SANTA MONICA NETWORKS, UAB

Uždaroji akcinė bendrovė, Perkūnkiemio g. 7, LT-12131 Vilnius, tel. (85) 2638700, faks. (85) 2638710, el.p. info@smn.lt Duomenys kaupiami ir saugomi Juridinių asmenų registre, juridinio asmens kodas 134162647, PVM kodas LT341626410

Valstybės įmonei Registrų centrui

KOMPIUTERINIO TINKLO SAUGOS ĮRANGOS PLĖTINIŲ PIRKIMO PASIŪLYMAS

2017 m. sausio 30 d. Nr. S-8
Vilnius

Tiekėjo pavadinimas ir kodas */Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių pavadinimai ir kodai/*	SANTA MONICA NETWORKS, UAB į/k 134162647
Tiekėjo adresas */Jeigu dalyvauja ūkio subjektų grupė, surašomi visi dalyvių adresai/*	Perkūnkiemio g. 7, LT-12131 Vilnius
Asmens, pasirašiusio pasiūlymą saugiu elektroniniu parašu, vardas, pavardė, pareigos	Sigitas Vasiliauskas Pardavimų vadovas
Telefono numeris	370 5 2638700
Fakso numeris	370 5 2638710
El. pašto adresas	sigitas.vasiliauskas@smn.lt

Pildoma, jei tiekėjas ketina pasitelkti subtiekėją (-us)	***I pirkimo objekto daliai***	***II pirkimo objekto daliai***
Subtiekėjo (-ų) pavadinimas (-ai) ir kodas (-ai)	***Nėra***	***Nėra***
Subtiekėjo (-ų) adresas (-ai)		
Įsipareigojimų dalis (nurodant konkrečius pagal pirkimo sutartį prisiimamus įsipareigojimus), kuriai ketinama pasitelkti subtiekėją (-us)		

Pildoma, jei tiekėjas ketina pasitelkti specialistus (ekspertus), kuriais bus remiamasi įrodinėjant kvalifikaciją ir vykdant sutartį, tačiau pasiūlymo pateikimo metu jie nėra tiekėjo ar jo pasitelkiamo(ų) subtiekėjo(ų) darbuotojai, tačiau laimėjimo atveju bus įdarbinti	***I pirkimo objekto daliai***	***II pirkimo objekto daliai***
Specialistai (ekspertai), kuriais bus remiamasi įrodinėjant kvalifikaciją ir vykdant sutartį, tačiau jie nėra tiekėjo ar tiekėjo pasitelkiamo(ų) subtiekėjo (ų) darbuotojai pasiūlymo pateikimo metu, bet laimėjimo atveju būtų įdarbinti	***Nėra***	***Nėra***

1. Šiuo pasiūlymu pažymime, kad sutinkame su visomis pirkimo sąlygomis, nustatytomis:

1.1. atviro konkurso skelbime, paskelbtame Viešųjų pirkimų įstatymo nustatyta tvarka CVP IS (https://pirkimai.eviesiejipirkimai.lt/app/notice/notices.asp?B=PPO);

1.2. kituose pirkimo dokumentuose (jų paaiškinimuose, papildymuose).

2. Pasirašydamas CVP IS priemonėmis pateiktą pasiūlymą saugiu elektroniniu parašu, patvirtinu, kad dokumentų skaitmeninės kopijos ir elektroninėmis priemonėmis pateikti duomenys yra tikri.

3. Mes siūlome šias prekes:

3.1. I pirkimo objekto dalis

(Pildoma, jei tiekėjas pasiūlymą teikia I pirkimo objekto daliai)

Eil. Nr.	Prekės pavadinimas	Mato vnt.	Kiekis	1 mėnesio nuomos kaina Eur be PVM	1 mėnesio nuomos kaina Eur su PVM	36 mėnesių nuomos kaina Eur be PVM	36 mėnesių nuomos kaina Eur su PVM
	1	2	3	4	5	6	7
1.	F5 dubliuotos internetinių aplikacijų ugniasienės (WAF) plėtinys*	Vnt.	1	2428,00	2937,88	87408,00	105763,68
2.	Palo Alto Networks dubliuotos didelio pralaidumo ugniasienės PA-5050 su IPDS funkcionalumu plėtinys su išplėtimo licencija „WildFire subscription for a device in an HA pair, PA-5050"*	Vnt.	1	6293,00	7614,53	226548,00	274123,08
3.	Kaina iš viso:					313956,00	379886,76

Bendra I pirkimo objekto dalies pasiūlymo kaina su PVM yra 379886 Eur 76 ct *(trys šimtai septyniasdešimt devyni tūkstančiai aštuoni šimtai aštuoniasdešimt šeši eurai ir septyniasdešimt šeši centai).* Į šią sumą įeina visos išlaidos ir visi mokesčiai, taip pat ir PVM, kuris sudaro 65930 Eur 76 ct *(šešiasdešimt penki tūkstančiai devyni šimtai trisdešimt eurų ir septyniasdešimt šeši centai).*

* Į kiekvienos nurodytos prekės kainą turi būti įskaičiuota ne mažiau kaip 30 val. konsultavimo diegimo ir eksploatavimo metu iškilusiais klausimais visu sutarties galiojimo laikotarpiu.

PASTABA: *Į kainą turi būti įskaičiuotas PVM, kiti mokesčiai bei visos kitos išlaidos. Tiekėjas finansiniame pasiūlyme turi nurodyti kainą Eur su PVM, jei tiekėjas yra PVM mokėtojas arba Eur be PVM, jei tiekėjas yra ne PVM mokėtojas. Prie kainos skaičiais būtina nurodyti žodžius „su PVM" arba „be PVM".*

Siūlomos prekės visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus ir jų savybės yra tokios:

1 lentelė:

