

Smlouva

o dodávce síťových prvků

uzavřená podle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále také jako „občanský zákoník“)
mezi:

Českou národní bankou

Na Příkopě 28

115 03 Praha 1

zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky

a

Ing. Zdeňkem Virusem, ředitelem sekce správní

IČO: 48136450

DIČ: CZ48136450

(dále jen „objednatel“)

a

CompuNet s. r. o.

Zubatého 295/5

150 00 Praha 5

IČO: 276 08 514

DIČ: CZ27608514

zastoupenou: Ing. Pavlem Pikhartem, jednatelem

č. účtu: 51-1998450287, kód banky: 0100

(dále jen „dodavatel“)

Článek I

Předmět smlouvy

1. Dodavatel se touto smlouvou zavazuje dodat objednateli zařízení dle specifikace stanovené v příloze č. 1 – „Technická specifikace zařízení“ (dále jen „zařízení“). Zařízení musí splňovat minimální požadavky stanovené v rámci přílohy č. 2 – „Technické požadavky objednatele a popis stávajícího řešení“.
2. Dodavatel se zavazuje se zařízením dodat veškeré doklady a dokumentaci potřebné k řádnému užívání, zejména návod k použití/montáži v českém jazyce a prohlášení o shodě.
3. Objednatel se zavazuje uhradit cenu podle čl. III smlouvy.

Článek II

Lhůta, předání a převzetí plnění

1. Smluvní strany se dohodly, že zařízení budou předána objednateli nepozději do 60 kalendářních dnů od podpisu smlouvy.
2. Dodavatel sdělí pověřené osobě objednatele zamýšlené datum a čas předání nejméně 3 pracovní dny předem.

3. Místo předání plnění je adresa sídla objednatele: Senovážné náměstí 30, 115 03 Praha 1.
4. Zařízení budou předána protokolem o předání a převzetí podepsaným pověřenými osobami objednatele a dodavatele.

Článek III **Cena a platební podmínky**

1. Cena plnění dle této smlouvy činí 1 802 302 Kč bez DPH. Bližší specifikace ceny je uvedena v cenové tabulce, která tvoří přílohu č. 3 smlouvy.
2. K ceně plnění dle této smlouvy bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění. Cena zahrnuje veškeré náklady dodavatele spojené s plněními podle této smlouvy včetně nákladů na poskytování nových verzí firmware podle čl. IV odst. 6.
3. Cenu plnění uhradí objednatel dodavateli na základě daňového dokladu vystaveného dodavatelem nejdříve v den podpisu protokolu o předání a převzetí plnění.
4. Daňové doklady budou vedle náležitostí stanovených zákonem o DPH, a dále § 435 zákona č. 89/2012 Sb., občanský zákoník, obsahovat i evidenční číslo smlouvy ČNB a bankovní účet, na který má být placeno a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován dodavatelem (dále jen „určený účet“). Daňový doklad bude nadto obsahovat náležitostí stanovené v zákoně o dani z přidané hodnoty. V případě, že doklad bude postrádat některou ze stanovených náležitostí, nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit dodavateli. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu.
5. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřená osoba dodavatele povinna na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zapláceno na bankovní účet uvedený v dokladu k úhradě, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení dodavatele podle předchozí věty.
6. Doklady k úhradě bude dodavatel zasílat elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e-mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Ve formátu ISDOC se číslo smlouvy uvádí v poli ID ve skupině Contract References. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem elektronické faktury. Nebude-li možné daňový doklad zaslat elektronicky, zašle dodavatel daňový doklad v analogové formě na adresu objednatele:

Česká národní banka
sekce rozpočtu a účetnictví
odbor účetnictví
Na Příkopě 28
115 03 Praha 1.
7. Splatnost daňového dokladu je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu dodavatele.
8. Smluvní strany se dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za dodavatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce dodavatele za objednatel, ať splatné či nesplatné.

