EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Výzva k podání nabídky na dodávku WiFi sítě na MČ Brno-střed

podle §6 zákona č. 134/2016 Sb., o veřejných zakázkách ve znění pozdějších předpisů, dále dle směrnice č. 9 – Zadávání veřejných zakázek dle zák. č. 134/2016 Sb. k podání nabídky

Zadavatel:

Statutární město Brno, městská část Brno-střed,
Dominikánská 2, 601 69 Brno
IČ: 44992785 01
DIČ: CZ44992785
Kontaktní osoba: Arnošt Kolbábek, vedoucí odboru informatiky, Dominikánská 2, Brno,
e-mail: arnost.kolbabek@brno-stred.cz.

Název zakázky: „Dodávka kompletního WiFi systému na MČ Brno-střed“

Druh zakázky: veřejná zakázka malého rozsahu na dodávku zboží a služeb

Lhůta pro podání nabídky začíná běžet dnem doručení výzvy a končí 14.11.2018 ve 14:00 hod.
Místo pro podání nabídky:
Portál veřejných zakázek – EZAK - https://zakazky.brno-stred.cz

Předmět zakázky:
Předmětem zakázky je vybudování wifi sítě v prostorách MČ Brno-střed – budovy na Dominikánské ulici.
Požadujeme pokrytí následujících prostorů :
Přízemí – Miniúřad, vrátnice, tajemník, sekretariát tajemníka
1-patro - Starosta a přilehlé kanceláře – sekretariát, místostarostové, sekretariát místostarostů, zasedací místnost RMČ, prostor před sekretariátem starosty
2-patro – místostarostové, sekretariáty
3-patro – zasedací salónek
Nádvoří radnice
Zasedací sál zastupitelstva
Sál za zastupitelstvem
Salonek za zastupitelstvem
Chodba matrika
Chodba bytový odbor

Technická specifikace předmětu plnění veřejné zakázky

Záruční dobu na veškerá hardwarová zařízení a zařízení pro centrální správu poskytnout v délce minimálně 24 měsíců a prokázat (potvrzení výrobce), že zařízení je určené pro trh ČR a bude vždy odborně servisováno. Zařízení nesmí překračovat při maximálních vysílacích výkonech pravidla ČTÚ a

to na všech kanálech 1-13 v pásmu 2,4 GHz a 36 - 64 a 100 - 140 v pásmu 5 GHz. Cílem ale je, aby byly kanceláře pokryty min. signálem o síle -67 dBm v obou pásmech, na chodbách je možné pokrytí o síle -67 dBm v pásmu 2,4 GHz. Dále byla zajištěna bezpečnost sítě před neoprávněným přístupem k bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup a to řídícím softwarem ve spolupráci s řídícím kontrolérem. Implementace protokolu Radius.

Požadavky na zavedení systému :

A) Nová wifi síť

- zmapování stávajícího stavu, návrh řešení a garance pokrytí vytýčených prostor
- vybudování přístupových bodů, které umožní bezdrátové připojení zařízení v rámci celé MČ
- zajištění kompletní dodávky hardwaru a softwaru nutných k vybudování a provozu sítě
- praktická realizace navrženého řešení, instalace a konfigurace
- proškolení správců sítě
- podpora (hotline)
- dodání zařízení pro centrální správu, řízení a zabezpečení přístupů uživatelů do bezdrátové sítě a do internetu