F5 dubliuotos internetinių aplikacijų ugniasienės (WAF) plėtinys		
Charakteristikos pavadinimas ir reikalaujama parametro reikšmė		**Tiekėjo pasiūlymas**
Nr.	**Sistemos sudėtis**	*F5-BIG-LTM-I2600 (2 vnt.)* BIG-IP i2600 Local Traffic Manager *F5-ADD-BIG-ASM-I2XXX (2 vnt.)* BIG-IP Application Security Manager Module for i2X00 https://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf
1.	Nuomojama aplikacijų ugniasienė turi turėti srautų balansavimo funkciją (aukšto patikimumo klasteris susidedantis iš 2 vienodų įrenginių).	Nuomojama aplikacijų ugniasienė turi srautų balansavimo funkciją (aukšto patikimumo klasteris susidedantis iš 2 vienodų įrenginių).
	Konstrukcija	
2.	Specializuotas identiškai atitinkantis aparatinis-programinis sprendimas, skirtas užtikrinti interneto tinklapių saugumą, vartotojams prie interneto tinklapių turinio jungiantis naudojant HTTP 0.9 / 1.0 / 1.1, HTTPS, bei atliekantis FTP, SMTP protokolų saugumo patikrą.	Specializuotas identiškai atitinkantis aparatinis-programinis sprendimas, skirtas užtikrinti interneto tinklapių saugumą, vartotojams prie interneto tinklapių turinio jungiantis naudojant HTTP 0.9 / 1.0 / 1.1, HTTPS, bei atliekantis FTP, SMTP protokolų saugumo patikrą.
3.	Ne mažiau kaip 4 10/100/1000 Base-T Ethernet prievadai.	4 10/100/1000 Base-T Ethernet prievadai.
4.	Ne mažiau kaip du 10G optiniai prievadai (SFP).	Du 10G optiniai prievadai (SFP).
5.	Montuojamas į 19 colių komutacinę spintą (montavimui reikalingos detalės turi būti pateiktos kartu su įranga).	Montuojamas į 19 colių komutacinę spintą (montavimui reikalingos detalės bus pateiktos kartu su įranga).
6.	Ne mažiau kaip 1 dedikuota valdymo sąsaja.	1 dedikuota valdymo sąsaja.
7.	Ne mažiau kaip 1 USB sąsaja.	1 USB sąsaja.
8.	Elektros maitinimas – kintamos srovės, 220V įtampos.	Elektros maitinimas – kintamos srovės, 220V įtampos.
	Aukštas patikimumas	
9.	Sprendimą turi sudaryti du vienas kitą dubliuojantys įrenginiai dirbantys Aktyvus/Pasyvus Aktyvus/Aktyvus režimais.	Sprendimą sudaro du vienas kitą dubliuojantys įrenginiai dirbantys Aktyvus/Pasyvus Aktyvus/Aktyvus režimais.
10.	Sutrikus aktyvaus įrenginio darbui aukšto patikimumo sistema turi automatiškai persijungti į dubliuojantį įrenginį, užmegztos sesijos turi nenutrūkti.	Sutrikus aktyvaus įrenginio darbui aukšto patikimumo sistema automatiškai persijungia į dubliuojantį įrenginį, užmegztos sesijos nenutrūksta.
	Kiekvieno sistemos nario našumas	
11.	Pralaidumas ne mažesnis kaip 8 Gbps.	Pralaidumas - 10 Gbps.
12.	L4 HTTP užklausų per sekundę skaičius ne mažesnis kaip 500 000.	L4 HTTP užklausų per sekundę skaičius 600 000.

13.	Ne mažiau kaip 200 000 L7 užklausų per sekundę.	350 000 L7 užklausų per sekundę.
14.	Ne mažiau kaip 4 000 000 sesijų palaikymas.	14 000 000 sesijų palaikymas.
	Įrangos plečiamumas	
15.	Esant poreikiui turi būti galimybė padidinti nuomojamos įrangos našumą įsigyjant papildomas licencijas (nekeičiant turimos aparatinės įrangos): Ne mažiau kaip 400 000 L7 užklausų per sekundę; L4 HTTP užklausų per sekundę skaičius ne mažesnis kaip 1 000 000.	Esant poreikiui yra galimybė padidinti nuomojamos įrangos našumą įsigyjant papildomas licencijas (nekeičiant turimos aparatinės įrangos): 650 000 L7 užklausų per sekundę; L4 HTTP užklausų per sekundę skaičius 1 000 000.
	Pagrindinės palaikomos funkcijos	
16.	Turi palaikyti HTTP 0.9 / 1.0 / 1.1, HTTPS, SSL 3.0/TLS 1.0, FTP, SMTP protokolus.	Palaiko HTTP 0.9 / 1.0 / 1.1, HTTPS, SSL 3.0/TLS 1.0, FTP, SMTP protokolus.
17.	HSTS palaikymas.	HSTS palaikymas.
18.	Palaikymas SHA, SHA256, SHA384.	Palaikymas SHA, SHA256, SHA384.
19.	Galimybė riboti SSL sesijų užmezgimo skaičių per klientą arba per serverį.	Galimybė riboti SSL sesijų užmezgimo skaičių per klientą arba per serverį.
20.	Saugumas užtikrinamas naudojant teigiamą ir neigiamą saugumo modelius.	Saugumas užtikrinamas naudojant teigiamą ir neigiamą saugumo modelius.
21.	Turi atlikti apsaugą nuo SQL ir HTML kodų įterpimų – (*angl. SQL injection*).	Atlieka apsaugą nuo SQL ir HTML kodų įterpimų – (*angl. SQL injection*).
22.	Turi atlikti apsaugą nuo pažeidžiamumų, leidžiančių įsilaužėliui manipuliuoti vartotojo duomenimis pažeidžiamos svetainės kontekste (*angl. crosssitescripting*)	Atlieka apsaugą nuo pažeidžiamumų, leidžiančių įsilaužėliui manipuliuoti vartotojo duomenimis pažeidžiamos svetainės kontekste (*angl. crosssitescripting*)
23.	Turi atlikti apsaugą nuo buferio persipildymo atakų (*angl. buferoverflow*)	Atlieka apsaugą nuo buferio persipildymo atakų (*angl. buferoverflow*)
24.	Turi atlikti apsaugą nuo automatinio skanavimo (*angl. bot*).	Atlieka apsaugą nuo automatinio skanavimo (*angl. bot*).
25.	Turi atlikti apsaugą nuo taikomosios programinės įrangos lygio DoS atakų.	Atlieka apsaugą nuo taikomosios programinės įrangos lygio DoS atakų.
26.	Galimybė įrašyti paketus DOS atakos metu.	Yra galimybė įrašyti paketus DOS atakos metu.
27.	Turi atlikti apsaugą nuo parametrų klastojimo (*angl. parametertampering*).	Atlieka apsaugą nuo parametrų klastojimo (*angl. parametertampering*).
28.	Turi atlikti apsaugą nuo sesijų vogimo (*angl. sessionhighjacking*).	Atlieka apsaugą nuo sesijų vogimo (*angl. sessionhighjacking*).
29.	Turi atlikti taikomosios programinės įrangos, naudojančios AJAX ir JSON duomenų perdavimui tarp kliento ir tarnybinės stoties, apsaugą. Atlikti Json/Ajax apsaugą nuo	Atlieka taikomosios programinės įrangos, naudojančios AJAX ir JSON duomenų perdavimui tarp kliento ir tarnybinės stoties, apsaugą. Atlikti Json/Ajax apsaugą nuo brutualaus

