TURIMOS TELEFONINĖS ĮRANGOS PRITAIKYMO PAKETINIO KOMUTAVIMO TECHNOLOGIJOMS TECHNINĖ SPECIFIKACIJA

1. Pirkimo objektas

1.1. Pirkimo objektas – Bendrojo pagalbos centro (toliau – BPC) informacinės sistemos (toliau – BPCIS) telefoninės įrangos BPC padalinyje Vilniuje pritaikymo paketinio komutavimo technologijoms įsigijimas, įdiegimas, konfigūravimas ir paruošimas naudoti.

2. BPCIS telefoninės įrangos komplektacija ir aprašymas

2.1. Telefoninę techninę ir programinę įrangą, esančią Petro Vileišio g. 20A, Vilnius, sudaro:

2.1.1. techninė įranga – Unify OpenScape 4000 V8 Duplex (Siemens HiPath 4000 V8), kurią sudaro:

2.1.1.1. 3 stacionarios išplėtimo lentynos AP 3700-13;

2.1.1.2. 2 nutolusios išplėtimo lentynos AP3700-9IP;

2.1.1.3. 7 DIU-N2 2-jų ISDN PRI E1 srautų plokštės;

2.1.1.4. 2 DIUT2-E1 2-jų ISDN PRI E1 srautų plokštės;

2.1.1.5. 6 SLMO24 – 24-ių skaitmeninių stoties abonentų pajungimo plokštės (Up0e);

2.1.1.6. 2 STMI4 VoIP abonentų pajungimo plokštės (VoIP Gateway);

2.1.1.7. 3 LTUCA stacionarių išplėtimo lentynų pajungimo plokštės;

2.1.1.8. 1 STMD3 8 prievadų ISDN BRI (S0) pajungimo plokštė;

2.1.1.9. 2 STHC kombinuota 4xISDN BRI (S0) ir 16 skaitmeninių stoties abonentų pajungimo plokštės;

2.1.1.10. 1 SLMAV – 24-ių analoginių abonentų pajungimo plokštė;

2.1.1.11. 1 SLMA24 - 24-ių analoginių abonentų pajungimo plokštė;

2.1.1.12. 2 NCUI4 – nutolusių IP lentynų pajungimo plokštės;

2.1.1.13. 730 OpenScape 4000 V10 Flex abonentų ir prievadų licencijų.

2.1.2. programinė įranga — Unify OpenScape Contact Center Enterprise Edition V9 (Siemens OpenScape Contact Center Enterprise V9).

3. Reikalavimai BPCIS telefoninės rangos atnaujinimui

3.1. Telefoninė įranga Unify OpenScape 4000 V8 Duplex (Siemens HiPath 4000 V8) esanti Petro Vileišio g. 20A, Vilnius, turi būti atnaujinta į Unify Openscape 4000 V10 Duplex.

3.2. Programinė įranga Siemens Unify OpenScape Contact Center Enterprise Edition V9 (Siemens OpenScape Contact Center Enterprise V9), esanti Petro Vileišio g. 20A, Vilnius, turi būti atnaujinta į Unify OpenScape ContactCenter V11.

3.3. Atnaujinant telefoninę (techninę) įrangą tiekėjas privalo:

3.3.1. užtikrinti sistemos perjungimą per minimalų laiką, minimaliai sutrikdant bazinių paslaugų veikimą viename centre (ne daugiau 5 min.), ne piko (nakties) metu, įskaitant nutolusius Vilniaus BPCIS stoties modulius Panevėžio Greitosios medicinos pagalbos stotyje (toliau – GMPS) ir BPC Alytaus skyriuje;

3.3.2. užtikrinti sistemos perjungimą per minimalų laiką, minimaliai sutrikdant visų esamų paslaugų (išskyrus bazines) veikimą viename centre (ne daugiau 4 val.), įskaitant nutolusius Vilniaus BPCIS stoties modulius Panevėžio GMPS ir BPC Alytaus skyriuje;

3.3.3. užtikrinti visų esamų ir šiuo metu naudojamų paslaugų analogišką veikimą;

