Konkurso sąlygų 2 priedas

PROJEKTO „VALSTYBĖS DEBESIJOS PASLAUGŲ TEIKIMO INFRASTRUKTŪROS SUKŪRIMAS“
SAUGUMO SPRENDIMO ĮSIGIJIMAS

TECHNINĖ SPECIFIKACIJA

I. BENDRA INFORMACIJA

I.1. Šiuo metu Informacinės visuomenės plėtros komitetas (toliau **– IVPK arba Perkančioji organizacija**) vykdydamas Lietuvos Respublikos Vyriausybės 2015 m. gegužės 13 d. nutarimą Nr. 498 „Dėl valstybės informacinių išteklių infrastruktūros konsolidavimo ir jos valdymo optimizavimo“ (aktuali redakcija), įgyvendina 2014 –2020 metų Europos Sąjungos fondų investicijų veiksmų programos 2 prioriteto „Informacinės visuomenės skatinimas“ priemonės Nr. J06-CPVA-V „IRT infrastruktūros optimizavimas ir sauga“ lėšomis finansuojamą investicijų projektą „Valstybės debesijos paslaugų teikimo infrastruktūros sukūrimas“ (toliau – **Projektas** arba **Investicijų projektas**), su kuriuo galima susipažinti adresu https://www.epaslaugos.lt/portal/file/e11229f7-33f0-456e-8e0f-c1dfaf1912ee.. Projekto tikslas – sukurti ir įdiegti valstybės debesijos paslaugų teikimo veiklai reikalingą informacinių ir ryšių technologijų (IRT) infrastruktūrą ir suformuoti žmogiškuosius išteklius, reikalingus valstybės debesijos paslaugoms teikti. Projektui keliami šie pagrindiniai uždaviniai:

I.1.1. Parengti detalią loginę debesijos paslaugų teikimo IT infrastruktūros architektūrą, apimant virtualizuotų tarnybinių stočių, virtualizuotų duomenų talpyklų, duomenų perdavimo tinklų topologijos architektūrų ir rezervinio kopijavimo sistemų veiklos modelius;

I.1.2. Įsigyti ir parengti techninę įrangą bei saugos sprendimo technines priemones debesijos paslaugų teikimui;

I.1.3. Sukurti ir įdiegti debesijos paslaugų teikimo valdymo platformą ir debesijos paslaugų teikimui reikalingas priemones;

I.1.4. Parengti / atnaujinti valstybės debesijos paslaugų tiekėjo organizacijos (toliau – **VDPT** arba **VITC**)[1] siekiamo IT veiklos valdymo bei veiklos planavimo ir valdymo reglamentavimą ir jo įgyvendinimo priemones (politikas, procesus, procedūras), būtinas sėkmingam Valstybės informacinių išteklių VII infrastruktūros konsolidavimui ir numatytiems rezultatams pasiekti;

[1] VDPT - Valstybės debesijos paslaugų teikėjas, VITC - Valstybės informacinių technologijų centras

I.1.5. Talpinti Valstybės informacinių išteklių infrastruktūrą VITC debesijos paslaugų teikimo IT infrastruktūroje, įgalinant jų veikimą ir tvarkymą naudojant debesijos paslaugas;

I.1.6. Suteikti ir sustiprinti VITC institucinių ir žmogiškųjų išteklių žinias, gebėjimus bei kompetencijas, reikalingas teikti Debesijos paslaugas ir valdyti VITC vadovaujantis pasaulyje pripažintomis metodikomis ir gerosiomis praktikomis;

I.1.7. Parengti priemones Projekto įgyvendinimui ir tęstinumui užtikrinti.[2]

I.2. Įgyvendinant Projektą, Perkančioji organizacija jau įvykdė viešąjį pirkimą ir pasirašė sutartį su paslaugų tiekėju,[3] kuris bendradarbiaudamas su Perkančiosios organizacijos atstovais parengė detalią VDPT loginę debesijos paslaugų teikimo IT infrastruktūros architektūrą (toliau – **Detali architektūra** arba **Architektūra**), kuri buvo suderinta su Nacionaliniu kibernetinio saugumo centru ir patvirtinta Perkančiosios organizacijos. Su dokumentu galima susipažinti adresu: https://ivpk.lrv.lt/uploads/ivpk/documents/files/veikla/VII%20konsolidavimas/Login%C4%97_Debesijos_paslaug%C5%B3_teikimo_IT_infrastrukt%C5%ABros_architekt%C5%ABra.pdf.

I.3. Vadovaujantis Detalios architektūros dokumentu, jame suprojektuotu ir patvirtintu sprendimu, Perkančioji organizacija vykdo VDPT techninės ir sisteminės programinės įrangos (toliau – **Įranga**) įsigijimą, diegimą ir konfigūravimą.

I.4. Siekdama užtikrinti rinkos konkurenciją, Perkančioji organizacija numato Detalioje architektūroje suprojektuoto sprendimo įgyvendinimui būtiną Įrangą įsigyti atskirais pirkimais / pirkimų dalimis. Atsižvelgiant į tai, kad Detalioje architektūroje suprojektuotas sprendimas turės veikti kaip viena visuma, o Įranga bus perkama atskirais pirkimais / pirkimų dalimis (t.y. potencialiai galimi skirtingi Įrangos tiekėjai / gamintojai), Perkančioji organizacija atskiru viešuoju pirkimu atrinko tiekėją, kuris teikia Įrangos įdiegimo bei integravimo paslaugas (toliau – **Diegėjas**). Diegėjas, glaudžiai bendradarbiaudamas su Įrangos tiekėjais / gamintojais (toliau – **Įrangos tiekėjai**) bei Perkančiosios organizacijos atstovais, privalo pilna apimtimi užtikrinti korektišką ir galutinį Detalioje architektūroje suprojektuoto sprendimo įdiegimą, integravimą bei pridavimą Perkančiajai organizacijai eksploatacijai, o kiekvienas Įrangos tiekėjas, laimėjęs viešąjį pirkimą, privalės ne tik laiku pristatyti Pirkimo dokumentų reikalavimus atitinkančią Įrangą, bet glaudžiai bendradarbiaudamas su Diegėju, Perkančiosios organizacijos atstovais bei kitais potencialiais Įrangos tiekėjas (kitų šio Projekto pirkimų / pirkimų dalių dalyviais) atlikti Pirkimo dokumentuose numatytus įrangos montavimo, instaliavimo, pradinio konfigūravimo ir kitus darbus, užtikrinančius Detalios

[2] Perkančioji organizacija taip pat įgyvendina susijusį investicijų projektą „Valstybės informacinių išteklių infrastruktūros konsolidavimas ir įgyvendinimas", finansuojamą iš 2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programos 10 prioriteto „Visuomenės poreikius atitinkantis ir pažangus viešasis valdymas" priemonės Nr. 10.1.1-ESFA-V-912 (galima susipažinti adresu https://www.epaslaugos.lt/portal/file/2cbef3ec-9cce-41e9-bf8d-b5d85edf527c), kurio uždaviniai ir rezultatai yra tiesiogiai susiję su Projekto uždaviniais ir rezultatais, todėl, siekiant bendrų tikslų ir rezultatų įgyvendinimo, visi Projekte dalyvaujantys įrangos/paslaugų tiekėjai (tame tarpe ir šio viešojo pirkimo laimėtojas), privalės glaudžiai bendradarbiauti su 10 prioriteto projekte dalyvaujančiais įrangos/paslaugų tiekėjais (prireikus).

[3] Informaciją apie viešąjį pirkimą galima rasti adresu: https://cvpp.eviesiejipirkimai.lt/Notice/Details/2018-699454

architektūros dokumente aprašytos infrastruktūros veikimą (konkrečios atsakomybių ribos tarp Įrangos tiekėjų, Diegėjo ir Perkančiosios organizacijos aprašytos atsakomybių matricoje – pridedama).