	brutualaus bandymo prisijungti (*angl. Brute force login*).	bandymo prisijungti (*angl. Brute force login*).
30.	WEBsocket apsauga.	WEBsocket apsauga.
31.	Turi užmaskuoti bandymus nustatyti naudojamas operacines sistemas.	Užmaskuoja bandymus nustatyti naudojamas operacines sistemas.
32.	Galimybė nurodyti HTTP antraštes, kurios turi būti kiekvienoje HTTP transakcijoje.	Yra galimybė nurodyti HTTP antraštes, kurios turi būti kiekvienoje HTTP transakcijoje.
33.	Galimybė patikrinti ar HTTP HOST antraštėje nėra IP adreso.	Yra galimybė patikrinti ar HTTP HOST antraštėje nėra IP adreso.
34.	Galimybė tikrinti ar HTTP duomenų srautas atitinka RFC standartą.	Yra galimybė tikrinti ar HTTP duomenų srautas atitinka RFC standartą.
35.	Kurti taisykles leidžiant ar draudžiant duomenų srautus iš skirtingų geografinių vietų (skirstymas pagal šalis).	Galima kurti taisykles leidžiant ar draudžiant duomenų srautus iš skirtingų geografinių vietų (skirstymas pagal šalis).
36.	Galimybė normalizuoti HTTP užklausas.	Yra galimybė normalizuoti HTTP užklausas.
37.	Galimybė nurodyti kokio tipo failai gali būti siunčiami.	Yra galimybė nurodyti kokio tipo failai gali būti siunčiami.
38.	XML filtravimas ir tikrinimas. XML schemų tikrinimas. Apsauga nuo XML DoS.	XML filtravimas ir tikrinimas. XML schemų tikrinimas. Apsauga nuo XML DoS.
39.	Galimybė kontroliuoti FTP komandų ilgius; Galimybė nurodyti leistinas FTP komandas; FTP apsauga nuo brutalių atakų (*angl. bruteforce*).	Yra galimybė kontroliuoti FTP komandų ilgius; yra galimybė nurodyti leistinas FTP komandas; FTP apsauga nuo brutalių atakų (*angl. bruteforce*).
40.	Galimybė blokuoti nepageidaujamas SMTP komandas; Galimybė tikrinti DNS SPF įrašus; Galimybė nustatyti leistiną laiškų per sekundę skaičių;	Yra galimybė blokuoti nepageidaujamas SMTP komandas; Yra galimybė tikrinti DNS SPF įrašus; Yra galimybė nustatyti leistiną laiškų per sekundę skaičių;
41.	Turi būti automatinio apsimokymo režimas (įranga surenka informaciją apie naudojamus failus, parametrus ir t. t.)	Yra automatinio apsimokymo režimas (įranga surenka informaciją apie naudojamus failus, parametrus ir t. t.)
42.	Turi būti galimybė kurti taisykles kiekvienai žiniatinklio svetainei atskirai.	Yra galimybė kurti taisykles kiekvienai žiniatinklio svetainei atskirai.
43.	Turi būti galimybė kurti atakų aprašus pačiam vartotojui.	Yra galimybė kurti atakų aprašus pačiam vartotojui.
44.	Turi būti galimybė kurti skirtingas taisyklių versijas	Yra galimybė kurti skirtingas taisyklių versijas
45.	Turi būti galimybė grįžti prie anksčiau naudotų taisyklių.	Yra galimybė grįžti prie anksčiau naudotų taisyklių.
46.	Turi dešifruoti SSL srautą (įdiegus skaitmeninius sertifikatus su atitinkamais privačiais raktais)	Dešifruoja SSL srautą (įdiegus skaitmeninius sertifikatus su atitinkamais privačiais raktais)
47.	Turi šifruoti HTTP srautą panaudojant skaitmeninį sertifikatą su privačiu raktu	Šifruoja HTTP srautą panaudojant skaitmeninį sertifikatą su privačiu raktu

48.	Turi būti galimybė nustatyti tarnybinės stoties tapatybę naudojant skaitmeninius sertifikatus	Yra galimybė nustatyti tarnybinės stoties tapatybę naudojant skaitmeninius sertifikatus
49.	Turi būti galimybė nustatyti kliento tapatybę naudojant skaitmeninius sertifikatus	Yra galimybė nustatyti kliento tapatybę naudojant skaitmeninius sertifikatus
50.	Įrenginyje turi būti galimybė sukurti savo sertifikatą (*angl. self-signed certificate*)	Įrenginyje yra galimybė sukurti savo sertifikatą (*angl. self-signed certificate*)
51.	Turi būti galimybė keisti SSL parametrus: SSL šifravimo mechanizmą, SSL versija.	Yra galimybė keisti SSL parametrus: SSL šifravimo mechanizmą, SSL versija.
52.	Apsauga nuo formų, slapukų (*angl. „cookie“*), URI informacijos keitimo. Šifruotų slapukų „cookie“ palaikymas.	Apsauga nuo formų, slapukų (*angl. „cookie“*), URI informacijos keitimo. Šifruotų slapukų „cookie“ palaikymas.
53.	Turi būti galimybė riboti slapukų „cookie“ skaičių.	Yra galimybė riboti slapukų „cookie“ skaičių.
54.	Turi būti galimybė riboti slapukų pavadinimo ir reikšmės ilgį.	Yra galimybė riboti slapukų pavadinimo ir reikšmės ilgį.
55.	Turi gebėti laikyti saugomų tinklapių statinius objektus ir juos pateikti klientams nesiunčiant jų iš tinklapių.	Geba laikyti saugomų tinklapių statinius objektus ir juos pateikti klientams nesiunčiant jų iš tinklapių.
56.	Turi būti galimybė apibrėžti sąlygas, kurioms esant įrenginys pašalina pas save saugomus tinklapių objektus (išvalyti cache).	Yra galimybė apibrėžti sąlygas, kurioms esant įrenginys pašalina pas save saugomus tinklapių objektus (išvalyti cache).
57.	Užblokavus užklausą, vartotojui turi būti parodomas pagalbos identifikacinis numeris, kuris identifikuoja sistemos įrašus susijusius su blokuota užklausa.	Užblokavus užklausą, vartotojui parodomas pagalbos identifikacinis numeris, kuris identifikuoja sistemos įrašus susijusius su blokuota užklausa.
58.	Galimybė integruoti įrenginį su tinklalapių pažeidžiamumų skanavimo įrangą. Turi būti galimybė pažeidžiamumų skanavimo įrangai tiesiogiai konfigūruoti interneto svetainių apsaugos įrenginį.	Yra galimybė integruoti įrenginį su tinklalapių pažeidžiamumų skanavimo įranga. Yra galimybė pažeidžiamumų skanavimo įrangai tiesiogiai konfigūruoti interneto svetainių apsaugos įrenginį.
59.	Turi būti galimybė keisti/modifikuoti klaidų ir blokuotus puslapius.	Yra galimybė keisti/modifikuoti klaidų ir blokuotus puslapius.
60.	Turi būti galimybė slėpti klaidų puslapius ir taikomųjų programų klaidų puslapius.	Yra galimybė slėpti klaidų puslapius ir taikomųjų programų klaidų puslapius.
61.	Turi gebėti pateikti statistiką apie: • Tarnybinės stoties vėlinimo laikas (*angl. „latency“*) apdorojant URI; • Labiausiai lankomi URI; • Aktyviausių siuntėjų IP adresai, sunaudotas pralaidumas ir transakcijų per sekundę skaičius.	Geba pateikti statistiką apie: • Tarnybinės stoties vėlinimo laikas (*angl. „latency“*) apdorojant URI; • Labiausiai lankomi URI; • Aktyviausių siuntėjų IP adresai, sunaudotas pralaidumas ir transakcijų per sekundę skaičius.