3.3.4. užtikrinti atnaujintos sistemos patikimumą ne mažesnį nei yra prieš atnaujinimą;

3.3.5. užtikrinti visų reikalingų licencijų pateikimą ir (arba) perkėlimą;

3.3.6. užtikrinti BPC administracijai teikiamų telefonijos paslaugų teikimą;

3.3.7. užtikrinti visų automobilyje integruoto avarinio skambučio eCall funkcijų veikimą;

3.3.8. užtikrinti balso pranešimų įrenginių (Interalia XMU) veikimą;

3.3.9. užtikrinti atnaujintų stočių laiko sinchronizavimą su Vidaus reikalų ministerijos laiko serveriu;

3.3.10. įdiegti funkciją, leidžiančią įkelti muzikos/pranešimo garso įrašą ir jį transliuoti skambučio užlaikymo metu (konferencijos organizavimo metu, BPC operatoriaus konsultacijos metu, 2-jų žingsnių skambučio peradresavimo metu);

3.3.11. užtikrinti skambinančiojo numerių transliavimą tiek įeinantiems skambučiams, tiek ir išeinantiems taip, kad transliavimas nesikeistų nuo šiuo metu naudojamo (užtikrinant skambinančiojo vietos nustatymo duomenų (toliau – VND) priėmimą ir atvaizdavimą, integracijos su Kauno, Klaipėdos, Šiaulių ir Vilniaus GMPS veikimą, korektišką išeinančių iš BPC telefono numerių transliavimą užklausose į mobiliojo ryšio tinklus ir kt.);

3.3.12. įdiegti priemones, leidžiančias nedelsiant identifikuoti OpenScape 4000 ISDN PRI sąsajų atskirų srauto B kanalų blokavimą dėl atsiradusių klaidų tinkle;

3.3.13. pateikti reikiamą serverinę įrangą Unify OpenScape ContactCenter V11 stabiliam dubliuotam veikimui;

3.3.14. pateikti detalų atnaujinimo planą užtikrinant nepertraukiamą 112 paslaugos teikimą. Nurodyti šalių atsakomybes plano įgyvendinimui.

3.4. Atnaujinant programinę įrangą tiekėjas privalo:

3.4.1. užtikrinti sistemos perjungimą per minimalų laiką, užtikrinant nepertraukiamą BPC teikiamų paslaugų veikimą, įskaitant nutolusius naudotojus Panevėžio GMPS ir BPC Alytaus skyriuje;

3.4.2. užtikrinti visų esamų ir šiuo metu naudojamų paslaugų analogišką veikimą po sistemos atnaujinimo;

3.4.3. užtikrinti visų CTI (angl. *Computer Telephone Interface*) funkcijų veikimą, įskaitant ir telefoninių pokalbių ir duomenų paskirstymą ir pateikimą BPC operatoriams, naudojantiems pagalbos skambučių priėmimo ir administravimo programinę įrangą „Siveillance“;

3.4.4. Privalo užtikrinti šių telefonijos funkcijų vykdymą per CTI sąsają: telefono valdymas, skambučių peradresavimas pagal „Siveillance“ telefono numerių DB, konferenciniai pokalbiai, pokalbio persiuntimas, konsultacija, operatoriaus prisijungimas/atsijungimas bei būsenos keitimas (pasirengęs/pertrauka).

3.4.5. užtikrinti visų esamų VND ir AML (angl. *Advanced Mobile Location*) funkcijų veikimą;

3.4.6. užtikrinti visų automobilyje integruoto avarinio skambučio eCall funkcijų veikimą integraliai su NG/IMS eCall 2.0 ir 3.0 eCall BDR dekoderiais;

3.4.7. užtikrinti eCall BDR atnaujinimo skambučio metu ir po perskambinimo funkcijas.