Článek IV

Záruka za jakost a ohlašování vad

1. Dodavatel poskytuje na dodaná zařízení záruku v délce 24 měsíců. Po tuto dobu se zavazuje dodavatel odstraňovat na vlastní náklady veškeré záruční závady. Záruční doba počíná běžet dnem převzetí plnění objednatelem.
2. Potřeba záruční opravy bude objednatelem ohlašována na kontaktní e-mailovou adresu dodavatele: helpdesk@compunet.cz, nebo na telefonní číslo 226 776 664 s následným písemným potvrzením e-mailem na výše uvedenou e-mailovou adresu dodavatele.
3. Záruční vada musí být odstraněna nejpozději do 3 pracovních dnů od jejího nahlášení, pokud si pověřené osoby smluvních stran písemně nedohodnou jinou lhůtu k odstranění vady. Záruční opravy mohou být prováděny v místě plnění pouze v pracovní dny v době od 8:00 do 18:00 hod.
4. Dodavatel je povinen nahlásit případnou změnu kontaktní údajů uvedených v odst. 2 tohoto článku nejpozději následující pracovní den po provedení změny, bez potřeby uzavření dodatku k této smlouvě.
5. Dodavatel je srozuměn s tím, že veškerá komunikace při hlášení a řešení závad bude mezi objednatelem a pracovníky dodavatele probíhat v českém jazyce.
6. Dodavatel poskytne objednateli po dobu trvání záruky všechny relevantní verze firmware nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání objednatele a fungovalo bez závad.
7. Dodavatel je povinen zajistit objednateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
8. Objednatel musí mít možnost se sám zaregistrovat na stránkách výrobce a musí mít možnost samostatného stahování nových verzí firmware a registrace k odběru automatických e-mailových zpráv týkajících se dodávaných zařízení a upozorňující na tyto skutečnosti:
 - a. bezpečnostní incidenty, které vyžadují od objednatele povýšení operačního systému/firmware či aplikování změny konfigurace či opravy (záplaty),
 - b. konec prodeje či podpory,
 - c. nové verze operačního systému/firmware,
 - d. známé chyby operačního systému/firmware.
9. Servisní zásahy v rámci záruky budou přednostně prováděny v místě plnění. Závada, jejíž odstranění z jakýchkoliv důvodů nebude na místě možné, nebo vhodné, bude řešena výměnným způsobem. Veškerá manipulace s opravovanou komponentou bude protokolárně zaznamenána. V případě, že oprava vadné komponenty nebude možná, bude předmětná komponenta nahrazena novou stejných nebo lepších parametrů, na níž bude možno provozovat stejný firmware jako na původní.

Článek V

Vlastnické právo a nebezpečí škody

1. Vlastnické právo k zařízením a nebezpečí škody přechází na objednatele okamžikem podepsání protokolu o předání a převzetí plnění dle čl. II odst. 4.

Článek VI

Smluvní pokuta, úrok z prodlení

1. V případě prodlení dodavatele ve lhůtě pro předání celého plnění podle čl. II odst. 1 je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý den prodlení.
2. V případě prodlení dodavatele s nástupem k opravě vady nebo s odstraněním vady ve stanovené lhůtě je objednatel oprávněn požadovat smluvní pokutu ve výši 100 Kč za každý pracovní den prodlení.
3. V případě prodlení objednatele s úhradou daňového dokladu je dodavatel oprávněn požadovat úrok z prodlení podle nařízení vlády č. 351/2013 Sb.
4. Splatnost dokladu k úhradě smluvní pokuty nebo úroku z prodlení je 14 dnů od doručení příslušného dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
5. Smluvní pokutou není dotčeno právo na náhradu škody.

Článek VII

Pověřené osoby smluvních stran

1. Smluvní strany se dohodly, že seznam pověřených osob včetně telefonického a e-mailového spojení si smluvní strany vzájemně sdělí e-mailem na adresu objednatele: servis.zarizeni@cnb.cz a na adresu dodavatele: helpdesk@compunet.cz

Článek VIII

Odstoupení od smlouvy

1. Objednatel si vyhrazuje právo odstoupit od této smlouvy v celém či částečném rozsahu v případě, že:
 - a) dodané zařízení nebude splňovat specifikaci dle přílohy č. 1 nebo přílohy č. 2 této smlouvy,
 - b) dodavatel bude v prodlení s plněním delším než 30 dnů.
2. Odstoupení od smlouvy je účinné doručením písemného oznámení o odstoupení dodavateli.

