přístup k provozním informacím. Přístup bude rozčleněn dle pravomocí pracovníků Zadavatele.

Všechny provozní informace budou ukládány do historické databáze nebo do souborů. Tyto informace budou přes webový portál on-line přístupné pro čtení odpovědným pracovníkům Zadavatele (po celou dobu trvání poskytovaných služeb). Úložná doba archivních materiálů bude jeden kalendářní rok dozadu pro logy a tři kalendářní roky dozadu pro změny konfigurace sítě.

Service Desk

Uchazeč disponuje vlastním systémem Service Desk.

Uchazeč zajistí Zadavateli možnost zaznamenání, komentování, monitorování a reportování zadaných požadavků a incidentů stejným způsobem, jako v případě řešení jiných požadavků na technickou podporu – Zadavatel bude v těchto případech kontaktovat dispečink technické podpory Uchazeče.

1.3.5. Četnost služeb

Dostupnost služeb

Služby budou poskytovány průběžně.

Přímý kontakt se Zadavatelem není omezen žádným časovým intervalem, bude poskytován nepřetržitě 7 dnů v týdnu, 24 hodin denně, přičemž pro všechny způsoby komunikace (prostřednictvím internetu, emailu, telefonu včetně zelené linky i faxu) mezi Zadavatelem a poskytovatelem technické podpory **bude zajištěna nepřetržitá (7 dnů v týdnu, 24 hodin denně), fyzická přítomnost pracovníků technické podpory ANECT.**

Veškeré požadavky na poskytování technické podpory jsou vyhodnocovány a zpracovávány průběžně.

SLA

V případě závady některé ze služeb dohledu se Uchazeč zavazuje odstranit tuto závadu do 48 hodin od nahlášení.

Do2D – 7x24 (zaručená doba opravy do 48 hodin)

Servisní služba poskytovaná 7 dnů v týdnu, 24 hodin denně, s povinnosti oznámit zadavateli jméno řešitele požadavku nejpozději do 1 hodiny a odstranit závadu nejpozději do 48 hodin po elektronickém nebo faxovém potvrzení požadavku na servisní zásah.

Uchazeč se zavazuje do 5 pracovních dnů po ukončení řešení mimořádného stavu nebo bezpečnostního incidentu zpracovat zprávu a poskytnout ji dohodnutým způsobem Zadavateli.

Požadavky na služby Proaktivního dohledu lze uplatňovat 7 dnů v týdnu, 24 hodin denně.

1.3.6. Technické a organizační prostředky pro zajištění služeb

Uchazeč zajistí, že pracovníci Zadavatele budou mít průběžně zajištěn přístup ke všem výše uvedeným provozním informacím v souladu s jejich pravomocemi, že budou včas doručovány poštovní zprávy (v případě výskytu incidentů bude vždy zadavatel kontaktován další nezávislý komunikačním kanálem – telefonicky). Dále se Uchazeč zavazuje k pravidelnému předávání (případně umožní pracovníkům Zadavatele přístup) dlouhodobých vyhodnocení provozu a mimořádných událostí dohodnutou elektronickou formou.

Pro výkon služeb Proaktivního dohledu bude Uchazeč používat zabezpečený přístup do sítě FINet-ADIS pomocí dedikované WAN spojnice.