3.4.8. užtikrinti analogiškų esamoms BPC operatorių darbo stebėjimo priemones (realaus laiko statistiką ir būsenų stebėjimą);

3.4.9. perkelti esamą naudotojų konfigūraciją įskaitant naudotojų paskyras, teises, žinių lygius (angl. *Skill Levels*);

3.4.10. užtikrinti, kad BPCIS naudojamo įvykių ir pokalbių informacijos susiejimo modulis galėtų susieti užregistruotus įvykius su pokalbiais iš karto, kai tik įvykis užregistruojamas, nelaukiant duomenų atnaujinimo Unify OpenScape Contact Center istorinės informacijos duomenų bazėje (15 min. intervalais);

3.4.11. Užtikrinti BPCIS naudojamo ataskaitų modulio (kurio vienas iš pagrindinių duomenų šaltinių yra OpenScape Contact Center) visų ataskaitų tikslumą po sistemos atnaujinimo;

3.4.12. užtikrinti atnaujintos sistemos patikimumą ne mažesnį nei yra prieš atnaujinimą;

3.4.13. užtikrinti visų reikalingų licencijų pateikimą;

3.4.14. užtikrinti skambučių iš įrenginių be SIM kortelių apdorojimą analogiškai esamam apdorojimui;

3.4.15. užtikrinti naudojamų balso pranešimų (eilės, laikino blokavimo, skambučių iš įrenginių be SIM kortelių) veikimą;

3.4.16. turi priimti ir apdoroti geografinės vietos įrašą SIP antraštėje (angl. *Header*) ir pagal jį skirstyti skambučius ir kitokius komunikacijos būdus pagal pasirinktas skirtumo taisykles.

3.4.17. užtikrinti laikinai blokuojamų numerių posistemio veikimą;

3.4.18. parengti ir pateikti atnaujintos telefoninės įrangos architektūros dokumentą;

3.4.19. parengti ir pateikti techninės ir programinės įrangos administravimo/konfigūravimo vadovą/instrukciją;

3.4.20. parengti ir pateikti programinės įrangos naudotojo vadovą/instrukciją;

3.4.21. parengti ir pateikti telefoninės įrangos atnaujinimo priėmimo testavimo scenarijus;

3.4.22. parengti ir pateikti techninės ir programinės įrangos garantinės priežiūros reglamentą

3.4.23. atlikti BPCIS administratorių mokymus susijusius su programinės įrangos konfigūravimu.

4. SIP sesijų ugniasienės valdiklio įrangos įdiegimas, suderinimas ir sukonfigūravimas

4.1. Tiekėjas privalo pateikti, įdiegti, suderinti su telefonine įranga ir atitinkamai sukonfigūruoti 2 vienetus SIP sesijų ugniasienės valdiklių (angl. *Sesssion Border Controller,* toliau – valdikliai).

4.2. Valdikliai turi būti visiškai suderinami su atnaujinta BPCIS telefonine įranga.

4.3. 2 vienetai valdiklių turi būti įdiegti adresu Petro Vileišio g. 20A

4.4. Valdiklius turi sudaryti techninė (aparatinė) įranga ir programinė įranga.

4.5. Turi būti užtikrintas valdiklių dubliavimas, užtikrinantis paslaugos teikimo nenutrūkstamumą vieno iš valdiklių gedimo atveju.

4.6. Teikėjas privalo būti programinės įrangos gamintojo partneris, turintis teisę parduoti siūlomą programinę įrangą. Turi būti pateiktos tai patvirtinančių dokumentų kopijos.

4.7. Programinės įrangos licencijų gamintojo palaikymo sąlygos turi leisti iš gamintojo gauti ir naudoti paskutinę programinės įrangos versiją bei atnaujinimus be papildomo mokesčio visu licencijos galiojimo laikotarpiu.

4.8. Valdikliai turi palaikyti atskiras tinklo sąsajas, skirtas valdymo prieigai, didelio pasiekiamumo klasterio veikimui, signalizacijai ir medijai;

4.9. Valdiklių virtualaus įrenginio medijos ir signalizacijos tinklo sąsajos turi būti programiškai konfigūruojamos tiek vidiniams tiek išoriniams sujungimams be apribojimų;

4.10. Valdikliai turi turėti funkciją būti konfigūruojamas veikti vienu metu tiek kaip prieigos įrenginys, aptarnaujantis individualių SIP abonentų registracijas, tiek kaip apjungimo įrenginys, sujungiantis skirtingus SIP ryšio tiekėjus su IP PBX telefonijos serveriais.