I.5. Projekto įgyvendinimo metu vykdomi/įvykdyti žemiau išvardinti pirkimai:[4]

I.5.1. Sprendimo diegimo ir integravimo paslaugų pirkimas - atlikta;

I.5.2. A, B, C tipo tarnybinių stočių pirkimas - atlikta;

I.5.3. Duomenų saugyklų ir SAN tipo komutatorių sprendimo pirkimas - atlikta;

I.5.4. Tinklo įrangos pirkimas - atlikta;

I.5.5. **Saugos sprendimo pirkimas (šio pirkimo objektas);**

I.5.6. Centralizuoto monitoringo sprendimo pirkimas;

I.5.7. Rezervinio duomenų kopijavimo ir atstatymo sprendimo pirkimas - vykdoma**;**

I.5.8. Tarnybinių stočių ir tinklo virtualizacijos licencijų pirkimas - atlikta;

I.5.9. Microsoft (operacinių sistemų ir DBVS) arba lygiaverčių licencijų pirkimas - atlikta;

I.5.10. Oracle (DBVS) arba lygiaverčių licencijų pirkimas – atlikta.

II. PIRKIMO TIKSLAS IR APIMTIS

II.1. Šio viešojo pirkimo tikslas – įsigyti Detalios architektūros dokumente aprašyto Saugumo sprendimo komponento, skirto prieigos kontrolės valdymui, įgyvendinimui reikalingą įrangą.

III. BENDRIEJI REIKALAVIMAI SIŪLOMAI ĮRANGAI IR PASLAUGOMS

III.1. **Bendrieji reikalavimai siūlomos įrangos tiekėjui:**

III.1.1. Įrangos tiekėjas turi būti siūlomos įrangos gamintojo atstovas, įgaliotas pateikti (parduoti), įdiegti ir aptarnauti siūlomą įrangą arba turi būti sudaręs sutartį su tokiu atstovu, turinčiu išvardintas teises. Pasiūlyme turi būti pateiktos Įrangos gamintojo pažymos, patvirtinančios, kad Įrangos tiekėjas yra siūlomos įrangos gamintojo atstovas, įgaliotas pateikti (parduoti), įdiegti ir aptarnauti siūlomą įrangą arba turi būti sudaręs sutartį su tokiu atstovu, turinčiu išvardintas teises (turi būti pateikta skaitmeninė kopija).

III.2. **Bendrieji reikalavimai siūlomai įrangai ir licencijoms:**

III.2.1. Į bendrą pasiūlymo kainą turi būti įtrauktos visos gamintojo licencijos, reikalingos perkamos Įrangos reikalaujamoms funkcijoms vykdyti ir palaikyti.

III.2.2. Jei licencija pagal gamintojo taisykles galioja vienam įrenginiui, licencijų reikia pateikti tiek, kiek reikalaujama įrenginių.

[4] Kai kurie pirkimai bus skaidomi į atskiras pirkimų dalis. Atsiradus poreikiui, Perkančioji organizacija gali keisti pirkimų ir/arba jų dalių sąrašą.

III.2.3. Įrangos tiekėjas, prieš teikdamas pasiūlymą, turi įvertinti tai, kad įsigyta Įranga bus naudojama Valstybės debesijos paslaugų teikimui, todėl turi būti siūlomos tokio tipo licencijos, kurios leistų Perkančiajai organizacijai be apribojimų teikti Valstybės debesijos paslaugas kitoms valstybės įstaigoms, įmonėms bei organizacijoms.

III.2.4. Įrangos tiekėjui pristačius Techninėje specifikacijoje numatytą įrangą bus pasirašomas priėmimo – perdavimo aktas. Taip pat, teikdamas pasiūlymą, Įrangos tiekėjas turi įvertinti tai, kad turės toliau glaudžiai bendradarbiauti su Diegėju bei Perkančiąja organizacija ir prireikus teikti visas būtinas konsultacijas pasiūlytos įrangos konfigūravimo, eksploatavimo ir kitais klausimais. Konsultacijos turės būti teikiamos tol, kol Perkančioji organizacija ir Diegėjas nepatvirtins, kad Detalioje architektūroje numatytas sprendimas pilna apimtimi įdiegtas ir priduotas eksploatacijai gamybiniu režimu (įskaitant sprendimo bandomąją eksploataciją).

III.2.5. Visą siūlomą techninę ir programinę įrangą Įrangos tiekėjas privalo užregistruoti Perkančiosios organizacijos vardu gamintojų nustatyta tvarka garantinio aptarnavimo paslaugų teikimui, o registracijos duomenis perduoti Perkančiajai organizacijai.

III.2.6. Perkančiajai organizacijai turi būti užtikrinta teisė į programinės įrangos nemokamus atnaujinimus ir klaidų taisymus (garantinio aptarnavimo laikotarpiu).

III.2.7. Visa siūloma įranga turi būti nauja, nenaudota, gamykliniame įpakavime. Pateikiama įranga negali būti gamintojo atnaujinta („Refurbished“ arba „Remarketed“).

III.2.8. Pasiūlyme Įrangos tiekėjas turi pateikti tikslias siūlomos įrangos konfigūracijas, kuriose būtų pateikti tikslūs siūlomos Įrangos komponentų modeliai, prekių kodai, kiekiai, pavadinimai ir kita standartiškai gamintojų konfigūratoriuose pateikiama informacija.

III.2.9. Atitikimas techninės specifikacijos reikalavimams turi būti užtikrintas esant tokiai pačiai (vienodai) siūlomos Įrangos konfigūracijai, t. y. kiekvieno konkretaus punkto iš nurodytų specifikacijoje žemiau atitikimas negali būti užtikrintas vertinant skirtingas įrangos konfigūracijas (dėl ko galimai būtų netenkinami kitų punktų reikalavimai).

III.3. **Bendrieji reikalavimai siūlomos įrangos pristatymui:**

III.3.1. Prieš nustatydama laimėjusį pasiūlymą, Perkančioji organizacija pasilieka teisę pareikalauti galimo pirkimo laimėtojo pristatyti siūlomos Įrangos pavyzdžius (Įranga turi būti Įrangos tiekėjo pristatyta patikrinimui ne vėliau kaip per 45 dienas nuo Perkančiosios organizacijos prašymo) tam, kad būtų praktiškai išmatuotas gamintojo ir/arba Įrangos tiekėjo siūlomos Įrangos charakteristikų atitikimas Techninės specifikacijos bei Lietuvos Respublikos nacionalinio saugumo keliamiems reikalavimams. Tam tikslui pasiekti, Perkančioji organizacija pasilieka teisę perduoti Nacionaliniam kibernetinio saugumo centrui (arba kitoms įgaliotoms įstaigoms) gautą Įrangą patikrinimui bei išvadų pateikimui. Nustačius, kad Įrangos tiekėjo siūloma Įranga realiai neatitinka

Įrangos tiekėjo pateiktame pasiūlyme deklaruojamų Įrangos charakteristikų ir/arba Techninės specifikacijos ir/arba Lietuvos Respublikos nacionalinio saugumo reikalavimų – Įrangos tiekėjo pasiūlymas bus atmetamas.

III.3.1.1. Įrangos tiekėjas įsipareigoja visą įsigyjamą įrangą pristatyti, ir įdiegti per 60 kalendorinių dienų nuo Sutarties įsigaliojimo dienos.

IV. SPECIALIEJI REIKALAVIMAI SIŪLOMAI ĮRANGAI IR PASLAUGOMS

IV.1.1. Visi funkciniai reikalavimai turi būti pagrįsti tiksliomis nuorodomis į gamintojo internetiniame puslapyje esančią informaciją, nurodant dokumentą ir puslapio numerį.

IV.1.2. Visi našumo reikalavimai turi būti pagrįsti nuorodomis į gamintojo techninę informaciją (angl. data sheets) arba kitus gamintojo našumą deklaruojančius dokumentus.