62.	Turi galėti vykdyti duomenų srautų paskirstymą (*angl. loadbalancing*).	Gali vykdyti duomenų srautų paskirstymą (*angl. loadbalancing*).
63.	Įrenginiai privalo palaikyti dinaminį apkrovos paskirstymo algoritmą, skirstyti duomenų srautus atsižvelgiant į momentinius tarnybinių stočių parametrus (operatyvinės atminties panaudojimas, procesorių apkrovimai, aktyvių procesų skaičius, aktyvių sesijų skaičius).	Įrenginiai palaiko dinaminį apkrovos paskirstymo algoritmą, skirstyti duomenų srautus atsižvelgiant į momentinius tarnybinių stočių parametrus (operatyvinės atminties panaudojimas, procesorių apkrovimai, aktyvių procesų skaičius, aktyvių sesijų skaičius).
64.	Tarnybinių stočių apkrovimo parametrai turi būti periodiškai, konfigūracijoje nurodytu intervalu, gaunami iš tarnybinių stočių panaudojant SNMP arba WMI (*angl. Windows Management Interface*) technologijas.	Tarnybinių stočių apkrovimo parametrai periodiškai, konfigūracijoje nurodytu intervalu, gaunami iš tarnybinių stočių panaudojant SNMP arba WMI (*angl. Windows Management Interface*) technologijas.
65.	Įrenginiai privalo palaikyti pastovumo (*angl. session persistence*) mechanizmą, kad kreipiniai iš tos pačios darbo vietos būtų nukreipti į tą pačią tarnybinę stotį. Kreipiniai turi būti identifikuojami pagal siuntėjo IP adresą, SSL-ID, HTTP slapukus (*angl. „cookie"*). Turi būti galimybė įterpti savo HTTP slapuką.	Įrenginiai palaiko pastovumo (*angl. session persistence*) mechanizmą, kad kreipiniai iš tos pačios darbo vietos būtų nukreipti į tą pačią tarnybinę stotį. Kreipiniai identifikuojami pagal siuntėjo IP adresą, SSL-ID, HTTP slapukus (*angl. „cookie"*). Yra galimybė įterpti savo HTTP slapuką.
66.	Turi palaikyti „Round robin" balansavimo metodą.	Palaiko „Round robin" balansavimo metodą.
67.	Turi palaikyti balansavimą pagal balansavimo grupės nario santykinį svorį.	Palaiko balansavimą pagal balansavimo grupės nario santykinį svorį.
68.	Turi palaikyti balansavimą atsižvelgiant į aktyvių sesijų skaičių.	Palaiko balansavimą atsižvelgiant į aktyvių sesijų skaičių.
69.	Turi palaikyti balansavimą atsižvelgiant į aktyvių sesijų, užmegztų su kiekvienu balansavimo grupės nariu, skaičių ir maksimalų sesijų skaičių, kuri gali aptarnauti grupės narys.	Palaiko balansavimą atsižvelgiant į aktyvių sesijų, užmegztų su kiekvienu balansavimo grupės nariu, skaičių ir maksimalų sesijų skaičių, kuri gali aptarnauti grupės narys.
70.	Turi palaikyti balansavimą pagal balansavimo grupės narių reitingą. Narius reitinguoja balansavimo įrenginiai.	Palaiko balansavimą pagal balansavimo grupės narių reitingą. Narius reitinguoja balansavimo įrenginiai.
71.	Turi palaikyti balansavimą pagal prognozuojamą narių našumą. Prognozė daroma atsižvelgiant buvusius L4 susijungimų su nariais skaičius.	Palaiko balansavimą pagal prognozuojamą narių našumą. Prognozė daroma atsižvelgiant buvusius L4 susijungimų su nariais skaičius.
72.	Balansavimo grupės nariai gali būti iš skirtingų loginių tinklų.	Balansavimo grupės nariai gali būti iš skirtingų loginių tinklų.
73.	Turi būti tarnybinių stočių gyvybingumo stebėjimo funkcijos.	Yra tarnybinių stočių gyvybingumo stebėjimo funkcijos.