4.11. Valdikliai privalo užtikrinti tinklo topologijos slėpimą, veikdami *Back-to-Back User Agent (B2BUA)* būdu.

4.12. Valdikliai turi užtikrinti kliento infrastruktūros kibernetinę apsaugą, apsaugą nuo perkrovos, dinaminę ir statinę prieigos kontrolę bei patikimų įrenginių klasifikavimą ir atskyrimą L3–L5 lygmenyje.

4.13. Valdikliai privalo užtikrinti būseną, saugančią giliąją paketų kontrolę (angl. *Deep Packet Inspection*);

4.14. Valdiklio apsauga nuo DoS atakų privalo užtikrinti, kad jo veikimas nebus sutrikdytas nukreiptąja DoS ataka šiais atvejais:

4.14.1. IP paketai iš nepatikimo šaltinio;

4.14.2. nepalaikomų arba išjungtų protokolų IP paketai;

4.14.3. signalizacijos prievadų neatitinkantys/netinkamai suformuoti (šiukšlių) paketai;

4.14.4. galiojančių arba negaliojančių skambučių užklausų, signalinių pranešimų ir pan. apimtimi pagrįsta ataka (angl. *Flood*);

4.14.5. per daug galiojančių arba negaliojančių skambučių užklausų iš teisėtų, patikimų šaltinių;

4.15. Valdikliai turi būti palaikyti NAT traversal (HNT) funkcionalumą.

4.16. Valdikliai turi palaikyti TLS ir SRTP šifravimo protokolus, naudojant AES-128/256 standartą.

4.17. Valdikliai turi užtikrinti internetinio sertifikato būsenos protokolo (OCSP) palaikymą (suderinamumą).

4.18. Valdikliai turi užtikrinti ICE, STUN saugos funkcionalumus.

4.19. Valdikliai turi būti funkcija, leidžianti sudaryti blokuojamų, leidžiamų, peradresuojamų, apriboto skambinimo telefono numerių sąrašus.

4.20. Įrenginiai privalo turėti funkciją, leidžiančią sudaryti lanksčius įvairius skambučio maršruto parinkimo algoritmus, pagal tokius kriterijus:

4.20.1. apkrovos balansavimas;

4.20.2. QoS pagrįstas maršrutas;

4.20.3. Active Directory pagristas maršruto parinkimas;

4.20.4. Mažiausios kainos maršruto parinkimas;

4.20.5. H.323 maršruto parinkimas.

4.21. Valdiklių maršruto parinkimo lentelės turi būti sudaromos naudojant E.164 telefono numerius arba SIP-URI protokolo eilutes.

4.22. Valdikliai turi palaikyti numerių vertimą pagal nustatytas taisykles. Numerių vertimai gali būti atliekami tiek gaunamo, tiek išeinančio skambučio, tiek prieš, tiek ir po skambučio nukreipimo.

4.23. Valdikliai turi užtikrinti suderinamumą su SIP ir H.323 protokolais ir jais paremtą sąveiką.

4.24. Valdikliai turi palaikyti TCP ir UDP protokolų tarpusavio sąveiką.

4.25. Valdikliai turi palaikyti TLS, MTLS, SRTP/SRTCP, IPSec.

4.26. Valdikliai privalo palaikyti realaus laiko perkodavimą iš/į šiuos kodekus: AMR/AMR-WB/EVS/G722/G729(A)/iLBC/Opus/SILK/PCMU/PCMA;

4.27. Valdikliai turi palaikyti kodeko ir DTMF srauto manipuliavimą;

4.28. Valdikliai turi palaikyti realaus laiko pervertinimą (*angl. trans-rating*), tokį kaip priverstinį paketų sudarymo laiką (*angl. ptime*);