1 lentelė. Prieigos kontrolės valdymo sistema – 1 komplektas

Eil. Nr.	Charakteristikos pavadinimas	Reikalaujama charakteristika (ne blogiau kaip)	Siūloma charakteristika
1.	Įrangos gamintojai, modeliai, modifikacijos (jei yra)	Būtina išvardinti siūlomos įrangos komponentus, jų kiekius, modelius, gamintojus ir produktų kodus. Jeigu siūloma įranga licencijuojama, būtina pateikti licencijų kodus ir trumpą funkcionalumo aprašymą, kurį kiekviena licencija suteikia ir kaip tai atitinka reikalavimus.	
2.	Sprendimo aprašymas	Prieigos kontrolės valdymui skirtas sprendimas turi apimti ne mažiau kaip privilegijuotų vartotojų kontrolės, keleto faktorių tapatybės nustatymo ir nuotolinio prisijungimo prie tinklo komponentus/sistemas.	
3.	Sprendimo architektūra	Sprendimas turi būti diegiamas į virtualią perkančiosios organizacijos infrastruktūrą. Turi būti pateikta visa (pagal gamintojo rekomendacijas) programinė įranga ir visos licencijos, reikalingos šioje lentelėje įvardintam funkcionalumui ir jo palaikymui užtikrinti. Jeigu siūlomo	

		sprendimo veikimui naudojama Oracle ir / arba Microsoft SQL duomenų bazės bei Windows operacinė sistema, šių licencijų pateikti nebūtina.	
4.	Reikalavimai privilegijuotų naudotojų kontrolės komponentui/sistemai:		
4.1.	Privilegijuotų naudotojų kontrolės komponento/sistemos aprašymas	Privilegijuotų naudotojų (administratorių) kontrolės sistema, užtikrinanti naudotojų prisijungimų kontrolę prie resursų bei saugų slaptažodžių maskavimą ir valdymą. Sprendimas turi leisti ne mažiau kaip: 1. valdyti privilegijuotų naudotojų teises ir prieigas; 2. užtikrinti privilegijuotų naudotojų teisių stebėseną; 3. užtikrinti privačių SSH raktų saugumą; 4. valdyti draudžiamų vykdyti CLI komandų sąrašus. Leisti nurodyti leidžiamas ir draudžiamas komandas, draudžiamų vykdyti CLI komandų sąrašus.	
4.2.	Naudotojų autorizacija	Turi būti leidžiama naudotojams prie siūlomos sistemos/komponento jungtis naudojant centralizuotą Microsoft Active directory sprendimą, tačiau autorizacija į galinius įrenginius turi būti vykdoma per skirtingus Microsoft Active directory domenus tarp kurių integracijų nėra t. y. sprendimas turi palaikyti integraciją su skirtingų tenantų infrastruktūra.	
4.3.	Suderinamumas su virtualizacijos platforma	Siūloma įranga turi būti suderinama su perkančiosios organizacijos turima Vmware virtualizacijos platforma.	
4.4.	Testavimo aplinka	Siūlomo sprendimo apimtyje turi būti pateikta programinė įranga (licencijos leidžiančios platforma naudotis ne mažiau kaip 10 darbuotojų) testavimo aplinkai, kurioje bus testuojamas PAM funkcionalumas ir atnaujinimai prieš pakeitimų diegimą į gamybinę aplinką.	

4.5.	Naudotojų, valdomos įrangos, privačių raktų, sesijų skaičiai	Siūlomas sprendimas turi leisti juo naudotis: 1. Ne mažiau kaip 100 naudotojų (administratorių); 2. Leisti naudoti ir stebėti ne mažiau kaip 100 aktyvių sesijų vienu metu; Ne mažiau kaip 5000 įrenginių; 3. Ne mažiau 100000 privačių raktų / slaptažodžių. 4. Neribojamas politikų ir nustatymų skaičius. Pasiūlyme būtina įvardinti licencijų ribojamą funkcionalumą.	
4.6.	Naudotojų valdymas	Sprendimas turi leisti valdyti naudotojus ne mažiau kaip nurodytose sistemose: 1. operacinėse sistemose: Windows, Unix, Linux; 2. duomenų bazėse: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, MySQL, SAP HANA; 3. infrastruktūros valdymo sprendimuose: DELL DRAC, HP iLO, LENOVO IMM/TMM; 4. tinklo ir saugos sprendimuose: Cisco (maršrutizatoriai, komutatoriai ir ugniasienės), Juniper, HPE, CheckPoint, Netscreen, Fortinet; 5. moduliuose: Microsoft Services, Scheduled tasks, IIS application Pool, registries, Microsoft domain accounts; 6. aplikacijose: WebLogic, SAP; 7. direktorijose: Active Directory; 8. virtualios infrastruktūros sprendimuose: VMWare ESX/ESXi, vSphere.	
4.7.	Palaikomos sistemos	Sprendimas be papildomų modulių / licencijų turi palaikyti ne mažiau kaip šias sistemas: 1. Cisco; 2. Microsoft Windows; 3. Microsoft SQL; 4. Linux/Unix; 5. Oracle; 6. MySQL; 7. VMWare;	

		8. SAP.	
4.8.	Palaikomi protokolai	Sprendimas be papildomų modulių / licencijų turi palaikyti ne mažiau kaip šiuos protokolus: 1. SSH; 2. RDP; 3. ODBC 4. HTML.	
4.9.	Valdymas	Siūlomas sprendimas turi užtikrinti ne mažiau kaip šiuos reikalavimus: 1. Visi siūlomi moduliai turi būti pateikiami vieno gamintojo ir tarpusavyje pilnai suderinami; 2. Visi sistemos komponentai turi būti prijungti prie centralizuoto valdymo; 3. Sprendimas turi leisti naudoti specializuotus vykdomuosius scenarijus nestandartiniams prisijungimams valdyti.	
4.10	Sprendimo patikimumas	Siūlomas sprendimas turi užtikrinti ne mažiau kaip šiuos reikalavimus: 1. Sprendimas turi būti diegiamas aukšto patikimumo (angl. HA) konfigūracijoje, kuri užtikrintų nepertraukiamą Sprendimo veikimą dviejuose duomenų centruose. 2. HA funkcionalumas turi būti užtikrintas siūlomo Sprendimo funkcionalu, o ne platformos ar trečių šalių sprendimais. 3. Sprendimas turi gebėti saugoti privilegijuotas paskyras geografiškai paskirstytuose komponentuose. 4. Sprendimas turi turėti funkcionalumą leidžiantį diegti tarpinius taškus (angl. proxy) nutolusiose lokacijose ir/arba skirtinguose tinklo segmentuose. 5. Sprendimas turi turėti funkcionalumą leidžiantį matyti visų sprendimo	

		komponentų greitaveikos ir būklės informaciją grafinėje naudotojo sąsajoje.	
4.11	Sprendimo saugumas	Siūlomas sprendimas turi užtikrinti ne mažiau kaip: 1. Sprendimas turi būti suderinamas su ne mažiau kaip šiais autentifikacijos sprendimais: LDAP, PKI, RADIUS, two factor authentication RSA SecureID; 2. Sprendimas turi atitikti FIPS 140-2 reikalavimus; 3. Komunikacijos tarp Sprendimo komponentų turi būti atliekamos šifruotais ryšio kanalais; 4. Privilegijuoti naudotojai neturi matyti valdomų paskyrų slaptažodžių; 5. Sprendimas turi leisti naudotojui prisijungti prie valdomų paskyrų nepateikiant slaptažodžio; 6. Sprendimas turi leisti naudotis paskyromis naudotojui nepateikiant slaptažodžio; 7. Sprendimas turi užtikrinti saugumą: slaptažodžiams, įrašytoms sesijoms, audito pranešimams ir t.t.	
4.12	Integracija	Siūlomas sprendimas turi integruotis su ne mažiau kaip: 1. SIEM sistemomis; 2. LDAP / Active Directory direktorijomis privilegijuotų naudotojų teisių priskyrimui bei pakeitimui; 3. Sprendimas turi leisti paklausti prisijungimo duomenų per aplikacijų programinius interfeisus (API); 4. Sprendimas turi siųsti SNMP ir el. pašto pranešimus; 5. Sprendimas turi integruotis su HSM. 6. Sprendimas turi palaikyti Java, C/C++, .Net arba lygiavertes programavimo kalbas.	
4.13	Ataskaitos ir auditas	Siūlomas Sprendimas turi užtikrinti ne mažiau kaip:	