Podrobnější specifikace

A) Nová wifi síť	
zmapování stávajícího stavu, návrh řešení	• Uchazeči budou přístupné prostory budovy a bude mu umožněno provést potřebná měření signálu v budově MČ. • Uchazeči bude umožněno seznámit se se strukturou sítě pomocí konzultací se správcem sítě. • Síť musí pokrývat správcem definované prostory MČ podle požadavků správce v předmětu zakázky.
vybudování přístupových bodů, které umožní bezdrátové připojení zařízení v rámci celé MČ	• Umístění přístupových bodů je možné jen uvnitř budovy MČ. Jediná výjimka je nádvoří radnice. Přístupové body budou tvořit jednotnou síť.
zajištění kompletní dodávky hardwaru a softwaru nutných k vybudování a provozu sítě	• Hardware a software potřebný pro vybudování sítě musí umožňovat v rámci jedné instalace běh několika na sobě nezávislých SSID, centrální správa, centrální řízení přístupů.
Jak by měla celá síť fungovat:	• Wifi připojení bude možné „kdekoliv“ (specifikováno výše) a všude budou nejméně 4 nezávislé sítě (různé SSID, zabezpečení) tak, aby se kterýkoliv wifi klient mohl připojit dle potřeby do libovolné ze sítí, bude-li k tomu oprávněn. • Pro návštěvnickou wifi síť umožnit dočasné povolení připojení (podobné jako captive portal). Toto povolení po jisté nastavitelné době přestane platit. • Je nutné mít možnost detailně konfigurovat vzájemné propojení těchto sítí a možnost komunikace z nich dále do Internetu na úrovni IP adres a protokolů (IP, TCP/IP, UDP/IP, …) • Automatické „předávání“ klienta v rámci různých AP Rozdělení 4 nezávislých sítí například:

A) Nová wifi síť	
	a) Správce-úřad i) infrastruktura (switche, routery, firewally, …) b) vedení i) přístup do internetu c) hosté i) přístup do internetu d) školení Toto rozdělení není závazné, je to jen pracovní návrh a ukázka jak bychom chtěli logicky oddělovat sítě. • Trvanlivost spojení- blokování přístupu po určitou dobu • Zaznamenávat IP adresy, MAC adresy, jméno, popřípadě email a mobilní telefon v případě host autorizace (a další údaje, které půjdou zjistit.) • Blokování útočníků po nastavenou dobu. • Detailně konfigurovat vzájemné propojení sítí a možnost komunikace z nich dále do Internetu na úrovni IP adres a protokolů (IP, TCP/IP, UDP/IP,)(možnost povolení aplikací definovaných na 7. vrstvě ISO/OSI modelu") • Systém musí umožnit stanovit pravidla autentizace pro každou sít (SSID) samostatně. • Přístup do sítě je umožněn pouze zařízením a uživatelům autentizovaných pomocí 802.1X, ve specifických případech i pomocí jednotného sdíleného klíče. Přístup do Internetu je umožněn uživatelům po autentizaci přes webové rozhraní.
„Řídící kontrolér“	K řízení WiFi sítě je požadován „řídící kontrolér“, který podporuje: • Licence pro alespoň 60 zařízení • Guest access • Integrated captive portal • Automatické přelaďování RF kanálů a optimalizace vysílacího výkonu • Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti v závislosti na typu připojení • S příslušnou licencí podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control) • Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování capacity • proxy funkce pro externí RADIUS • PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST • Možnost použití a podpora TACACS+ klient pro administraci zařízení

A) Nová wifi síť	
	• Ověření uživatelů heslem nebo certifikátem • Ověření MAC adresou připojovaného zařízení • Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle: (stavu a typu koncového zařízení, uživatele (role, skupiny), místa připojení, historie připojení) • Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě • Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě • Využívání Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu“ • Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat • Zaznamenávání aktivity uživatelů a zařízení připojených k síti, možnost předání informací do Syslog serveru • Dotazovací systém, korelace záznamů, centralizované výkazy • Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, RADIUS klient pro AAA (autentizace, autorizace, accounting), dostupnost externích databází, aktivita filtrů) • Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi (kalendář přístupu) • Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů • Ověření hostů přes HTTP a HTTPS (preferujeme HTTPS) • Možnost automatického rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) • Možnost podpory BYOD, (specifické politiky pro BYOD zařízení, možnost nastavení limitu BYOD zařízení pro jednoho uživatele, interní CA, pro vydávání certifikátů BYOD zařízením, interní CA lze řetězit jako subordinate pod firemní CA • Možnost autentizace oproti AD doméně (nemusí být v trust režimu) • Podpora Multi-Domain integrace s AD • Podpora SXP (Exchange Protocol) dle IETF • Centralizovaná správa • Definice rolí administrátorů a úrovní přístupu k

