**TECHNINĖ SPECIFIKACIJA**

| Nr. | Rodiklis | Reikalavimai | Atitikimas |
|---|---|---|---|
| 1. | Sujungimo adresai | Jogailos g. 14, Vilnius | |
| 2. | Sujungimo sparta | 100 Mb/s tiek tarptautinis, tiek Lietuvos internetas | |
| 3. | Spartos užtikrinimas | Teikėjas privalo vidiniais metodais savo tinkle užtikrinti nurodytas spartas, vienodas įeinančiam ir išeinančiam srautui. Jei teikėjas siūlo didesnės greitaveikos paslaugą, tuo pačiu turi didinti ir atitinkamų sąsajų greitaveiką tokiu būdu, kad visi virtualūs kanalai galėtų dirbti pilna greitaveika vienu metu. | |
| 4. | Ryšio standartai: | | |
| 5. | *ISO OSI lygiai* | Protokolai | |
| 6. | Fizinis lygis | Optinė skirtoji linija | |
| 7. | Duomenų perdavimo lygis | Ethernet | |
| 8. | Tinklinis lygis | IP | |
| 9. | Paslaugos pateikiamumas | Nemažiau kaip 99% per metus | |
| 10. | Prieigos prie paslaugos teikėjo tipas | Optinė ryšio linija | |
| 11. | Maksimalus statistinis duomenų srautų iš/į tarptautinį, paslaugų teikėjo ir vietinį interneto tinklą greičių ribojimas | 1:1 | |
| 12. | Garantuojama greitaveika | Ne mažiau 99% užsakytos sujungimo greitaveikos. | |
| 13. | Kokybės užtikrinimas | Paslaugų teikėjas privalo pateikti kokybės užtikrinimo procedūrų aprašymus, gedimų šalinimo tvarką ir terminus. | |
| 14. | Stebėjimas | Paslaugų teikėjas pateikia priemonę, įgalinančią stebėti duomenų perdavimo kanalo būklę. | |
| 15. | Gedimų pašalinimo laikas | darbo metu (pirmadienis - ketvirtadienis: nuo 8.00 iki 17.00 val., penktadienis: nuo 8.00 iki 16.15 val.) - 4 valandos;<br>nedarbo metu (visas laikas, kuris nėra darbo metas) -12 valandų. | |
| 16. | Reakcijos laikas | darbo metu (pirmadienis – ketvirtadienis: nuo 8.00 iki 17.00 val., penktadienis: nuo 8.00 iki 16.15 val.) - 2 valandos; nedarbo metu (visas laikas, kuris nėra darbo metas) - 4 valandos. | |
| 17. | Kvalifikuoti sertifikatai | Turi būti įdiegti Perkančiosios organizacijos | |

| | | | |
|---|---|---|---|
| | | pateikti sertifikatai | |
| 18. | Dvikryptis vėlinimas (Round Trip Delay) | Nedaugiau kaip 25 ms. | |
| 19. | Vėlinimo pokytis (Jitter) | Ne daugiau kaip 10 ms. | |
| 20. | Paketų praradimas (Packet Loss) | Nedaugiau kaip 0,2% | |
| 21. | Įranga | Prijungimo taškuose tiekėjo panaudota įranga turi būti sertifikuota Lietuvoje ir atitikti Lietuvos ir europinius ETSI standartus. Tiekėjo įranga, montuojama Pirkėjo patalpose, jokiu būdu neturi įtakoti ten esančios Pirkėjo įrangos darbui | |
| 22. | Galines įrangos sąsaja | Elektrinė pilno duplekso (RJ-45 jungtis): 10/100 BaseTX Fast Ethernet, kuri turi pilnai atitikti ISO/IEC 8802-3 IEEE 802.3 standartų reikalavimams. | |
| 23. | Kompiuterinio tinklo technologija | Fast ethernet (optika). | |
| 24. | Duomenų perdavimo terpė | Turi būti „skaidri“ visiems IP v4 (Internet Protocol Version 4) protokolams, taip pat IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q | |
| 25. | Įtampa | Perkančioji organizacija Teikėjo sumontuotai įrangai teikis standartinę 220 V 50 Hz maitinimo įtampą | |
| 26. | Tinklų sujungimu infrastruktūra | Paslaugos teikėjas turi turėti nuosavą infrastruktūrą tinklų sujungimo paslaugoms teikti. | |
| 27. | Pirminio DNS vardų serverio adresai | Nurodyti | |
| 28. | Paslaugų gavėjui suteikti Paslaugų teikėjo tinkle ir internete maršrutizuojamus IP adresus | Ne mažiau 16 IP adresų | |
| 29. | Potinklio šablonas (subnet mask) | Nurodyti | |