74.	Turi būti galimybė sukonfigūruoti gyvybingumo stebėjimą apkrovos balansavimo grupei, individualiam grupės nariui.	Yra galimybė sukonfigūruoti gyvybingumo stebėjimą apkrovos balansavimo grupei, individualiam grupės nariui.
	Kitos palaikomos funkcijos	
75.	Prievadų loginis grupavimas pagal IEEE 802.3ad ar lygiavertį standartą.	Prievadų loginis grupavimas pagal IEEE 802.3ad ar lygiavertį standartą.
76.	OSPF v3 grakštus perkrovimas (*angl. Graceful restart*).	OSPF v3 grakštus perkrovimas (*angl. Graceful restart*).
77.	VLAN palaikymas (IEEE 802.1Q).	VLAN palaikymas (IEEE 802.1Q).
78.	IPv6 protokolo palaikymas.	IPv6 protokolo palaikymas.
79.	Saugumo filtrai pagal įvairią OSI L3/L4 lygių informaciją (siuntėjo ir gavėjo IP adresą, siuntėjo ir gavėjo TCP/UDP porto numerį). Saugumo filtrai turi būti „stateful“.	Saugumo filtrai pagal įvairią OSI L3/L4 lygių informaciją (siuntėjo ir gavėjo IP adresą, siuntėjo ir gavėjo TCP/UDP porto numerį). Saugumo filtrai yra „stateful“.
	Licencijos	
80.	Turi būti pateiktos visos prašomam funkcionalumo veikimui reikalingos licencijos.	Bus pateiktos visos prašomam funkcionalumo veikimui reikalingos licencijos.
81.	Licencijų palaikymo terminas – 36 (trisdešimt šeši) mėnesiai	Licencijų palaikymo terminas – 36 (trisdešimt šeši) mėnesiai
	Techninis aptarnavimas	
82.	Tiekėjas visu sutarties galiojimo laikotarpiu (nuo perdavimo–priėmimo akto pasirašymo dienos) atlieka abiejų nuomojamų įrenginių techninį aptarnavimą kuris turi apimti gamintojo signatūrų (įsilaužimų ir kitų grėsmių aprašų) prenumeratą.	Tiekėjas visu sutarties galiojimo laikotarpiu (nuo perdavimo–priėmimo akto pasirašymo dienos) atlieka abiejų nuomojamų įrenginių techninį aptarnavimą kuris apims gamintojo signatūrų (įsilaužimų ir kitų grėsmių aprašų) prenumeratą.
83.	Tiekėjas garantuoja 8x5 techninį įrangos aptarnavimą naudojimo vietoje (angl. on-site) ir su ne blogesniu kaip 4 val. reakcijos laiku	Tiekėjas garantuoja 8x5 techninį įrangos aptarnavimą naudojimo vietoje (angl. on-site) ir su ne blogesniu kaip 4 val. reakcijos laiku
84.	Perkančioji organizacija, sutarties galiojimo laikotarpiu pastebėjusi techninės įrangos trūkumų, turi teisę savo pasirinkimu pareikalauti, kad techninė įranga būtų pakeista tinkamos kokybės techninė įranga, arba kad tiekėjas neatlygintinai per protingą, perkančiosios organizacijos nurodytą terminą pašalintų techninės įrangos trūkumus	Perkančioji organizacija, sutarties galiojimo laikotarpiu pastebėjusi techninės įrangos trūkumus, turi teisę savo pasirinkimu pareikalauti, kad techninė įranga būtų pakeista tinkamos kokybės techninė įranga, arba kad tiekėjas neatlygintinai per protingą, perkančiosios organizacijos nurodytą terminą pašalintų techninės įrangos trūkumus
85.	Ne mažiau kaip 30 val. konsultavimo diegimo ir eksploatavimo klausimais visu sutarties galiojimo laikotarpiu.	30 val. konsultavimo diegimo ir eksploatavimo klausimais visu sutarties galiojimo laikotarpiu.

2 lentelė:

Palo Alto Networks dubliuotos didelio pralaidumo ugniasienės PA-5050 su IPDS funkcionalumu plėtinys su išplėtimo licencija „WildFire subscription for a device in an HA pair, PA-5050“		
Eil. Nr.	**Charakteristikos pavadinimas ir reikalaujama parametro reikšmė**	**Tiekėjo pasiūlymas**
		PAN-WF-500 (1 vnt.) Palo Alto Networks WF-500, 2TB RAID storage (4 1TB RAID certified drives preinstalled). 4 post rack mount rails included. *PAN-PA-5050-WF-HA2 (2 vnt.)* WildFire subscription for device in an HA pair year 1, PA-5050 https://www.paloaltonetworks.com/resources/datasheets/wildfire
1.	Didelio pralaidumo ugniasienės sistemos PaloAlto PA-5050 išplėtimo licencija „WildFire subscription for a device in an HA pair, PA-5050“ (2 vnt.).	Didelio pralaidumo ugniasienės sistemos PaloAlto PA-5050 išplėtimo licencija „WildFire subscription for a device in an HA pair, PA-5050“ (2 vnt.).
2.	Licencijos palaikymo terminas – 36 (trisdešimt šeši) mėnesiai.	Licencijos palaikymo terminas – 36 (trisdešimt šeši) mėnesiai.
3.	**Konstrukcija**	
3.1.	Įrenginys turi būti montuojamas į 19 colių komutacinę spintą (montavimui reikalingos detalės turi būti pateiktos kartu su įranga). Aukštis ne didesnis kaip 2 RU.	Įrenginys montuojamas į 19 colių komutacinę spintą (montavimui reikalingos detalės bus pateiktos kartu su įranga). Aukštis – 2 RU.
3.2.	Specializuotas identiškai atitinkantis aparatinis-programinis sprendimas, skirtas aptikti ir sustabdyti nežinomas atakas, tikslines atakas, kenksmingą kodą. Kenksmingo kodo aptikimas atliekamas virtualioje aplinkoje imituojant darbo vietą ir tikrinant failų atliekamus veiksmus sisteminiame lygmenyje.	Specializuotas identiškai atitinkantis aparatinis-programinis sprendimas, skirtas aptikti ir sustabdyti nežinomas atakas, tikslines atakas, kenksmingą kodą. Kenksmingo kodo aptikimas atliekamas virtualioje aplinkoje imituojant darbo vietą ir tikrinant failų atliekamus veiksmus sisteminiame lygmenyje.
3.3.	Atminties diskai turi būti apjungti RAID technologija (arba lygiaverte) ir sudaryti ne mažiau kaip 2 TB bendros talpos. Diskai turi pilnai dubliuoti vienas kitą, t. y. vienam diskui sugedus duomenys neturi būti prarasti.	Atminties diskai apjungti RAID technologija ir sudaro 2 TB bendros talpos. Diskai dubliuoja vienas kitą, t. y. vienam diskui sugedus duomenys nebus prarasti.
3.4.	Turi būti ne mažiau kaip 2 maitinimo šaltiniai, kurie dubliuotų vienas kitą. Maitinimo šaltiniai keičiami neišjungus įrangos. Įranga turi veikti sugedus vienam maitinimo šaltiniui.	2 maitinimo šaltiniai, kurie dubliuoja vienas kitą. Maitinimo šaltiniai keičiami neišjungus įrangos. Įranga veikia sugedus vienam maitinimo šaltiniui.