		1. Sprendimas turi pateikti paskyras, naudotas prisijungimams nurodytu laiko intervalu; 2. Sprendimas turi turėti galimybę pateikti paskyrų panaudojimo ir stebėsenos duomenis; 3. Sprendimas turi gebėti generuoti ataskaitas nurodytais laiko intervalais ar pagal pageidavimą; 4. Sprendimas turi leisti suformuoti šias ataskaitas: • prieigos ataskaitą, • privilegijuotų naudotojų veiksmų ataskaitą, • privilegijuotų paskyrų suvestinę ataskaitą, • valdomų aplikacijų suvestinę ataskaitą; 5. Sprendimas turi leisti sugeneruoti ataskaitas ne mažiau kaip šiais formatais: Microsoft Excel, CSV; 6. Sprendimas turi leisti generuoti atskaitas apie prieigą prie valdomų sistemų; 7. Sprendimas turi leisti sugeneruoti ataskaitas apie prieigos prašymus; 8. Sprendimas turi leisti sugeneruoti atskaitas apie nesėkmingas slaptažodžių užklausas ir nesėkmingus prisijungimus; 9. Audito informaciją turi būti galima eksportuoti į išorines sistemas ataskaitų generavimui ir analizei; 10. Sprendimas turi leisti siųsti ataskaitas arba nuorodas į jas el. paštu.	
4.14	Slaptažodžių prieigos	Sprendimas turi turėti galimybę realizuoti "4 akių politiką", kai prieiga yra suteikiama tik esant patvirtinimui. Sprendimas turi leisti privilegijuotam naudotojui užsakyti prieigą vėlesniam laikui.	

		Sprendimas turi audituoti kiekvieną slaptažodžio užklausą ir prieigos suteikimą.	
4.15	Prisijungimo duomenų valdymas	Siūlomas sprendimas turi užtikrinti ne mažiau kaip šiuos funkcionalumus: 1. Sprendimas turi neleisti naudoti prieš tai buvusių slaptažodžių; 2. Sprendimas turi leisti naudoti keletą MS AD ar LDAP autentifikacijos valdymo sprendimų vienu metu; 3. Sprendimas turi leisti siųsti el. laiškus apie veiksmus su paskyromis; 4. Sprendimas turi užtikrinti unifikuotą prieigą prie nutolusių sistemų, neatskleidžiant prisijungimo duomenų privilegijuotam naudotojui; 5. Sprendimas turi turėti funkcionalumą leidžiantį sugeneruoti ir patikrinti slaptažodžius pagal iš anksto nustatytas taisykles; 6. Sprendimas turi leisti palyginti PAM saugomus slaptažodžius su įrenginių prie kurių jungiamasi slaptažodžiais ir esant poreikiui juos suvienodinti; 7. Sprendimas turi leisti periodiškai keisti valdomų įrenginių paskyrų (angl. account) slaptažodžius; 8. Sprendimas turi leisti pakeisti valdomų įrenginių paskyrų slaptažodį po panaudojimo; 9. Sprendimas turi identifikuoti privilegijuotas paskyras (pvz. administrator, root ir pan.) nurodytuose įrenginiuose; 10. Sprendimas turi leisti saugoti valdomų paskyrų slaptažodžių istoriją; 11. Sprendimas turi turėti funkcionalumą leidžiantį įkelti valdomų įrenginių paskyrų sąrašą iš struktūrizuotos bylos;	

		12. Sprendimas turi turėti funkcionalumą valdomai paskyrai nurodyti viršesnę paskyrą, leidžiančią atstatyti slaptažodžius net jei valdoma paskyra yra blokuota ar slaptažodžiai nesutampa; 13. Sprendimas turi rinkti audito informaciją: • valdomose sistemose atliktus veiksmus, • paskyrų pakeitimus, • slaptažodžių panaudojimą, • slaptažodžių užklausas ir patvirtinimus, atmetimus.	
4.16	Stebėsena ir kontrolė	Siūlomas Sprendimas turi užtikrinti ne mažiau kaip šiuos funkcionalumus: 1. Sprendimas turi veikti kaip tarpinis taškas (angl. jump, proxy) prisijungimams prie valdomų sistemų; 2. Sprendimas turi veikti be papildomų agentų diegimo stebimose sistemose; 3. Sprendimas turi gebėti įrašyti veiksmus, vykdomus šiose sistemose: - Windows, - UNIX/Linux, - maršrutizatoriuose ir komutatoriuose, - duomenų bazėse, virtualizacijos platformų valdymo sprendimuose (VMWare Client), - domeno valdikliuose. 4. Stebėsena neturi paveikti valdomos sistemos greitaveikos; 5. Turi būti galimybė stebėti valdymo valdomas sistemas nereikalaujant tinklo struktūros pakeitimų; 6. Sprendimas turi gebėti saugoti stebėsenos įrašus saugiame, šifruotame formate ir užtikrinti įrašų integralumą; 7. Sprendimas turi turėti detaliai pasirenkamą stebėsenos ir	

		kontrolės audito mechanizmą ir sukauptų duomenų peržiūrą; 8. Sprendimas turi leisti atlikti vykdytų komandų paiešką įrašytose sesijose; 9. Sprendimas turi gebėti atvaizduoti įrašytas sesijas; 10. Sprendimas turi leisti matyti realiu laiku vykstančias sesijas ir jas nutraukti; 11. Sprendimas turi gebėti persiųsti detalią informaciją į SIEM sprendimus; 12. Sprendimas turi gebėti suspausti įrašus ilgalaikiam saugojimui; 13. Sprendimas neturi reikalauti papildomų agentų ar aplikacijų, kurios yra būtinos norint paleisti tarpines (angl. proxy) sesijos privilegijuotų naudotojų įrenginiuose; 14. Sprendimas turi leisti privilegijuotiems naudotojams pasiekti valdomas sistemas šiais įrankiais: - bet kokio tipo nuotolinės prieigos aplikacija, gebančia komunikuoti MS RDP protokolu, - bet kokio tipo tekstine valdymo aplikacija, gebančia komunikuoti SSH protokolu; 15. Sprendimas turi išsaugoti visus naudotojo mygtukų paspaudimus.	
4.17	Unix / Linux komandų valdymas	Siūlomas sprendimas turi užtikrinti ne mažiau kaip šiuos funkcionalumus: 1. Sprendimas turi leisti nurodyti, kokias komandas privilegijuoti naudotojai gali vykdyti Unix/Linux tipo sistemose; 2. Sprendimas turi leisti kontroliuoti naudojamas SSH komandas naudojant „baltuosius“ ir „juoduosius“ sąrašus 3. Sprendimas turi leisti įrašyti visas CLI vykdomas komandas;	

		4. Sprendimas turi leisti įrašyti visas CLI vykdytas komandas; 5. Sprendimas turi leisti įrašyti visą įvesties ir išvesties tekstą CLI sąsajoje.	
4.18	SSH raktų valdymas	Sprendimas turi leisti saugoti privačius SSH raktus apsaugotoje saugykloje. Sprendimas turi leisti užtikrinti tokio lygio privačių SSH raktų apsaugą, kokia yra taikoma slaptažodžiams.	
4.19	Microsoft Windows operacinių sistemų valdymas	Siūlomas sprendimas turi užtikrinti ne mažiau kaip šiuos funkcionalumus: 1. Sprendimas turi leisti realizuoti rolėmis grįstą naudotojų prieigą (RBAC); 2. Sprendimas turi leisti realizuoti politikų išimtis; 3. Sprendimas turi leisti kontroliuoti sistemas, neįtrauktas į domeną; 4. Sprendimas turi leisti fiksuoti visus naudotojų veiksmus stebimose Microsoft Windows aplikacijose; 5. Sprendimas turi leisti kontroliuoti lokalias administratorių paskyras.	
4.20	Suderinamumas su Syslog	Sprendimas turi leisti siųsti žurnalinius įrašus Syslog protokolu.	
4.21	Grafinė sąsaja	Sprendimas turi turėti ne mažiau kaip: 1. Grafinę naudotojų sąsają, pasiekiamą saugiu HTTPS protokolu interneto naršykle ir nereikalauti nesaugių trečių šalių technologijų, tokių kaip Flash, ActiveX ar JAVA; 2. Funkcionalumą leidžiantį pasiekti valdomų sistemų darbalaukius per saugią grafinę HTML5 sąsają.	
5.	Reikalavimai keleto faktorių tapatybės nustatymo kontrolės sprendimui:		
5.1.	Suderinamumas	Siūloma sistema turi būti pilnai suderinama su siūloma privilegijuotų naudotojų valdymo ir nuotolinio prisijungimo prie	