4.29. Valdikliai turi užtikrinti suderinamumą su IPv4, IPv6;

4.30. Valdikliai turi palaikyti tinklo adresų transliavimą (NAT) ir ugniasienės praėjimą (angl. *Firewal Traversal*).

4.31. Valdikliai turi būti palaikyti kelis VLAN toje pačioje virtualioje sąsajoje;

4.32. Valdikliai turi užtikrinti DNS, DHCP, NTP palaikymą;

4.33. Skirtumų tarp SIP tinklų suvienodinimui, kai naudojamos skirtingų tiekėjų ir gamintojų SIP paslaugos, valdikliai turi palaikyti šias antraštės (*angl. Header*) manipuliavimo taisykles (HMR):

4.33.1. įterpti, trinti ar modifikuoti SIP antraštes ar parametrus;

4.33.2. kopijuoti ar perkelti antraštės ar parametrų vertes;

4.33.3. modifikuoti MIME turinį apimant SDP;

4.33.4. keisti žinutės informaciją, kai būtina normalizacija;

4.33.5. išsaugoti žinutės informaciją ir įterpti į kitą žinutę.

4.34. Valdikliai turi atlikti šiuos veiksmus pagal šiuos kriterijus:

4.34.1. SIP žinutės tipą (užklausa ir atsakymas);

4.34.2. užklausos tipą (angl. *Invite, Register*);

4.34.3. įprastos išraiškos sėkmingą ar nesėkmingą bandymą atitikti antraštę ar parametrą.

4.35. Valdikliuose turi būti funkcija, leidžianti sujungti valdiklius poromis užtikrinant aukštą patikimumą (angl. *High Availability*) naudojant aktyvus-laukiantis (*angl. active-standby*) režimą. Laukiantis įrenginys turi būti nuolat sinchronizuojamas su aktyviuoju įrenginiu naudojant dedikuotą sujungimą.

4.36. Turi būti leidžiama sudaryti daugiau nei vieną aukšto patikimumo valdiklių aukšto patikimumo porą neįsigyjant jokių papildomų licencijų.

4.37. Valdikliai, veikdami aukšto patikimumo poroje turi būti sinchronizuoti ir, esant vieno valdiklio gedimui, automatiškai perimti aktyvias sesijas (signalizacijos ir medija sesijas) be sesijų pertraukimo. Perjungimas turi įvykti ne ilgiau kaip per 100 milisekundžių.

4.38. Kiekviena aukšto patikimumo valdiklių pora turi būti pasiekiama tinkle balso srauto apdorojimui naudojant vieną virtualų IP adresą. VRRP ir/ar HSRP ir/ar analogiško standarto palaikymas yra būtinas.

4.39. Turi būti nustatymas, įgalinantis valdiklį periodiškai užklausti IP maršruto parinktuvus ARP žinutėmis siekiant automatiškai aptikti ir pranešti apie ryšio su maršruto parinktuvu nutrūkimą.

4.40. Valdikliai turi būti aprūpinti licencijomis leidžiančios atlikti ne mažiau 120 vienalaikių SIP sesijų.

4.41. Valdikliai privalo palaikyti SIPREC protokolą, kad galėtų sąveikauti su SIPREC suderinama skambučių įrašymo platforma.

4.42. Valdikliai turi užtikrinti SIPREC su SIP REFER antraštės mechanizmo palaikymą, kuris automatiškai išsaugos UCID, XUCID, GUID, GUCID ir UUI metaduomenyse ir persiųsti šią informaciją į išorinį SIPREC standartą palaikantį įrašymo įrenginį.

4.43. Valdikliai turi būti integruoti su turima ReDAT programinę įranga naudojant SIPREC protokolą ir taip užtikrinti visų įeinančių ir išeinančių SIP skambučių įrašymą ReDAT programinėje įrangoje.