3.5.	Elektros maitinimas – kintamos srovės, 220V įtampos.	Elektros maitinimas – kintamos srovės, 220V įtampos.
3.6.	Turi būti ne mažiau kaip 1 konsolės prievadas įrangos valdymui (DB9).	1 konsolės prievadas įrangos valdymui (DB9).
3.7.	Turi būti ne mažiau kaip 2 USB prievadai.	2 USB prievadai.
3.8.	Turi turėti ne mažiau kaip 4 dedikuotus 10/100/1000 Base-T tinklo prievadus.	4 dedikuoti 10/100/1000 Base-T tinklo prievadus.
4.	**Suderinamumas**	
4.1.	Turi būti suderinama su Registrų centro naudojamomis perimetro ugniasienėmis Palo Alto Networks PA-5050. Failai siunčiami per perimetro ugniasienę turi būti automatiškai perduodami siūlomos sistemos patikrai. Perimetro ugniasienės turi gauti grįžtamąjį ryšį iš siūlomos sistemos apie aptiktas grėsmes. Šios grėsmės turi būti atvaizduotos perimetro ugniasienių ataskaitose koreliuojant įvykius.	Suderinama su Registrų centro naudojamomis perimetro ugniasienėmis Palo Alto Networks PA-5050. Failai siunčiami per perimetro ugniasienę automatiškai perduodami siūlomos sistemos patikrai. Perimetro ugniasienės gauna grįžtamąjį ryšį iš siūlomos sistemos apie aptiktas grėsmes. Šios grėsmės yra atvaizduotos perimetro ugniasienių ataskaitose koreliuojant įvykius.
4.2.	Turi būti atviras API sąsaja integracijai su trečių šalių produktais.	Atviras API sąsaja integracijai su trečių šalių produktais.
4.3.	Sistema turi priimti ne mažiau kaip 40 bylų per minutę iš perimetro ugniasienės.	Sistema priima ne mažiau kaip 40 bylų per minutę iš perimetro ugniasienės.
4.4.	Sistema turi gauti iš perimetro ugniasienės informaciją apie naudotoją (jei jis nustatytas ugniasienėje AD ar kitomis priemonėmis), kuris siuntėsi įtartiną bylą ir tai turi atsispindėti ataskaitoje.	Sistema gauna iš perimetro ugniasienės informaciją apie naudotoją (jei jis nustatytas ugniasienėje AD ar kitomis priemonėmis), kuris siuntėsi įtartiną bylą ir tai atsispindi ataskaitoje.
5.	**Funkcionalumas**	
5.1.	Turi būti galimybė įkelti failus patikrai rankiniu būdu.	Yra galimybė įkelti failus patikrai rankiniu būdu.
5.2.	Sistema turi tikrinti bylas naudojant iš anksto žinomas kenksmingų bylų maišos reikšmes (*angl. Hash*) spartesniam jau žinomų kenksmingų failų aptikimui.	Sistema tikrina bylas naudojant iš anksto žinomas kenksmingų bylų maišos reikšmes (*angl. Hash*) spartesniam jau žinomų kenksmingų failų aptikimui.
5.3.	Sistema aptikusi naują, dar nežinomą, kenksmingą kodą turi gebėti sukurti bylos atakos aprašą ir jį perduoti perimetro ugniasienei.	Sistema aptikusi naują, dar nežinomą, kenksmingą kodą geba sukurti bylos atakos aprašą ir jį perduoti perimetro ugniasienei.
5.4.	Sistema turi gebėti analizuoti bylas neišsiunčiant/neperduodant jų išoriniams aktoriams.	Sistema geba analizuoti bylas neišsiunčiant/neperduodant jų išoriniams aktoriams.
5.5.	Sistema analizuojanti bylas virtualiose sistemose turi gebėti aptikti tokias kenksmingo kodo funkcijas kaip: konfigūracijos pakeitimai, kodo įterpimas į standartinius procesus, bylų pakeitimai, komunikacija su pavojingais	Sistema analizuojanti bylas virtualiose sistemose geba aptikti tokias kenksmingo kodo funkcijas kaip: konfigūracijos pakeitimai, kodo įterpimas į standartinius procesus, bylų