		tinklo sistemomis/komponentais bei Vmware virtualizacijos platforma.	
5.2.	Kiekis	Sprendimą turi sudaryti ne mažiau kaip 4 vnt. vieno gamintojo aukšto patikimumo sistemų (kiekviena sistema turi būti sudaryta iš ne mažiau kaip dviejų klasterio narių). Turi būti pateiktos dvi vidutinio ir dvi mažo našumo sistemos.	
5.3.	Funkcionalumas	Kiekviena siūlomo sprendimo sistema turi užtikrinti ne mažiau kaip šiuos funkcionalumus: 1. Turi veikti kaip dviejų faktorių naudotojų tapatybės nustatymo serveris; 2. Turi integruotis su įvairiomis IT sistemomis, siekiant pakeisti tapatybės nustatymą statinių slaptažodžių pagalba į tapatybės nustatymą vienkartinių slaptažodžių pagalba; 3. Turi turėti integruotą duomenų bazę; 4. Turi veikti kaip RADIUS serveris; 5. RADIUS serveris turi palaikyti ne mažiau kaip: • 802.1X, • EAP; 6. Valdymas turi būti realizuotas per HTTPS arba lygiavertį sprendimą; 7. Turi leisti naudoti kelių lygių administratorius, turinčius skirtingas teises.	
5.4.	Naudotojų, kodų generatorių kiekis	Kiekviena vidutinio našumo sistema: 1. Turi leisti dirbti ne mažiau kaip 200 naudotojų; 2. Turi būti galimybė, esant poreikiui, plėsti iki ne mažiau kaip 2000 naudotojų. 3. Turi būti pateikta ne mažiau kaip 200 vnt. vienkartinių kodų generatorių (programinių), kurių galiojimo trukmė būtų ne mažesnė kaip 60 mėn. Kodų generatoriai turi veikti savarankiškai be papildomų	

		perdavimo terpių kaip internetas/GSM ir pan. Kiekviena mažo našumo sistema: 1. Turi leisti dirbti ne mažiau kaip 50 naudotojų; 2. Turi būti galimybė, esant poreikiui, plėsti iki ne mažiau kaip 2000 naudotojų. 3. Turi būti pateikta ne mažiau kaip 50 vnt. vienkartinių kodų generatorių (programinių), kurių galiojimo trukmė būtų ne mažesnė kaip 60 mėn. Kodų generatoriai turi veikti savarankiškai be papildomų perdavimo terpių kaip internetas/GSM ir pan.	
5.5.	Sprendimo patikimumas	Kiekviena siūlomo sprendimo sistema turi būti diegiama aukšto patikimumo (angl. HA) konfigūracijoje, kuri užtikrintų nepertraukiamą sistemos veikimą dviejuose duomenų centruose. . HA funkcionalumas turi būti užtikrintas siūlomos sistemos funkcionalu, o ne platformos ar trečių šalių sprendimais. Kiekvieną sistemą turi sudaryti ne mažiau kaip du virtualizuoti įrenginiai (mazgai), kurie diegiami skirtinguose duomenų centruose. Kiekviena sistema turi palaikyti ne mažiau kaip šias aukšto patikimumo funkcijas: • Sutrikus pagrindinio įrenginio darbui sistema automatiškai persijungia į žemesnį prioritetą turintį įrenginį; • Konfigūracija tarp įrenginių turi būti sinchronizuojama; • Prievadų stebėjimas; • Įrenginių susijungimui į aukšto patikimumo sistemą turi būti naudojamas slaptažodis ar lygiavertė saugumo priemonė užtikrinanti,	

		kad į telkinį susijungtų tik numatytieji įrenginiai Tarp aukšto patikimumo konfigūracijoje naudojamų virtualių įrenginių turi būti automatiškai sinchronizuojama ne mažiau nei ši informacija: • informacija apie kodų generatorius; • informacija apie naudotojus; • informacija apie naudotojų susiejimą su kodų generatoriais.	
5.6.	Vienkartiniai kodų generatoriai	Kiekviena siūlomo sprendimo sistema turi palaikyti ne mažiau kaip: 1. Aparatinius vienkartinių kodų generatorius. Šie kodų generatoriai turi veikli be jokio išorinio ryšio t. y. be interneto/GSM ar panašių perdavimo terpių. 2. Programinius vienkartinių kodų generatorius, diegiamus į kompiuterius ir mobiliuosius įrenginius, kuriuose įdiegtos ne mažiau kaip nurodytos operacinės sistemos: - Windows OS, - iOS, - Android. 3. Programiniai vienkartiniai kodų generatoriai turi veikti be jokio išorinio ryšio t. y. be interneto/GSM ar panašių perdavimo terpių; 4. Leisti nustatyti, kad programinis vienkartinių kodų generatorius būtų naudojamas su PIN kodu; 5. Leisti nustatyti koks turi būti programinio vienkartinio kodų generatoriaus PIN kodo ilgis.	
5.7.	Naudotojų savitarna	Kiekviena siūlomo sprendimo sistema turi užtikrinti ne mažiau kaip šiuos funkcionalumus: 1. Turi būti savitarnos portalas, kuris vienkartinių kodų generatorių naudotojams	

		naršyklės pagalba leistų atlikti ne mažiau kaip šiuos veiksmus, susijusius su vienkartinių kodų generatoriumi: • užpildyti prašymą gauti naują generatorių; • pranešti apie prarastą generatorių; • generatoriaus sinchronizavimas. 2. Turi leisti junktis prie savitarnos portalo nenaudojant vienkartinių kodų generatoriaus.	
5.8.	Integracijos	Kiekviena sprendimo sistema turi užtikrinti integracijas su ne mažiau kaip su: 1. MS Active Directory; 2. LDAP; 3. SIEM sistemomis; 4. Tinklo komutatoriais; 5. Tinklo maršrutizatoriais; 6. Tinklo ugniasienėmis; 7. VPN koncentratoriais; 8. Linux operacinėmis sistemomis; 9. Windows operacinėmis sistemomis.	
5.9.	Ataskaitos ir auditas	Kiekviena sprendimo sistema turi užtikrinti ne mažiau kaip šiuos funkcionalumus: 1. Turi leisti kaupti informaciją apie administratorių ir naudotojų atliekamus veiksmus, tapatybės nustatymo proceso įvykius; 2. Turi leisti generuoti ataskaitas.	
6.	Reikalavimai nuotolinio prisijungimo prie tinklo sprendimui:		
6.1.	Suderinamumas	Siūlomas sprendimas turi būti pilnai suderinamas su siūloma privilegijuotų naudotojų valdymo sistema ir siūloma keleto faktorių tapatybės nustatymo kontrolės sistema.	
6.2.	Kiekis	Sprendimą turi sudaryti 4 vieno gamintojo aukšto patikimumo sistemos (kiekviena sistema turi būti sudaryta iš ne mažiau kaip dviejų klasterio narių). Turi būti pateiktos dvi vidutinio našumo ir dvi mažo našumo sistemos. Vidutinio našumo sistemose turi būti naudojami vidutinio našumo	