A) Nová wifi síť	
	ověřovacímu systému • Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení • Grafické rozhraní pro definici pravidel přístupu k síti • Grafické rozhraní pro monitorování, definici výkazů, řešení problémů • Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture) • Podpora SNMPv3 • NTP pro synchronizaci času (všechna zařízení, i AP) • SMTP pro zasílání zpráv a výstrah přes e-mail • Podpora IPv6
Wifi Access Pointy	WiFi Access Pointy podporují: • Plné řízení kontrolérem • Antény integrované pro obě pásma, provoz v pásmu 2,4 i 5 GHz současně • Podpora minimálně 2x2 MIMO, MU-MIMO a až 80 MHz kanál pro 802.11ac wave 2 • Možnost napájení přes PoE - 802.3af / 802.3at • Min. 30 současně připojených uživatelů k jednotlivému AP • AP v zasedacím sále zastupitelstva musí současně zvládnout 120 uživatelů • Min. možnost konfigurace až 10 SSID • Podpora 1Gbps rychlosti na fyzickém Ethernet portu • Detekce cizích access pointů (Rougue AP detection), podpora spektrální analýzy (detekce zdroje rušivého signálu – interference) • Optimalizace a formování více signálů pro jednoho klienta, podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma • Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům
Proškolení správců sítě	Školení pro 2 osoby, min. délka školení 2 x 3 (45 minut) hodiny, dodané materiály (stačí elektronické), zaměřeno na praktické použití.
Podpora (hotline)	Po dobu minimálně tří měsíců od zahájení provozu zabezpečit možnost bezplatné podpory a konzultace. Další podpora dle požadavků zákazníka a dle platného ceníku dodavatele

B) Zabezpečení síťového provozu MČ	
Zmapování stávajícího stavu, návrh řešení	Uchazeči bude umožněno seznámit se se stávající strukturou sítě, pomocí konzultací se správcem sítě.
Dodání zařízení pro centrální správu pro řízení a zabezpečení přístupů uživatelů do bezdrátové sítě a do internetu	Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení, čas připojení apod.) Pokud je produkt licencován, tak je potřeba minimální licence pro 250 současně připojených uživatelů Ověření uživatelů heslem, certifikátem, SMS, mail Ověření MAC adresou připojovaného zařízení Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle: stavu a typu koncového zařízení (viz níže), uživatele (role, skupiny), místa připojení, historie připojení Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu a výstupu sítě Zaznamenávání aktivity uživatelů a zařízení připojených k síti a ve spolupráci s řídícím kontrolérem poskytuje ochranu před neoprávněným přístupem k bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů) Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů Samoobslužný portál pro hosty Ověření hostů přes HTTP a HTTPS RADIUS pro autentizaci, autorizaci, zaznamenávání (AAA). Proxy funkce pro externí RADIUS Podpora protokolů PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST Podpora pro IPv6 koncová zařízení Centralizovaná správa Grafické rozhraní pro definici pravidel přístupu k síti Grafické rozhraní pro monitorování, definici výkazů, řešení problémů