Článek IX

Uveřejnění smlouvy a skutečně uhrazené ceny

1. Dodavatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků a výši skutečně uhrazené ceny za plnění této smlouvy.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“) uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je <https://ezak.cnb.cz/>.
3. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 219 ZZVZ.
4. Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek X

Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.
2. Smlouvu je možno měnit nebo doplňovat pouze formou písemných chronologicky číslovaných dodatků podepsaných oprávněnými zástupci smluvních stran, vyjma případů uvedených v této smlouvě.
3. Závazkový vztah založený touto smlouvou, se řídí českým právním řádem, zejména zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
4. Smlouva se vyhotovuje ve třech stejnopisech, z nichž objednatel obdrží dva stejnopisy, dodavatel jeden stejnopis.

Přílohy:

- č. 1 Technická specifikace zařízení
- č. 2 Technické požadavky objednatele a popis stávajícího řešení
- č. 3 Cenová tabulka

V Praze dne 24. 9. 2019

V Praze dne 19. 9. 2019

Za objednatele:

[Redacted signature]

Ing. Milan Zirnsák
ředitel sekce informatiky

[Redacted signature]

Ing. Zdeněk Virius
ředitel sekce správ

[Redacted signature]

ČNB ČESKÁ NÁRODNÍ BANKA
Na Příkopě 28, 115 03 Praha 1
48

Za dodavatele:

[Redacted signature]

Ing. Pavel Pikhart
jednatel

CompuNet s.r.o.
Zubatého 295/5
150 00 Praha 5
08514, DIČ: CZ27608514

Technická specifikace zařízení

| POPIS | PRODUKT. OZN. | POČET |
|--|---------------|-------|
| Aruba AP-315 802.11n/ac 2x2:2/4x4:4 MU-MIMO Dual Radio Integrated Antenna AP | JW797A | 170 |
| AP-220-MNT-W1W Flat Surface Wall/Ceiling White AP Basic Flat Surface Mount Kit | JW047A | 170 |
| Aruba ClearPass C2000 DL20 Gen9 HW Appliance | JZ509A | 2 |
| HPE 3Y Partner-Branded NBD Support SVC - HPE Aruba CP C2k DL20 G9 HW Appl Support [for JZ509A] | H1L06A3#Y1P | 2 |
| Aruba ClearPass NL AC 500 CE E-LTU | JZ401AAE | 1 |
| HPE 3Y Partner-Branded NBD Support SVC - HPE Aruba ClearPassNLAC500 CE E-LTU Supp [for JZ401AAE] | H1L06A3#Y1W | 1 |
| Aruba 7205 (RW) 2-port 10GBASE-X (SFP+) Controller | JW735A | 1 |
| PC-AC-EC Continental CZKopean/Schuko AC Power Cord | JW118A | 1 |
| Aruba LIC-AP Controller per AP Capacity License E-LTU | JW472AAE | 170 |
| Aruba LIC-PEF Controller Policy Enforcement Firewall Per AP License E-LTU | JW473AAE | 170 |
| HPE 3Y Partner-Branded NBD Support SVC - HPE Aruba 7205 Controller Supp [for JW735A] | H1L06A3#XA4 | 1 |
| HPE 3Y Partner-Branded NBD Support SVC - HPE Aruba Cntrl per AP Capcty E-LTU Supp [for JW472AAE] | H1L06A3#ZXQ | 170 |
| HPE 3Y Partner-Branded NBD Support SVC - HPE Aruba License PEF Contro Supp [for JW473AAE] | H1L06A3#XS4 | 170 |