4.44. Valdiklio valdymo ir vartotojo autentifikavimo nustatymai privalo turėti:

4.44.1. pasirinkimą, leidžiantį įrenginį valdyti grafine sąsaja (Web GUI) HTTPS protokolu;

4.44.2. pasirinkimą, leidžiantį įrenginį valdyti komandine eilute (CLI) SSH protokolu;

4.44.3. monitoringo funkciją, leidžiančią Web GUI aplinkoje stebėti SIP sesijas;

4.44.4. funkciją, leidžiančią pildyti SIP protokolo sesijų įrašų žurnalą išorinėje vidinio tinklo saugykloje;

4.44.5. REST API palaikymą;

4.44.6. pasirinkimą, leidžiantį naudotojui autentifikuotis naudojant vietines paskyras, RADIUS ir TACACS+ autorizacijų serverius;

4.44.7. funkciją, leidžiančią saugoti skambučių detalius įrašus (CDR) vietinėje programinės įrangos laikmenoje ir perkelti CDR į RADIUS (angl. *Remote Authentication Dial-In User Service*) serverį arba RADIUS serverių grupę;

4.44.8. SNMP v3 palaikymą;

4.44.9. funkciją, leidžiančią siųsti sistemos žurnalo ir procesų žurnalo duomenis, juos saugoti bei analizuoti.

5. Reikalavimai programinės įrangos licencijai

5.1. Turi užtikrinti lankstaus programinės įrangos licencijavimo modelio palaikymą. Licencija neturi būti priskirta konkrečiai programinei įrangai ir, esant poreikiui, turi būti leidžiama ją perkelti į kitą programinę įrangą arba paskirstyta tarp kelių programinių įrangų.

5.2. Programinės įrangos licencija turi užtikrinti ne mažiau kaip 1000 vienalaikių SIP sesijų ir RTP/SRTP srautų vienoje programinėje įrangoje.

6. Reikalavimai įdiegimui, konfigūtavimui ir paruošimui eksploatacijai

6.1. Turi būti sukurti, paruošti naudojimui ir ištestuoti SIP sujungimai su 3 mobiliojo ryšio tinklais ir 1 fiksuoto ryšio tinklu naudojant atskirus VLAN potinklius.

7. Reikalavimai nacionaliniam saugumui

7.1. Tiekėjo siūloma programinės įrangos licencija neturi kelti grėsmės nacionaliniam saugumui. Tiekėjas teikdamas ir pasirašydamas pasiūlymą patvirtina, kad siūloma licencija nekelia grėsmės nacionaliniam saugumui.

7.2. Perkančioji organizacija visais atvejais laikys, kad Tiekėjas nėra patikimas ir kelia pavojų nacionaliniam ar kitos valstybės narės saugumui, jeigu ji gaus kompetentingų institucijų pateiktą tai patvirtinančią informaciją.

7.3. Perkančioji organizacija, vadovaudamasi Viešųjų pirkimų įstatymo 17 straipsnio 5 dalimi pirkime neleidžia dalyvauti tiekėjams (juridiniams asmenims)/subtiekėjams (juridiniams asmenims), kurie nėra registruoti Europos Sąjungos valstybėje narėje, Šiaurės Atlanto sutarties organizacijos valstybėje narėje ar trečiojoje šalyje, pasirašiusioje Pasaulio prekybos organizacijos sutartį dėl viešųjų pirkimų ir kitus tarptautinius susitarimus. Taip pat pirkime neleidžiama dalyvauti tiekėjams

(fiziniams asmenims)/subtiekėjams (fiziniams asmenims), kurie nėra deklaravę gyvenamosios vietos Europos Sąjungos valstybėje narėje, Šiaurės Atlanto sutarties organizacijos valstybėje narėje ar trečiojoje šalyje, pasirašiusioje Pasaulio prekybos organizacijos sutartį dėl viešųjų pirkimų ir kitus tarptautinius susitarimus.

7.4. Tiekėjas turi užtikrinti, kad siūlomoje programinėje įrangoje nebūtų įdiegta jokios papildomos programinės įrangos, kuri nėra būtina. Paaiškėjus, kad yra įdiegta kenkimo programinė įranga, tai būtų traktuojama kaip reikalavimų neatitikimas ir sutarties sąlygų nesilaikymas bei Teikėjas tiekėjas privalėtų padengti Perkančiajai organizacijai patirtą materialinę žalą.

_____