	nutolusiais serveriais, dalies kodo įkėlimo į atskirus laikinosios atminties blokus (*angl. memory heap spray*), kitą įtartiną veiklą/anomalijas.	pakeitimai, komunikacija su pavojingais nutolusiais serveriais, dalies kodo įkėlimo į atskirus laikinosios atminties blokus (*angl. memory heap spray*), kitą įtartiną veiklą/anomalijas.
5.6.	Sistema analizuojanti bylas turi tikrinti įtartinos bylos komunikaciją tinkle: bandymus sukurti neleistinos prieigos taškus iš išorės (*angl. backdoor*), bandymus atsisiųsti papildomą kenksmingą kodą, bandymus jungtis prie blogos reputacijos WEB svetainių, bandymus atlikti tinklo skenavimą siekiant surinkti informaciją.	Sistema analizuojanti bylas tikrina įtartinos bylos komunikaciją tinkle: bandymus sukurti neleistinos prieigos taškus iš išorės (*angl. backdoor*), bandymus atsisiųsti papildomą kenksmingą kodą, bandymus jungtis prie blogos reputacijos WEB svetainių, bandymus atlikti tinklo skenavimą siekiant surinkti informaciją.
5.7.	Sistema turi leisti pavojingai bylai užmegzti ryšį su išoriniu valdymo serveriu tolimesnių veiksmų analizei, tačiau šaltinio vietą paslėpti, taip neleidžiant valdymo serveriui žinoti Registrų centro IP adresų.	Sistema leidžia pavojingai bylai užmegzti ryšį su išoriniu valdymo serveriu tolimesnių veiksmų analizei, tačiau šaltinio vietą paslėpia, taip neleidžiant valdymo serveriui žinoti Registrų centro IP adresų.
5.8.	Sistema turi informuoti apie nustatytas grėsmingas bylas šiais arba lygiaverčiais būdais: el. paštu, Syslog, SNMP.	Sistema informauoja apie nustatytas grėsmingas bylas šiais arba lygiaverčiais būdais: el. paštu, Syslog, SNMP.
5.9.	Bylų tikrinimas atliekamas pasitelkiant statinę ir dinaminę analizę. Sistema turi atpažinti bylas, kurios stengiasi išvengti patikrinimo (*angl. sandbox evasion*), skirto tokių kenksmingų bylų analizei. Sistema turi atpažinti nestandartiniais SSL prievadais vykdomą komunikaciją.	Bylų tikrinimas atliekamas pasitelkiant statinę ir dinaminę analizę. Sistema atpažįsta bylas, kurios stengiasi išvengti patikrinimo (*angl. sandbox evasion*), skirto tokių kenksmingų bylų analizei. Sistema atpažįsta nestandartiniais SSL prievadais vykdomą komunikaciją.
5.10.	Sistema turi imituoti darbo aplinkas (kuriuose tikrinama bylų elgsena): Windows XP, 7.	Sistema imituoja darbo aplinkas (kuriuose tikrinama bylų elgsena): Windows XP, 7.
5.11.	Sistema turi atpažinti ir analizuoti šiuos failų tipus: exe, dll, zip, pdf, MS Office failus, Java, Adobe Flash.	Sistema atpažįsta ir analizuoja šiuos failų tipus: exe, dll, zip, pdf, MS Office failus, Java, Adobe Flash.
5.12.	Sistema turi analizuoti URL nuorodas esančias el. laiškuose.	Sistema analizuoja URL nuorodas esančias el. laiškuose.
5.13.	Turi būti pateikiama išsami informacija/ ataskaita apie: • Kiekvieną kenksmingą failą; • Informacija apie tai kas ir kada tą failą siuntė; • Prieigą prie kenksmingo failo.	Pateikiama išsami informacija/ ataskaita apie: • Kiekvieną kenksmingą failą; • Informacija apie tai kas ir kada tą failą siuntė; • Prieigą prie kenksmingo failo.

5.14.	Ataskaitoje apie kenksmingo kodo bylą turi būti informacija su data, kada pirmą sykį toks failas buvo užfiksuotas.	Ataskaitoje apie kenksmingo kodo bylą yra informacija su data, kada pirmą sykį toks failas buvo užfiksuotas.
6.	**Techninis aptarnavimas**	
6.1.	Tiekėjas visu sutarties galiojimo laikotarpiu (nuo perdavimo–priėmimo akto pasirašymo dienos) atlieka abiejų nuomojamų įrenginių techninį aptarnavimą, kuris turi apimti gamintojo signatūrų (įsilaužimų ir kitų grėsmių aprašų) prenumeratą	Tiekėjas visu sutarties galiojimo laikotarpiu (nuo perdavimo–priėmimo akto pasirašymo dienos) atlieka abiejų nuomojamų įrenginių techninį aptarnavimą, kuris apima gamintojo signatūrų (įsilaužimų ir kitų grėsmių aprašų) prenumeratą
6.2.	Tiekėjas garantuoja 8x5 techninį įrangos aptarnavimą naudojimo vietoje (angl. on-site) ir su ne blogesniu kaip 4 val. reakcijos laiku	Tiekėjas garantuoja 8x5 techninį įrangos aptarnavimą naudojimo vietoje (angl. on-site) ir su ne blogesniu kaip 4 val. reakcijos laiku
6.3.	Perkančioji organizacija, sutarties galiojimo laikotarpiu pastebėjusi techninės įrangos trūkumų, turi teisę savo pasirinkimu pareikalauti, kad techninė įranga būtų pakeista tinkamos kokybės techninė įranga, arba kad tiekėjas neatlygintinai per protingą, perkančiosios organizacijos nurodytą terminą pašalintų techninės įrangos trūkumus	Perkančioji organizacija, sutarties galiojimo laikotarpiu pastebėjusi techninės įrangos trūkumų, turi teisę savo pasirinkimu pareikalauti, kad techninė įranga būtų pakeista tinkamos kokybės techninė įranga, arba kad tiekėjas neatlygintinai per protingą, perkančiosios organizacijos nurodytą terminą pašalintų techninės įrangos trūkumus
6.4.	Ne mažiau kaip 30 val. konsultavimo diegimo ir eksploatavimo klausimais visu sutarties galiojimo laikotarpiu.	30 val. konsultavimo diegimo ir eksploatavimo klausimais visu sutarties galiojimo laikotarpiu.

3.2. II pirkimo objekto dalis

(Pildoma, jei tiekėjas pasiūlymą teikia II pirkimo objekto daliai)

Eil. Nr.	Prekės pavadinimas*	Mato vnt.	Kiekis	Kaina, Eur be PVM	Kaina, Eur su PVM
	1	2	3	4	5
1.	Centralizuotos įvykių kaupimo ir analizavimo sistemos išplėtimo licencija „IBM Security QRadar SIEM Event Capacity Pack Increase of 2.5K EPS Install License“ (1 vnt.) su 24 mėn. palaikymu	Vnt.	1	71360,00	86345,60
2.	Centralizuotos įvykių kaupimo ir analizavimo sistemos išplėtimo licencija „IBM Security QRadar SIEM Flow Capacity Increase from 25K to 50K FPM Install License“ (1 vnt.) su 24 mėn. palaikymu	Vnt.	1	24137,00	29205,77
3.	Centralizuotos įvykių kaupimo ir analizavimo sistemos išplėtimo licencija „IBM Security QRadar SIEM Flow Capacity Increase 50K to 100K FPM Install License“ (1 vnt.) su 24 mėn. palaikymu	Vnt.	1	44107,00	53369,47
4.	Kaina iš viso:			139604,00	168920,84

Bendra I pirkimo objekto dalies pasiūlymo kaina su PVM yra 168920 Eur 84 ct *(vienas šimtas šešiasdešimt aštuoni tūkstančiai devyni šimtai dvidešimt eurų ir aštuoniasdešimt keturi centai)*. Į šią sumą įeina visos išlaidos ir visi mokesčiai, taip pat ir PVM, kuris sudaro 29316 Eur 84 ct *(dvidešimt devyni tūkstančiai trys šimtai šešiolika eurų ir aštuoniasdešimt keturi centai)*.