Technické požadavky objednatele a popis stávajícího stavu

1. Technické požadavky objednatele

1.1 AP – přístupové body (Wifi vysílače)

- počet kusů: 170
- třída zařízení: indoor AP
- uzavřená konstrukce bez ventilátorů
- podpora bezdrátového standardu: 802.11ac Wave2
- certifikace Wi-Fi Alliance: IEEE 802.11a/b/g/n/ac
- pracovní režim AP řízené kontrolérem (lightweight)
- počet portů ethernet LAN: 1x10/100/1000 Mbit/s RJ45 (minimální počet)
- podpora standardů IEEE 802.3af (PoE) a IEEE 802.3at (PoE+)
- podpora standardního PoE 15,4W bez nutnosti redukce výkonu 5GHz rádia
- podpora napájení z AC napájecího zdroje
- vestavěná interní anténa: MIMO, omni down-tilt
- radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz
- MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2
- MIMO a počet nezávislých streamů na 5GHz rádio: 4x4:4
- podpora šířky kanálu 160MHz
- podpora MU-MIMO
- automatické ladění kanálu a síly signálu v koordinaci s ostatními AP
- komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 1.73 Gbit (minimální rychlost)
- podpora 802.11ac explicitního beamformingu
- počet inzerovaných SSID (BSSID) na rádio: 16
- mapování SSID do různých VLAN podle IEEE 802.1Q
- podpora spektrální analýzy
- hardware filtry pro filtraci intermodulačního rušení pocházejícím z mobilních sítí (Advanced Cellular Coexistence) nebo obdobné
- 802.11w ochrana management rámců
- SSHv2, SNMPv2c a SNMPv3
- součástí AP je příslušenství pro montáž na zeď nebo strop
- kompatibilní s dodaným kontrolérem

1.2 Centrální kontroler pro správu přístupových bodů

- počet kusů: 1
- forma dodání: fyzická appliance
- velikost umožňující montáž do standardního 19" datového rozvaděče
- napájecí zdroj: 1x interní AC
- počet kombo portů gigabit ethernet: 4x 1000BASE-T/SFP combo

- počet optických portů 10Gbit/s s volitelným fyzickým rozhraním: 2x 10Gbit/s SFP+ (minimální počet)
- podporovaný počet AP bez nutnosti přidávání hardware: 256 (minimální počet)
- podporovaný počet současně připojených klientů: 8000 (minimální počet)
- výkon statefull firewallu: 12 Gbit/s, 1mil. Session (minimální počet)
- sdílení licencí mezi více kontrolery
- podpora Redundance (HA) kontrolerů v režimech: active-active a active-standby. Výpadek aktivního kontroleru v redundantním páru nemá dopad na provoz již připojených klientů (tj. bez potřeby opětovné autentizace).
- vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP, podpora roamingu přes AP na vzdálené lokalitě
- podpora VLAN podle IEEE 802.1Q: ano, 4000 aktivních VLAN (minimální počet)
- počet záznamů v tabulce MAC adres: 32000 (minimální počet)
- podpora linkové agregace IEEE 802.3ad
- IEEE 802.1w - Rapid spanning Tree
- podpora STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- detekce protilehlého zařízení LLDP
- statické směrování IPv4 a IPv6
- dynamické směrování OSPFv2 včetně podpory stub a NSSA
- podpora Multicast: IGMP a MLD
- NTP včetně MD5 autentizace
- podpora překladu adres PAT/NAT
- podpora standardu 802.11ac Wave 2 a zpětná kompatibilita s 802.11a/b/g/n
- režimy přenosu uživatelských dat: tunelování přes kontrolér a lokální AP bridging
- VLAN Pooling
- podpora IPv6: konfigurace, správa (SSH, SNMP, Syslog, DHCPv6,RADIUS), syst. komunikace mezi AP a kontrolérem. Kompatibilita s RFC 2460, RFC 3162, RFC 3736, RFC 6106
- typy autentizace: WPA/WPA2-PSK, WPA/WPA2-Enterprise, 802.1X, MAC autentizace, "captive portal", 802.1X ověření s následným ověřením MAC
- podporované autentizační/autorizační zdroje: RADIUS, LDAP, Active Directory, RFC 3576 Change of Authorization
- funkce řízení a ochrany rádiového spektra s automatickou optimalizací sítě (přidělování kanálů, fast roaming, rozdělení klientů na jednotlivá AP)
- aktivní scanování 802.11 kanálů pro výběr nejlepšího včetně automatického zastavení scanování v případě že probíhá časově senzitivní provoz (např. VoIP)
- klasifikace klientských zařízení do tříd na základě typu nebo OS zařízení a následné uplatnění definovaných politik pro danou třídu
- vestavěný "captive portal" pro hosty s podporou nativních IPv6 klientů. S možností úpravy vzhledu a přidáním vlastního loga včetně vestavěného rozhraní pro vytváření dočasných guest účtů.
- podpora pro 802.11u, 802.11v a 802.11k
- automatické dynamické rozpoznání a prioritizace hlasových protokolů jako SIP, SCCP, VOCERA a SVP pomocí funkce DPI a jejich SLA monitoring
- podporované úrovně oprávnění v administračním rozhraní: administrator, read-only, guest-provisioning
- podpora XML a REST API pro automatizovanou konfiguraci kontroléru