| **Elektroninio pašto paslaugos** | |
|---|---|
| El.pašto filtravimas | Paslaugų teikėjas turi teikti praeinančio el.pašto filtravimą nuo virusų ir nepageidaujamo pašto (spam) paslaugą |
| **Internetinės svetainės palaikymas** | |
| Interneto adresų sritys | (www).kt.gov.lt; konkuren.lt, https://kotis.konkuren.lt, https://kotis.kt.gov.lt palaikymas |
| Galimybė Paslaugų gavėjui valdyti paslaugas | Turi būti suteikta |
| Dedikuotas virtualus serveris kt.gov.lt | Procesorius 1, RAM 4 GB, HDD 100 GB. Turi būti numatyta vieta duomenų kopijoms |
| Dedikuoto virtualaus serverio programinė įranga | Linux OS 64bit / Apache 2.2+ / Mod_Rewrite On /.htaccess palaikymas / PHP 5.4.x / php_curl |

| | |
|---|---|
| | / php_gd2 / php_mbstring / php_mysql / php_pdo_mysql / php_soap / Postfix pašto tarnyba / MySQL 5.x+ / APC. |
| Papildomi reikalavimai old.kt.gov.lt | Apache, MySQL, php, ne mažiau 4000 MB, perduodamų duomenų kiekis – ne mažiau 5 GB/mėn. |
| **Saugumas** | |
| Tinklo darbo žlugdymas (Deniai of Service (DoS), Distributed Deniai of Service (DDos) | Paslauga turi būti apsaugota nuo trečiųjų šalių antpuolių, žlugdančių tinklo darbą. Turi būti apsaugoma nuo ne mažesnio kaip 1 Gbps nepageidaujamo duomenų srauto. |
| Nepageidaujamas duomenų srautas | Diegiant paslaugą tarp paslaugų teikėjo ir perkančiosios organizacijos sutariamos taisyklės pagal kurias blokuojamas nepageidaujamas duomenų srautas, viršijantis numatytas parametrų reikšmes (atitinkamą sesijų skaičių arba paketų kiekį per sekundę). |
| Apsaugos parametrai (apsaugos nuo trečiųjų šalių antpuolių, žlugdančių tinklo darbą) | Paslaugų teikėjo stebimi parametrai dėl apsaugos nuo trečiųjų šalių antpuolių, žlugdančių tinklo darbą, turi būti šie:<br>tcp_syn_flood - rodiklis nustato, kiek tcp SYN paketų praleisti link perkančiosios organizacijos per vieną sekundę;<br>tcp_port_scan - rodiklis nustato, kiek tcp SYN paketų praleisti link perkančiosios organizacijos iš vieno šaltinio per vieną sekundę;<br>• tcp_src_session - rodiklis nustato, kiek tcp sesijų praleisti link perkančiosios organizacijos iš vieno šaltinio;<br>• tcp_dst_session - rodiklis nustato, kiek tcp sesijų praleisti link perkančiosios organizacijos;<br>udp_flood - rodiklis nustato, kiek udp paketų praleisti link perkančiosios organizacijos per vieną sekundę;<br>• udp_scan - rodiklis nustato, kiek udp paketų praleisti link perkančiosios organizacijos iš vieno šaltinio per vieną sekundę;<br>• udp_src_session - rodiklis nustato, kiek udp sesijų praleisti link perkančiosios organizacijos iš vieno šaltinio;<br>• udp_dst_session - rodiklis nustato, kiek udp sesijų praleisti link perkančiosios organizacijos;<br>• icmp_flood - rodiklis nustato, kiek icmp paketų praleisti link perkančiosios organizacijos per vieną sekundę;<br>icmp_sweep - rodiklis nustato, kiek icmp paketų praleisti link perkančiosios organizacijos iš vieno šaltinio per vieną sekundę;<br>icmp_src_session - rodiklis nustato, kiek icmp sesijų praleisti link perkančiosios organizacijos iš vieno šaltinio; |

| | |
|---|---|
| | icmpj3st_session - rodiklis nustato, kiek icmp sesijų praleisti link perkančiosios organizacijos;<br>• ip_src__session- rodiklis nustato, kiek ip sesijų (bendras kiekis, visais protokolais) praleisti link perkančiosios organizacijos iš vieno šaltinio;<br>• ip_dst_session - rodiklis nustato, kiek ip sesijų (bendras kiekis, visais protokolais) praleisti link perkančiosios organizacijos. |
| Standartinis šablonas | Turi būti blokuojamas nepageidaujamas duomenų srautas, jeigu viršijami šie rodikliai: tcp__src_session 5000 udp src session 5000 |