* Į nurodytų prekių kainą turi būti įskaičiuota ne mažiau kaip 30 val. konsultavimo diegimo ir eksploatavimo metu iškilusiais klausimais visu sutarties galiojimo laikotarpiu.

PASTABA: *Į kainą turi būti įskaičiuotas PVM, kiti mokesčiai bei visos kitos išlaidos. Tiekėjas finansiniame pasiūlyme turi nurodyti kainą Eur su PVM, jei tiekėjas yra PVM mokėtojas arba Eur be PVM, jei tiekėjas yra ne PVM mokėtojas. Prie kainos skaičiais būtina nurodyti žodžius „su PVM" arba „be PVM".*

Siūlomos prekės visiškai atitinka pirkimo dokumentuose nurodytus reikalavimus ir jų sąvybės yra tokios:

Eil. Nr.	Pavadinimas ir reikalaujama reikšmė	Tiekėjo pasiūlymas
1.	Centralizuotos įvykių kaupimo ir analizavimo sistemos išplėtimo licencija „IBM Security QRadar SIEM Event Capacity Pack Increase of 2.5K EPS Install License" (1 vnt.)	Centralizuotos įvykių kaupimo ir analizavimo sistemos išplėtimo licencija „IBM Security QRadar SIEM Event Capacity Pack Increase of 2.5K EPS Install License" (1 vnt.)
2.	Centralizuotos įvykių kaupimo ir analizavimo sistemos išplėtimo licencija „IBM Security QRadar SIEM Flow Capacity Increase from 25K to 50K FPM Install License" (1 vnt.)	Centralizuotos įvykių kaupimo ir analizavimo sistemos išplėtimo licencija „IBM Security QRadar SIEM Flow Capacity Increase from 25K to 50K FPM Install License" (1 vnt.)
3.	Centralizuotos įvykių kaupimo ir analizavimo sistemos išplėtimo licencija „IBM Security QRadar SIEM Flow Capacity Increase 50K to 100K FPM Install License" (1 vnt.)	Centralizuotos įvykių kaupimo ir analizavimo sistemos išplėtimo licencija „IBM Security QRadar SIEM Flow Capacity Increase 50K to 100K FPM Install License" (1 vnt.)
4.	Licencijos palaikymo terminas – 24 (dvidešimt keturi) mėnesiai.	Licencijos palaikymo terminas – 24 (dvidešimt keturi) mėnesiai.
5.	Ne mažiau kaip 30 val. konsultavimo diegimo ir eksploatavimo klausimais visu sutarties galiojimo laikotarpiu	30 val. konsultavimo diegimo ir eksploatavimo klausimais visu sutarties galiojimo laikotarpiu

4. Kartu su pasiūlymu pateikiami šie dokumentai:

Eil. Nr.	Pateiktų dokumentų pavadinimas	Dokumento puslapių skaičius
1.	Valstybės įmonės Registrų centras pažyma, patvirtinanti jungtinius kompetentingų institucijų tvarkomus duomenis	2
2.	VRM IRD pažyma	1
3.	VRM IRD pažyma	1
4.	Tiekėjo deklaracija	1

5.	Deklaracija	1
6.	Valstybės įmonės Registrų centras elektroninis sertifikuotas išrašas	3
7.	Įstatai	27
8.	Sutarčių sąrašas	1
9.	Deklaracija dėl sutarties	1
10.	Gamintojo pažyma	10
11.	Specialistų sąrašas	1
12.	Specialistų CV	18
13.	Specialistų deklaracijos	5
14.	Specialistų diplomai	9
15.	Specialistų sertifikatai	15
16.	Įgaliojimas	2

5. Šiame pasiūlyme yra pateikta ir konfidenciali informacija[1]:

Eil. Nr.	Pateikto dokumento pavadinimas	Dokumentas yra įkeltas šioje CVP IS pasiūlymo lango eilutėje („Prisegti dokumentai“)	Informacija konfidenciali *taip/ne*
1.	Valstybės įmonės Registrų centras pažyma, patvirtinanti jungtinius kompetentingų institucijų tvarkomus duomenis	Prisegti dokumentai, 2 eilutė	Taip
2.	VRM IRD pažyma	Prisegti dokumentai, 3 eilutė	Taip
3.	VRM IRD pažyma	Prisegti dokumentai, 4 eilutė	Taip
4.	Tiekėjo deklaracija	Prisegti dokumentai, 5 eilutė	Ne
5.	Deklaracija	Prisegti dokumentai, 6 eilutė	Taip
6.	Valstybės įmonės Registrų centras elektroninis sertifikuotas išrašas	Prisegti dokumentai, 7 eilutė	Taip
7.	Įstatai	Prisegti dokumentai, 8 eilutė	Taip
8.	Sutarčių sąrašas	Prisegti dokumentai, 9 eilutė	Taip
9.	Deklaracija dėl sutarties	Prisegti dokumentai, 10 eilutė	Taip
10.	Gamintojo pažyma	Prisegti dokumentai, 11-15 eilutės	Taip
11.	Specialistų sąrašas	Prisegti dokumentai, 16 eilutė	Taip
12.	Specialistų CV	Prisegti dokumentai, 17-21 eilutė	Taip
13.	Specialistų deklaracijos	Prisegti dokumentai, 22-26 eilutė	Taip
14.	Specialistų diplomai	Prisegti dokumentai, 27-33 eilutė	Taip

[1] Pildyti, jei bus pateikta konfidenciali informacija. Tiekėjas negali nurodyti, kad konfidenciali yra pasiūlymo kaina arba kad visas pasiūlymas yra konfidencialus. Tiekėjui nenurodžius, kokia informacija yra konfidenciali, laikoma, kad konfidencialios informacijos pasiūlyme nėra.

15.	Specialistų sertifikatai	Prisegti dokumentai, 34-38 eilutė	Taip
16.	Įgaliojimas	Prisegti dokumentai, 39-40 eilutė	Taip

Pasiūlymas galioja iki termino, nustatyto pirkimo dokumentuose.

Pardavimų vadovas		Sigitas Vasiliauskas
(Tiekėjo arba jo įgalioto asmens pareigų pavadinimas)	*(Parašas[2])*	*(Vardas ir pavardė)*

[2] Pasirašoma atskirai elektroniniu parašu tuo atveju, kai dokumente nurodytas kitas nei visą pasiūlymą pasirašantis asmuo.