- automatizovaná migrace klientů na optimální frekvenci, AP či rádio s využitím min. těchto parametrů: kategorie daného klienta, SNR, schopnosti klienta, kvalita signálu
- grafický uživatelský dashboard zobrazující kvalitu a obsazenost kanálů, jednotlivé klienty, náhledy na VoIP přes WiFi síť a zobrazující informace o MOS (mean opinion score) aktivních hovorů. Možnost realtime analýzy kvality prováděných hovorů
- podpora rozpoznávání aplikací na 7. vrstvě (aplikace typu: Youtube, Facebook, Dropbox, BitTorrent, Skype, Office365, apod.). Možnost jejich povolování, zakazování, prioritizace nebo omezování s možností vytvořit minimálně 20 souběžných aplikačních pravidel k omezení provozu konkrétních aplikací.
- centrální správa, aktualizace, konfigurace vč. bezpečnostních politik a QoS profilů pro všechna AP
- blacklist zařízení překračující nastavitelné prahy (opakovaná autentizace, porušení bezpečnostní politiky)
- podpora RadSec (RADIUS over TLS)
- podpora tvorby bezpečnostních politik na základě časových pravidel
- podpora L2 a L3 roaming bez nutnosti speciálního SW na klientovi
- podpora Rogue Wireless detekce a containment
- podpora PKI
- možnost terminace vzdálených VPN klientů (podpora SSL i IPSec VPN)
- podpora WIPS pro detekci útoků na bezdrátovou síť
- podpora spektrální analýzy
- podpora ochrany pomocí IDS signatur
- ochrana řídicích rámců - 802.11w
- CLI formou RJ45 serial konsolové port
- ethernet port pro out-of-band management
- dual boot flash
- podpora SSHv2 a HTTPS web GUI
- SNMPv2c, SNMPv3
- nástroj pro odchyťování WLAN datového provozu včetně 802.11 hlaviček a možnost jeho zasílání do Ethernetového analyzátoru
- podpora upgrade firmware pomocí: HTTPS, TFTP, FTP a USB
- plná kompatibilita s nabízenými přístupovými body
- kompatibilní s kontrolerem Aruba 7205 (RW) - ve smyslu vytvoření clusteru AOS 8.X

1.3 Radius server

- počet kusů: 2
- forma dodání: fyzická appliance
- velikost umožňující montáž do standardního 19" datového rozvaděče
- celková kapacita řešení pro počet současně autentizovaných uživatelů: 5000 (minimální počet)
- licenční pokrytí pro 500 uživatelů (minimální počet)
- řešení musí poskytovat vysokou dostupnost tak aby v případě výpadku primárního AAA serveru převzal jeho roli sekundární server
- řešení musí umožňovat distribuci přes cluster minimálně 30ti virtuálních či fyzických appliance pro možnost distribuce zátěže a geografické zálohování
- možnost napojení se až na 30 Active Directory zdrojů pro geografické zálohování externí databáze identit