Taip pat Paslaugos teikėjas įsipareigoja sutarties galiojimo laikotarpiu kurti saugius šifruotus duomenų perdavimo kanalus VPN (angl. *Virtual Private Network*) pagal perkančiosios organizacijos pateiktus techninius reikalavimus ir užtikrinti jau dabar egzistuojančių veikiančių paslaugų nepertraukiamumą, pagal žemiau išvardintus Konkurencijos tarybai paslaugų ar/ir duomenų teikėjų pateiktus techninius reikalavimus:

1. **Saugus ryšys su Finansų ministerijos VBAMS sistema:**

1. Elektroninių ryšių tinklas (toliau – Tinklas) turi būti naudojamas tik veiklai, suderinamai su visų valstybės informacinių išteklių rūšių saugos poreikiais.
2. Tinklo saugumo lygis turi atitikti ne mažesnius nei Lietuvos standartuose LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 ir LST ISO/IEC 20000-1:2015 nustatytus reikalavimus, susijusius su elektroninių ryšių tinklo saugumu.
3. Tinklo operatorius privalo naudotis Tinklo saugumo valdymo priemonėmis, atitinkančiomis LST ISO/IEC 27005 ir ISO/IEC 27033-1 standartų nuostatas.
4. Visas Tinklas turi būti uždaras ir apsaugotas nuo viešųjų ryšio tinklų (interneto).
5. Tinklas turi turėti patikimą apsaugą nuo pagrindinių per Tinklą vykdomų atakų: SQL įskverbties (angl. SQL injection), XSS (angl. Cross-site scripting), atkirtimo nuo paslaugos (angl. DOS), dedikuoto atkirtimo nuo paslaugos (angl. DDOS) ir kitų; pagrindinių per Tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. The Open Web Application Security Project (OWASP) interneto svetainėje www.owasp.org.
6. Tinklo perimetrui apsaugoti turi būti naudojami filtrai, saugantys elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo.
7. Tinkle turi būti įdiegtos priemonės, užtikrinančios, kad:
7.1. elektroninė informacija perdavimo metu nebūtų pakeista;
7.2. elektroninė informacija perdavimo metu nebūtų perimta.
8. Turi būti įdiegtos ir nuolat atnaujinamos apsaugos nuo kenkėjiškos programinės įrangos (kompiuterinių virusų, „Trojos arklių“) priemonės (antivirusinė programinė įranga).
9. Tinklo naudojamos užkardos turi atitikti EAL4 lygį pagal standartą ISO/IEC 15408 ir būti naudojamos pagal šio standarto reikalavimus. Siekiant įvertinti bandymus sutrikdyti Tinklo veiklą, periodiškai turi būti peržiūrimi užkardų įrašai.
10. Saugus Tinklo naudotojų prijungimas prie Tinklo turi būti užtikrintas įgyvendinant šiuos reikalavimus:
10.1. Tinklo naudotojų tinklų tarnybinės stotys, Tinklo naudotojų darbo vietos ir kita įranga, siunčianti ir gaunanti elektroninę informaciją per Tinklą, turi turėti fiksuotus vidinius IP adresus Tinklo naudotojo tinkle;
10.2. Tinklo naudotojų tinklas prie viešųjų ryšio tinklų turi būti prijungiamas per vieną koncentruojantį įrenginį ir apsaugotas užkarda;