		įrenginiai, mažo našumo sistemose – mažo našumo įrenginiai. Kiekvienas įrenginys turi atitikti žemiau išvardintus reikalavimus (punktai nuo 6.3. iki 6.43.)	
6.3.	Licencijos	Siūlomų įrenginių bazinis funkcionalumas turi būti nuolatinis, t.y. pasibaigus garantiniam aptarnavimui turi veikti maršrutizavimo, ugniasienės, VPN (IPSEC, SSL) funkcionalumai.	
6.4.	Suderinamumas su virtualizacijos platformomis	Siūloma įranga turi būti suderinama su Vmware ESXi 6.7 ir 7.x arba lygiavertėmis virtualizacijos platformomis. Siūloma įranga privalo palaikyti SR-IOV PCI-Express tinklo prievadų plokščių resursų valdymo perdavimą virtualizuotai operacinei sistemai (*angl. guest OS*).	
6.5.	Palaikomos virtualios tinklo sąsajos	Vidutinio našumo įrenginys: Ne mažiau 10 Mažo našumo įrenginys: Ne mažiau 10	
6.6.	Kombinuotas ugniasienės pralaidumas naudojant aplikacijų atpažinimą realiame duomenų sraute, matuojant „enterprise MIX“ arba lygiaverčio (IMIX) srauto turinyje. Jeigu naudojamas ne „enterprise MIX“ turinys, pateikti informaciją apie našumo skaičiavimo metodologiją.	Vidutinio našumo įrenginys: Ne mažiau kaip 5Gbps Mažo našumo įrenginys: Ne mažiau kaip 2,5Gbps	
6.7.	Kombinuotas ugniasienės pralaidumas naudojant aplikacijų atpažinimą, apsaugą nuo įsilaužimų (IPS) bei antivirusinę patikrą realiame duomenų sraute, matuojant „enterprise MIX“ arba lygiaverčio (IMIX) srauto turinyje. Jeigu naudojamas ne „enterprise MIX“ turinys, pateikti informaciją apie našumo skaičiavimo metodologiją.	Vidutinio našumo įrenginys: Ne mažiau kaip 2,5 Gbps. Mažo našumo įrenginys: Ne mažiau kaip 1,5 Gbps	

6.8.	Maksimalus sesijų skaičius vienu metu	Vidutinio našumo įrenginys: Ne mažiau kaip 4000000. Mažo našumo įrenginys: Ne mažiau kaip 2000000	
6.9.	Naudotojų/vartotojų skaičius	Neribotas	
6.10	Įrenginio darbo režimai	Siūlomi įrenginiai turi palaikyti žemiau nurodytus darbo režimus: • maršrutizavimo tarp skirtingų tinklų (OSI L3); • skaidrus – atliekant kontrolę tame pačiame tinkle (OSI L2); • stebėjimo – pasyviai surenkant informacija nuo tinklo įrangos, kuri sugeba atiduoti duomenų srauto kopiją.	
6.11	Maršrutizavimas	Siūlomi įrenginiai privalo palaikyti statinius bei dinaminius maršrutizavimo protokolus bei policy pagrįstą maršrutizavimą (angl. Policy based routing).	
6.12	Dinaminio maršrutizavimo protokolai	Siūlomi įrenginiai privalo palaikyti žemiau įvardintus arba lygiaverčius protokolus: • BGP; • OSPF v2 ir v3; • RIP v2.	
6.13	BGP funkcionalumas	Siūlomi įrenginiai privalo turėti grakštaus BGP perkrovimo (graceful restart) funkcionalumą.	
6.14	IGMP protokolo palaikymas	Siūlomi įrenginiai privalo palaikyti IGMP protokolą	
6.15	IPv6 palaikymas	Siūlomi įrenginiai privalo palaikyti IPv6.	
6.16	NAT maršrutizavimo protokolai	Siūlomi įrenginiai privalo palaikyti žemiau įvardintą arba lygiavertį funkcionalumą: • NAT64; • Statinis adresų transliavimas; • Dinaminis adresų transliavimas keičiant prievadus (PAT).	
6.17	Valdymas	Ne mažiau kaip: WEB (HTTP, HTTPS) ir SSH.	
6.18	Centralizuotas valdymas	Turi būti galimybė siūlomus įrenginius centralizuotai valdyti iš Perkančiosios organizacijos šiuo metu naudojamų Fortinet Manager arba Checkpoint centrinio	

		valdymo serverių. Jei siūlomi įrenginiai negali būti valdomi paminėtų centrinio valdymo serverių pagalba, turi būti pateiktas centrinio valdymo sprendimas, kuris centralizuotai valdys siūlomus įrenginius.	
6.19	Aukšto patikimumo savybės	Siūlomi įrenginiai privalo palaikyti žemiau įvardintą funkcionalumą: 1. Apjungti į telkinį įrenginiai turi galėti dirbti aktyvus – pasyvus ir aktyvus – aktyvus darbo režimais; 2. Turi būti galimybė nurodyti, kad veikiantis ir aukštesnį prioritetą turintis įrenginys visada būtų aktyvus telkinio narys; 3. Aukšto patikimumo sistema turi užtikrinti, kad persijungimo metu aktyvios sesijos nenutrūktų; 4. Turi būti galimybė iš įrenginio stebėti ar aktyvūs nurodyti IP adresai. Sistema turi automatiškai persijungti jei nurodyti IP adresai tampa neaktyviais.	
6.20	Integracija su SNMP (Simple Network Management Protocol)	Siūlomi įrenginiai privalo palaikyti SNMP protokolo 2 ir 3 versijas.	
6.21	Suderinamumas su Syslog	Siūlomi įrenginiai turi palaikyti Syslog protokolą.	
6.22	Įvykių žurnalų (event log) palaikymas	Siūlomi įrenginiai privalo palaikyti žemiau įvardintus įvykių žurnalus: • Sisteminiai; • Administravimo; • VPN; • Naudotojų autentifikavimo; • Maršrutizavimo; • Saugos incidentų įvykiai; • Visi konkrečios taisyklės įvykiai.	
6.23	Įvykių žurnalų kaupimas	Siūlomi įrenginiai privalo leisti kaupti įvykių žurnalus įrenginio talpykloje ir/arba siųsti į nuotolinį – centralizuotą įvykių žurnalų kaupimui skirtą įrenginį.	

		Kaupimo vieta turi būti lanksčiai konfigūruojama per kiekvieną fizinę ir virtualią sistemą.	
6.24	Diagnostikos priemonės	Siūlomi įrenginiai privalo leisti srauto / paketų nuo konkretaus interfeiso „įsirašymą“ (packet capture) diagnostikos tikslais su papildomu filtrų (pageidaujami įsirašymo parametrai) užsidėjimu.	
6.25	Nutolusių naudotojų duomenų bazių palaikymas	Siūlomi įrenginiai privalo palaikyti žemiau įvardintas arba lygiavertes duomenų bazes: • LDAP; • RADIUS; • TACACS+; • Dviejų lygių (two-factor) autentifikacija.	
6.26	Prieigos teisių valdymas	Siūlomi įrenginiai privalo: 1. Leisti suteikti prieigos teises tik naudotojams, kurių tapatybė yra patvirtinta; 2. Leisti suteikti prieigos teises naudotojams ir/arba naudotojų grupėms; 3. Leisti nustatyti naudotojų tapatybę, neprašydamas suvesti naudotojo vardo ir slaptažodžio, o pasinaudodamas jau esamomis tinklo paslaugomis, pvz., Active directory arba programinės įrangos (agento) pagalba; 4. Leisti sukurti naudotoją – administratorių, kuris turėtų tik read-only teises (galimybė matyti visą konfigūraciją, bet keisti nieko negalima); 5. Leisti detaliai/individualiai apibrėžti kiekvieno fizinio ir/ar virtualaus naudotojo/administratoriaus teises: - teisė keisti sisteminius įrenginio nustatymus; - teisė kurti, keisti saugumo taisykles; - teisė kurti, keisti taisyklių objektus; - teisė konfigūruoti saugumo patikrų nustatymus; - teisė peržiūrėti įvykių žurnalus; - teisė peržiūrėti ataskaitas;	