- podpora 802.1X a TACACS+ autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení
- podpora mechanismu řízení přístupu do sítě pro aktivní prvky plně nepodporující 802.1X. Zjištění připojeného uživatele skrze WMI. Vynucení politik připojení a detekce připojené stanice skrze SNMP.
- konfigurace autentizačních politik v rámci clusteru je centralizována a nevyžaduje manuální znovukonfiguraci na každém appliance
- cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance
- podpora následujících výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě): CISCO, HPE (Aruba Networks), Juniper, Meraki, Ruckus, Linksys, Huawei, Netgear, ZyXEL, TP-Link
- požadované metody autentizace uživatelů a zařízení: PEAP-MSCHAPv2, EAP-TLS, EAP-FAST, EAP-TTLS, MAC autentizace, povolení MAC autentizace neznámých klientů
- podpora RADIUS CoA dle RFC3576
- podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD
- možnost TACACS+ autentizace správců síťových zařízení
- další požadované autentizační a autorizační zdroje a metody: LDAP, Microsoft AD, Token, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth)
- možnost integrace s MDM (Mobile Device Management) platformami třetích stran. Minimálně tři výrobci MDM řešení (airwatch, SOTI, XenMobile, MaaS360, Microsoft Intune).
- podpora REST API pro většinu základních úkonů AAA platformy
- podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.). Administrátor musí mít možnost konstruovat vlastní obsah http REST API volání založených na proměnných daného autentizačního kontextu.
- zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení.
- administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran
- sběr dodatečných informací o připojených zařízeních ("profiling") jako jsou DHCP volby klienta, HTTP uživatelský agent, předvolba MAC adresy či stav otevřených portů daného zařízení. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě. Informace pro profiling musí být možné získat přímým monitorováním provozu, přímo jako výsledek práce aktivních prvků, příjmem flow metadata informací skrze API a integrovaným NMAP skenovacím nástrojem.
- podpora LAN a WLAN portálu pro hosty s HTTP/HTTPS autentizací. Možnost vytváření dočasných uživatelských guest účtů skrze netechnické uživatelské rozhraní odděleného od hlavního administrativního rozhraní.
- LAN a WLAN Guest portál musí umožňovat grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě pomocí SMS a ověřením emailem.
- funkce portálu pro hosty je řešena stejnými licencemi jako základní řízení přístupu. Pokud ne, je třeba nabídku doplnit o guest licence ve stejném počtu.

- možnost rozšíření systému o bezpečnou registraci soukromých zařízení do interní sítě na základě uživatelských údajů externí autentizační databáze jako např. AD či LDAP. Uživatel musí být schopen jednoduchým uživatelským wizardem instalovat osobní certifikát a síťový profil na své soukromé zařízení (BYOD systém). Certifikační autorita pro vydávání certifikátů na soukromá zařízení musí být součástí AAA platformy.
- podpora protokolu SCEP
- hosté či interní uživatelé musí mít možnost přístupu do samoobslužného portálu pro správu svých vlastních registrací
- jakékoliv funkční rozšíření systému musí být vždy v rámci stejné hardwarové appliance jako je AAA systém

2. Popis stávajícího řešení

Bezdrátová síť ČNB je provozována na mobility kontroleru Aruba 7205 a je osazena bezdrátovými vysílači AP-315. Radius server je realizována iMC UAM modulem, který využívá jako zdroj uživatelských certifikátů AD. Uživatelé jsou přiřazováni do jednotlivých VLAN na základě definovaných politik (802.1X). Řešení správy přístupu do bezdrátové sítě krom 802.1X autentizace zajišťuje rovněž portál pro přístup hostů a management (generování) ticketů.

Cenová tabulka - Obnova bezdrátové sítě - WIFI

| Položka | Popis | Cena za 1 ks v Kč bez DPH* | Požadovaný počet ks | Cena za všechny ks v Kč bez DPH |
|----------------------------|--|----------------------------|---------------------|---------------------------------|
| 1 | Wifi vysílač (AP) včetně příslušenství | 6 234,00 | 170 | 1 059 780,00 |
| 2 | Kontroler | 357 746,00 | 1 | 357 746,00 |
| 3 | Radius server | 192 388,00 | 2 | 384 776,00 |
| Cena celkem bez DPH | | | | 1 802 302,00 |