10.3. Tinklo naudotojų mobiliosios darbo vietos prie Tinklo naudotojų tinklų turi būti prijungiamos naudojant atskirus Tinklo naudotojų virtualius tinklus; tai turi būti atliekama per vieną koncentruojantį įrenginį ir apsaugota užkarda;
10.4. Tinklo naudotojų tinklų dalis, turinti ryšį su Tinklu, neturi turėti tiesioginių (naudojant tinklo adresų transliaciją – NAT) ryšių su viešųjų ryšių tinklais.
11. Siekiant aptikti neleistinus Tinklo operatoriaus darbuotojų ir Tinklo naudotojų darbuotojų veiksmus perduodant, keičiant, trinant ar modifikuojant elektroninę informaciją, pagal Tinklo operatoriaus vadovo nustatytą tvarką turi būti vykdoma Tinkle vykdytų veiksmų apskaita ir auditas.
12. Siekiant palengvinti neleistinų Tinklo operatoriaus darbuotojų ir Tinklo naudotojų darbuotojų veiksmų tyrimą, būtina kaupti ir saugoti Tinkle vykdytų veiksmų žurnalus (angl. log).
13. Turi būti taikomas toks Tinkle vykdytų veiksmų registravimas, kuris leistų užtikrinti Tinklo transakcijų nepaneigiamumą.
14. Siekdamas užtikrinti Tinklo atitikties saugos reikalavimams ir galimų grėsmių elektroninės informacijos saugai įvertinimą, Tinklo operatorius privalo organizuoti Tinklo saugos rizikos analizę:
14.1. periodiškai, ne rečiau kaip kartą per metus;
14.2. atliekant Tinklo, atskirų jo struktūrinių dalių, funkcinių sistemų keitimus, plėtrą ir naujų Tinklų paslaugų kūrimą;
14.3. kitais Tinklo operatoriaus vadovo nustatytais atvejais.
15. Vykdant Tinklo saugos rizikos analizę taip pat turi būti atliekamas Tinklo informacinių išteklių pažeidžiamumo įvertinimas (angl. penetration test).
16. Tinklo operatorius, siekdamas sumažinti neigiamą galimų Tinklo veiklos sutrikimų poveikį, turi turėti parengtą ir Tinklo operatoriaus vadovo (ar jo įgalioto asmens) patvirtintą Tinklo veiklos tęstinumo valdymo planą, kurio veiksmingumas turi būti išbandomas ne rečiau kaip kartą per metus.
17. Kadangi vartotojai su VBAMS sistema dirba naudodami MicroSoft terminalinio serverio galimybes, vienam VBAMS vartotojui turėtų būti užtikrintas ne mažesnis kaip 128Kbits saugaus tinklo greitis.

**2. Saugus ryšys su Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos Administracinių teisės pažeidimų registru**

| Eil. Nr. | Parametras | Reikšmė |
|---|---|---|
| 1. | Sąsaja | Ethernet 10/100 base TX (IEEE 802.3) |
| 2. | Sąsajos sparta | Bent 10 Mbps |
| 3. | Jungtis duomenų perdavimo tinklo vartų pusėje | RJ45 |
| 4. | Maksimali paslaugų gavėjo duomenų perdavimo sparta | Bent 10 Mbps |
| 5 | Protokolai | TCP/IP (IP v4) |
| 6 | Šifravimo algoritmas | AES-256 |
| 7 | Šifruoto kanalo inicijavimo būdas | *pre-shared secret* |

| | |
|---|---|
| VPN Gatevvay IP Address | Bus pateikta |
| VPN Device Description | Palo Alto |
| VPN Device Version | n/a |
| VPN Device Location | Vidaus reikalų ministerija |
| Encryption Mode | Tunnel |
| **VPN Configuration Phase 1** | |
| Authentication Method | Pre-Shared Key |
| Encryption Scheme | IKE |

| | |
|---|---|
| Diffie-Hellman Group | DH Group 5 |
| Encryption Algorithm | AES-256 |
| Hashing Algorithm | SHA 1 |
| Main or Aggressive Mode | Main |
| Lifetime (for renegotiation) | 1440mins |
| Pre-Shared Kev | Derinama atskirai |
| **VPN Configuration Phase 2** | |
| Encapsulation (ESP or AH) | ESP |
| Encryption Algorithm | AES-256 |
| Authentication Algorithm | SHA 1 |
| Perfect Forward Secrecy | No |
| Lifetime (for renegotiation) | 3600s |
| Lifesize in KB (for renegotiation) | 0 |

2. **Saugus ryšys su Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos Tarpžinybine mokestinių duomenų saugykla (TDS)**

| **Eil. Nr.** | **Parametras** | **Reikšmė** |
|---|---|---|
| 1. | Sąsaja | Ethernet |
| 2. | Sąsajos sparta | Bent 10 Mbps |
| 3 | Sąsajos tinklo lygmens protokolas | IPv4 |
| 3. | Jungtis duomenų perdavimo tinklo vartų pusėje | RJ45 |
| 4. | Maksimali paslaugų gavėjo duomenų perdavimo sparta | Bent 10 Mbps |
| 5 | Protokolai | IPSec |
| 6 | Šifravimo algoritmas | 3DES arba AES-128 |
| 7 | Šifruoto kanalo inicijavimo būdas | Automatinis |

3. **Saugus ryšys su Valstybine mokesčių inspekcija prie Finansų ministerijos**

Ryšiui naudojamas SQLNET2 protokolas, duomenys teikiami šifruotu kanalu naudojant VPN. Detalesnė specifikacija bus pateikta derinant naują sutartį ar jos pakeitimą.

4. **Saugus ryšys su Lietuvos Respublikos Vyriausybės kanceliarijos dokumentų mainaviete**