B) Zabezpečení síťového provozu MČ	
	Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture) Zaznamenávání událostí na externí syslog server Podpora SNMPv3 NTP pro synchronizaci času SMTP pro zasílání zpráv a výstrah přes e-mail
Zajištění kompletní dodávky potřebného hardwaru a softwaru	Software pro zařízení bude realizován prostřednictvím trvalých licencí.
Praktická realizace navrženého řešení, instalace a konfigurace	Zařízení musí být předáno ve funkční podobě, musí být nakonfigurováno tak, aby zabezpečilo autentizaci a autorizaci v bezdrátoví síti.
Podpora (hotline), záruka	Závazek poskytnout po dobu záruky na zařízení servis podobný NBD (next business day)
Autentizace klientů	Systém musí umožnit stanovit pravidla autentizace pro každou síť (SSID) samostatně. Přístup do sítě je umožněn pouze zařízením a uživatelům autentizovaných pomocí 802.1X, ve specifických případech i pomocí jednotného sdíleného klíče. Přístup do Internetu je umožněn uživatelům po autentizaci přes webové rozhraní.
Blokování sítě	Možnost nastavení trvanlivosti spojení- blokování přístupu po určitou dobu Zaznamenávat IP adresy, MAC adresy, jméno, popřípadě email a mobilní telefon v případě host autorizace (a další údaje, které půjdou zjistit.) Blokování útočníků po nastavenou dobu. Detailně konfigurovat vzájemné propojení sítí a možnost komunikace z nich dále do Internetu na úrovni IP adres a protokolů (IP, TCP/IP, UDP/IP,)(možnost povolení aplikací definovaných na 7. vrstvě ISO/OSI modelu")
Navázání na současné serverové řešení MČ	Je možné použít stávající servery jako zdroj externí databáze pro přihlašování. Pokud bude pro provoz Wi-Fi sítě nutný speciální server, je nutné, aby byl součástí dodávky. Možnost nasazení části systému na našem virtuálním prostředí s podporou VMware ESXi 5.5

Kabeláž a natažení přívodů k jednotlivým AP není součástí nabídky a bude zajištěno v rámci MČ po dohodě umístění AP.

Podmínky a požadavky na zpracování a podání nabídky:

Nabídka bude podána prostřednictvím Portálu veřejných zakázek _EZAK
https://zakazky.brno-stred.cz

požadavky na zpracování nabídky: součástí nabídky bude

- Krycí list nabídky – obsahuje:
  - identifikační údaje uchazeče
  - kontaktní informace
  - Celkovou nabídková cena v Kč bez DPH i s DPH, je cena celková, konečná, včetně dopravy do místa plnění – sídlo zadavatele, instalace a školení. Součástí celkové nabídkové ceny budou nabídkové ceny za každé zařízení/položku samostatně v Kč bez DPH a s DPH (pokud není dodáváno jako celek);
- Technické parametry všech nabízených zařízení
- Cenu za AP a řídící kontroler
- Cenu za systém Zabezpečení síťového provozu

Doba plnění zakázky: listopad 2018

Místo plnění zakázky: Statutární město Brno, městská část Brno-střed, Dominikánská 2, 601 69 Brno

Způsob hodnocení nabídek:
Základním hodnotícím kritériem je ekonomická výhodnost předložených nabídek. Hodnocena 100% nabídková cena.

Pro hodnocení ceny:

Nabídková cena je stanovena jako cena v Kč (bez DPH a včetně DPH), nabídkovou cenu uvede uchazeč do krycího listu nabídky.

Zadavatel nepřipouští variantní nabídky.

Ostatní:

- Dodavatel je oprávněn po zadavateli požadovat vysvětlení zadávacích podmínek. Pokud bude písemná žádost o vysvětlení, tak musí být zadavateli doručena nejpozději 4 pracovní dny před uplynutím lhůty pro podání nabídek. Zadavatel odešle vysvětlení zadávacích podmínek nejpozději do 2 pracovních dní po doručení žádosti.
- Zadavatel si vyhrazuje právo veřejnou zakázku zrušit i bez udání důvodů
- Zadavatel si vyhrazuje právo změnit nebo doplnit soutěžní podmínky, upřesnit technickou specifikaci u zařízení v průběhu lhůty pro podání nabídek a to všem zájemcům shodně
- Smlouva (objednávka), uzavřená z vítězným dodavatelem, včetně jejích případných změn, bude zveřejněna na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, vyjma informací uvedených v §7- §11 zákona. Veškeré údaje, které požívají ochrany dle

zvláštních zákonů, zejména osobní a citlivé údaje, obchodní tajemství, aj. budou anonymizovány.

- Dobu návštěvy a prohlídku prostor je nutné domluvit na tel. 542526353, p. Kolbábek

Bc. Arnošt Kolbábek

vedoucí Odboru informatika