		teisė generuoti ataskaitas.	
6.27	Autorizacijos integracija (single sign on)	Siūlomi įrenginiai privalo turėti integracijas su žemiau įvardintomis arba lygiavertėmis sistemomis: • Windows AD; • Microsoft Exchange server; • Windows Terminal Server Agent; • RADIUS; • 802.1x.	
6.28	SSL šifruoto srauto inspekcija	Siūlomi įrenginiai privalo palaikyti SSL šifruoto srauto inspekciją įrenginyje atitinkamai įkeliant reikiamus sertifikatus.	
6.29	Pranešimai naudotojams	Siūlomi įrenginiai turi leisti redaguoti pranešimus naudotojams apie WEB puslapių blokavimą.	
6.30	Botnet valdymas	Siūlomi įrenginiai turi leisti blokuoti Botnet serverių IP adresus bei palaikyti Botnet serverių IP adresų duomenų bazes.	
6.31	DoS apsauga	Siūlomi įrenginiai privalo leisti riboti sesijų arba paketų per sekundę skaičius jų šaltiniui arba adresatui.	
6.32	IPS funkcionalumas	Siūlomi įrenginiai privalo turėti žemiau įvardintą funkcionalumą: 1. Įsilaužimų/pažeidžiamumų (IPS) signatūrų duomenų bazės palaikymas pačiame įrenginyje ir nuolatinis tos bazės atnaujinimas. Funkcionalumas nemokamai (turi būti įtraukta į pasiūlymo kainą) turi veikti ne trumpesniu nei įrangos garantinis laikotarpiu. 2. Turi leisti pasirinkti žemiau įvardintus karantinavimo variantus IPS atakos atveju: - Atakuojantis IP adresas; - Atakuojančio ir atakuojamojo IP adresai. 3. Leisti nustačius grėsmę automatiškai įrašyti paketus, susijusius su grėsme.	
6.33	Protokolų anomalijos	Siūlomi įrenginiai privalo palaikyti protokolų anomalijų aptikimą.	
6.34	Aplikacijų valdymas	Siūloma įranga privalo palaikyti: 1. Aplikacijų identifikavimą sraute ir jų parašus (atpažinimo) ne	

		mažiau kaip 2000 aplikacijų. Privalo būti pateikiami nemokamai (arba įskaičiuoti į pasiūlymo kainą) netrumpesniam kaip garantinio aptarnavimo laikotarpiui; 2. Aplikacijų atpažinimo, nuosavo „parašo“ susikūrimą ir įkėlimą į sistemą; 3. Aplikacijų blokavimą (Application Control); 4. Aplikacijų, naudojančių servisą debesyje (pvz. Google Docs, Drop box ir pan.) atpažinimas ir kontrolė;	
6.35	WEB valdymas	Siūlomi įrenginiai privalo leisti: 1. Administratoriui aprašyti WEB filtravimą pagal URL, turinį, MIME header; 2. URL filtravimą ir kategorizavimą pagal pilną URL, t.y. tikrinama URL host ir atskiros URL dalys. Turi atskirti skirtingų WEB kategorijų turinius, esančius toje pačioje internetinėje svetainėje; 3. Kategorizuoti WEB puslapius duomenų bazėje; 4. Kategorizuoti WEB puslapių kategorijas (ne mažiau kaip 50 vnt.); 5. Laikinai suteikti naudotojui prieigą prie uždraustos WEB kategorijos.	
6.36	Ugniasienės taisyklės	Siūlomi įrenginiai privalo leisti kurti žemiau įvardintas taisykles: 1. Pagal šalis, t.y. siuntėjo ir/arba gavėjo laukuose nurodyti šalį; 2. Per naudotoją.	
6.37	VoIP srautai	Siūlomi įrenginiai privalo palaikyti SIP/H.323 ir RTP pin holding arba lygiaverčius standartus.	
6.38	VPN funkcionalumas	Siūlomi įrenginiai privalo turėti žemiau įvardintą VPN funkcionalumą: 1. Nuotolinio prisijungimo naudotojo VPN klientas turi veikti Windows 10, Android, iOS, MocOS operacinėse sistemose;	

		2. Nuotolinio prisijungimo naudotojo VPN klientas turi mokėti dirbti IPSec ir SSL protokolais; 3. Nuotolinio prisijungimo naudotojo SSL VPN klientas (programinė įranga) turi būti to paties gamintojo kaip ir ugniasienės arba kelių gamintojų, suderinami bendram darbui; 4. Nuotolinio prisijungimo naudotojo VPN klientas turi palaikyti galimybę naudoti skaitmeninius sertifikatus tapatybės nustatymui.	
6.39	Nuotolinio prisijungimo naudotojai	Siūlomi vidutinio našumo įrenginiai privalo būti pateikti su ne mažiau kaip 400 konkurentinių nuotolinio prisijungimo naudotojų VPN klientų licencijų. Siūlomi mažo našumo įrenginiai privalo būti pateikti su ne mažiau kaip 100 konkurentinių nuotolinio prisijungimo naudotojų VPN klientų licencijų. Licencijos turi leisti naudotis SSL VPN ir IPSec VPN tuneliais. Licencijos turi būti įtrauktos į pasiūlymo kainą. Prisijungimas turi veikti ir iš mobilių įrenginių.	
6.40	IPSec kriptavimo algoritmai	Siūlomi įrenginiai privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec kriptavimo algoritmus: • 3DES; • AES128; • AES192; • AES256.	
6.41	IPSec autentifikavimo algoritmai	Siūlomi įrenginiai privalo palaikyti žemiau įvardintus arba lygiaverčius IPSec autentifikavimo algoritmus: • MD5; • SHA-1; • SHA-256; • SHA-384; • SHA-512.	
6.42	Atnaujinimai	Garantinio aptarnavimo laikotarpiu turi būti teikiami programinės įrangos, virusų, piktybinių programų,	

		pažeidžiamumų, įsilaužimų aprašų, URL filtravimo atnaujinimai.	
6.43	Srauto ribojimas	Siūlomi įrenginiai privalo leisti riboti srautą ir taikyti QoS per taisyklę (policy) ir aplikaciją.	
7.	Garantiniai įsipareigojimai, techninis aptarnavimas.	Visiems pateiktiems techniniams ir programiniams komponentams turi būti taikoma ne mažiau kaip 5 metų (ne prasčiau kaip 24 valandos per parą 7 dienos per savaitę 365 dienos per metus) gamintojo užtikrinta garantinė priežiūra įrangos eksploatavimo vietoje (pateikti tai liudijančią gamintojo dokumentaciją jei tai yra standartiniai oficialūs gamintojo įsipareigojimai arba komplektuoti papildomus gamintojo serviso paketus nurodant pasiūlyme jų kodus ir pavadinimus). Garantinė priežiūra turi būti atliekama paties įrangos gamintojo arba jo autorizuoto aptarnavimo atstovo. Garantiniu laikotarpiu turi būti teikiamas nemokamas garantinis aptarnavimas bei atnaujinimų teikimas (visą garantinį laikotarpį įranga turi leisti naudoti visus šioje lentelėje įvardintus funkcionalumus). Perkančiajai organizacijai turi būti suteikta teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas ne blogiau kaip 24x7) internetu, elektroniniu paštu arba telefonu. Turi būti užtikrinta prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekų. Tiekėjas turi pateikti nuorodą į gamintojo internetinę prieigą, kuri įgalina naudojant produkto kodą ir/arba serijinį numerį patikrinti suteiktą gamintojo garantiją internetiniame puslapyje.	

TECHNINĖS SPECIFIKACIJOS PRIEDAS
ATSAKOMYBIŲ MATRICA

Diegėjas, glaudžiai bendradarbiaudamas su Įrangos tiekėjais / gamintojais bei Perkančiosios organizacijos atstovais, privalės pilna apimtimi užtikrinti korektišką ir galutinį Detalioje architektūroje suprojektuoto sprendimo (toliau – Sprendimas) įdiegimą, integravimą bei pridavimą Perkančiajai organizacijai eksploatacijai (bandomajai ir gamybinei). Žemiau pateikiama Sprendimo diegimo (toliau – Diegimas) atsakomybių matrica, apibrėžianti konkrečias atsakomybių ribas tarp Diegėjo, Įrangos tiekėjų ir Perkančiosios organizacijos.

1 lentelė. Atsakomybių matrica

Eil. nr.	Veiksmas	Įrangos tiekėjas	Diegėjas	Perkančioji organizacija
1. Diegimo planavimas ir reikalavimų ruošimas				
1.1	Parengti ir suderinti Diegimo įgyvendinimo planą ir kitą Diegimo dokumentaciją, apibrėžiančią ne mažiau kaip: a) tikslus, apimtį, prielaidas bei apribojimus; b) valdymo struktūrą ir dalyvių atsakomybes; c) komunikavimo procedūrą; d) kokybės valdymo procedūrą; e) rizikų valdymo procedūrą; f) pokyčių valdymo procedūrą; g) dokumentų ir rezultatų derinimo bei galutinio priėmimo procedūrą; h) veiklų grafiką (etapai, veiklos, trukmės, tarpusavio priklausomybės, rezultatų pateikimo terminai).		R[5]	A[6]
1.2	Parengti ir suderinti reikalavimus / standartus Įrangos montavimui, diegimui, pradiniam konfigūravimui, kabeliavimui, žymėjimui, testavimo vykdymui bei rezultatų pateikimo dokumentų šablonus.		R	A
1.3	Parengti ir suderinti Įrangos tiekėjų pristatytos Įrangos testavimo scenarijus bei viso Sprendimo galutinio testavimo scenarijus.		R	A
1.4	Parengti ir suderinti techninės dokumentacijos šablonus.		R	A

[5] R (Responsible) - vykdo darbus
[6] A (Accountable) - priima darbų rezultatus

Eil. nr.	Veiksmas	Įrangos tiekėjas	Diegėjas	Perkančioji organizacija
1.5	Parengti ir suderinti bandomosios eksploatacijos reglamentą.		R	A
2. Įrangos pristatymas, montavimas ir pradinis konfigūravimas				
2.1	Parengti duomenų centro patalpas ir spintas Įrangos montavimui įskaitant el. tiekimą, vėdinimą, fizinę apsaugą, el. rozečių (PDU) montavimą spintose.			R
2.2	Realizuoti duomenų centrų sujungimus pagal Detalios architektūros dokumente apibrėžtus reikalavimus, duomenų perdavimo tinklui.			R
2.3	Pristatyti Įrangą.	R		A
2.4	Pristatyti elementus, reikalingus Įrangos montavimui ir prijungimui duomenų centrų patalpose (reikiamų parametrų kabeliai, tvirtinimo elementai ir pan.).*	R		A
2.5	Parengti ir pateikti Įrangos tiekėjams Įrangos diegimui / konfigūravimui reikalingą informaciją (pvz. Įrangos diegimo planas, Įrangos montavimo ir sujungimo schemos, IP adresavimo taisyklės, ir pan.).		R	A
2.6	Atlikti Įrangos montavimo, prijungimo prie elektros, LAN bei SAN tinklų (sujungimai turi būti užtikrinti visuose duomenų centruose DC1, DC2 ir DC3), kabeliavimo, kabelių žymėjimo, diegimo bei pradinio konfigūravimo darbus ir techninės dokumentacijos paruošimą pagal apibrėžtus reikalavimus ir standartus.*	R	A	
2.7	Atlikti pateikiamos programinės ir techninės Įrangos bei jos vidinės programinės Įrangos (mikrokodo angl. firmware) atnaujinimą ir pilną parengimą eksploatacijai, pateikti darbų sekas ir kitus reikalingus duomenis bei dokumentus Įrangai eksploatuoti elektroniniame pavidale.*	R	A	
2.8	Parengti ir suderinti techninę dokumentaciją, kurioje būtų pateikta: Įrangos montavimo schemos, elektros, LAN bei SAN tinklų sujungimo schemos, kabelių žymėjimo aprašymai bei kiti duomenys, reikalingi tolimesniam Įrangos konfigūravimui ir eksploatavimui (IP adresai, valdymo programų vardai, prisijungimų vardai, slaptažodžiai ir pan.).*	R	A	
2.9	Užregistruoti techninę ir programinę Įrangą Perkančiosios organizacijos vardu gamintojų nustatyta tvarka garantinių paslaugų teikimui ir registracijos duomenis perduoti Perkančiajai organizacijai.	R		A
2.10	Įvertinti ar Įranga pristatyta ir sumontuota pagal apibrėžtus reikalavimus ir standartus.		R	A
2.11	Įvertinti ar Įranga įdiegta ir paruošta tolimesniam Sprendimo konfigūravimui pagal apibrėžtus reikalavimus ir standartus.		R	A

Eil. nr.	Veiksmas	Įrangos tiekėjas	Diegėjas	Perkančioji organizacija
2.12	Atlikti įdiegtos Įrangos veikimo testavimus pagal iš anksto suderintus testavimo scenarijus (aukšto patikimumo, našumo savybių ir pan.) ir pateikti testų rezultatus popieriniu bei elektroniniu formatu pagal apibrėžtus reikalavimus / standartus.*	R	A	
2.13	Įvertinti, ar Įrangos veikimo testavimai atlikti pagal patvirtintus testavimo scenarijus, apibrėžtus reikalavimus ir standartus.		R	A
2.14	Perduoti – priimti pristatytą, sumontuotą ir įdiegtą Įrangą bei pateiktą dokumentaciją.	R		A
3. Sprendimo diegimas ir galutinis konfigūravimas				
3.1	Įdiegti ir pilna apimtimi sukonfigūruoti Detalioje architektūroje numatytą Sprendimą.		R	A
3.2	Parengti ir/arba atnaujinti bei suderinti įdiegto Sprendimo dokumentaciją.		R	A
3.3	Dalyvauti Sprendimo diegimo procese ir glaudžiai bendradarbiauti su Diegėju bei Perkančiąja organizacija, teikti visas būtinas konsultacijas pasiūlytos Įrangos konfigūravimo, komutavimo, eksploatavimo ir kitais klausimais.	R	A	
3.4	Įvertinti ar įdiegtas Sprendimas atitinka Detalioje architektūroje numatytą Sprendimą.			A
3.5	Atlikti Sprendimo veikimo testavimus pagal iš anksto suderintus testavimo scenarijus ir pateikti testų rezultatus popieriniu bei elektroniniu formatu pagal apibrėžtus standartus		R	A
3.6	Įvertinti, ar Sprendimo veikimo testavimai atlikti pagal patvirtintus testavimo scenarijus, apibrėžtus reikalavimus ir standartus.			R
3.7	Perduoti – priimti bandomajai eksploatacijai įdiegtą, sukonfigūruotą ir ištestuotą Sprendimą.		R	A
4. Bandomoji eksploatacija				
4.1	Vykdyti Sprendimo bandomąją eksploataciją pagal suderintą bandomosios eksploatacijos reglamentą. Fiksuoti klaidas, gedimus, trūkumus ir kt., informuoti apie pastebėtus neatitikimus.			R
4.2	Vykdyti Sprendimo bandomąją eksploataciją pagal suderintą bandomosios eksploatacijos reglamentą. Vykdyti techninės ir programinės Įrangos veikimo nuolatinį stebėjimą, fiksuoti klaidas, gedimus, trūkumus ir kt., informuoti apie pastebėtus neatitikimus.		R	A
4.3	Šalinti visas Sprendimo techninės ir programinės Įrangos veikimo klaidas, gedimus, trūkumus ir neatitikimus.		R	A
4.4	Teikti visas būtinas konsultacijas pasiūlytos Įrangos konfigūravimo, komutavimo, eksploatavimo ir kitais klausimais.	R	A	

Eil. nr.	Veiksmas	Įrangos tiekėjas	Diegėjas	Perkančioji organizacija
4.5	Vykdyti visus būtinus Sprendimo techninės ir programinės Įrangos atnaujinimus.		R	A
4.6	Konsultuoti Perkančiosios organizacijos atstovus įdiegto Sprendimo naudojimo, administravimo, konfigūravimo, priežiūros ir kitais klausimais.		R	A
4.7	Atnaujinti ir derinti įdiegto Sprendimo dokumentaciją.		R	A
4.8	Atlikti galutinius Sprendimo veikimo testavimus pagal iš anksto suderintus testavimo scenarijus.		R	A
4.9	Parengti ir suderinti bandomosios eksploatacijos rezultatus pagal bandomosios eksploatacijos reglamentą.		R	A
4.10	Perduoti – priimti gamybinei eksploatacijai pilnai įdiegtą, sukonfigūruotą ir ištestuotą Sprendimą.		R	A
5. Gamybinė eksploatacija ir garantinis aptarnavimas				
5.1	Naudoti Sprendimą gamybiniu režimu.			R
5.2	Teikti Įrangos garantinį aptarnavimą.	R		A
5.3	Teikti įdiegto Sprendimo ir Įrangos konfigūracijos garantinį aptarnavimą.		R	A

* - netaikoma programinės įrangos tiekėjams