PRIVILEGIJUOTŲ TEISIŲ VALDYMO (PAM) SPRENDIMO ĮSIGIJIMO IR DIEGIMO PASLAUGOS
TECHNINĖ SPECIFIKACIJA

Eil. Nr.	Pirkimo dokumentuose nustatyti prekių techniniai rodikliai
1.	**Bendrieji reikalavimai:**
1.1.	Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie siūlomos programinės įrangos gamybos arba tobulinimo nutraukimą (pvz., angl. end of life time arba Discontinued) ir kartu su pasiūlymu pateikti Programinės įrangos gamintojo patvirtinimą, kad įrangos gamintojas nėra paskelbęs apie siūlomos įsigyti įrangos gamybos arba tobulinimo nutraukimą (pvz., angl. „End of life time“ ar „Discontinued“).
1.2.	Programinės įrangos dokumentai turi būti lietuvių arba anglų kalba. Programinė įranga ir kompiuterių technikos sisteminiai pranešimai turi būti anglų arba lietuvių kalba. Gamintojo interneto svetainėje tvarkyklių ir dokumentų paieška turi būti pateikiama anglų arba lietuvių kalba.
1.3.	Tiekėjas turi pateikti nuorodą ar nuorodas į gamintojo interneto puslapį, kuriame yra tiksli pasiūlymą atitinkančios programinės įrangos techninė specifikacija. Jeigu sprendimui įgyvendinti reikalingas papildomas konfigūravimas, kuris nėra aprašytas techninėje dokumentacijoje, tiekėjas gali pateikti deklaraciją, patvirtinančią, kad šį sprendimą įgyvendins. Su papildomu konfigūravimu susijusios išlaidos turi būti Tiekėjo įvertintos ir įtraukti į pasiūlymo kainą.
1.4.	Perkančioji organizacija, vadovaudamasi VPĮ 37 straipsnio 8 ir 9 dalimi laikys, kad prekės ar paslaugos kelia grėsmę nacionaliniam saugumui, kai: - techninės ar programinės įrangos gamintojas ar jį kontroliuojantis asmuo yra registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose; - techninės ar programinės įrangos priežiūra ar palaikymas būtų vykdomas iš VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.
1.5.	Perkančioji organizacija, vadovaudamasi VPĮ 47 straipsnio 9 dalimi laikys, kad prekės ar paslaugos kelia grėsmę nacionaliniam saugumui, kai tiekėjas turi interesų, galinčių kelti grėsmę nacionaliniam saugumui, ir draudžia pirkime dalyvauti tiekėjams, jų subtiekėjams ar ūkio subjektams, kurių pajėgumais remiamasi, kurie patys ar juos kontroliuojantys asmenys yra registruoti (jeigu tiekėjas, jo subtiekėjas, ūkio subjektas, kurio pajėgumais remiamasi, ar kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose.
1.6.	Tiekėjas turi užtikrinti, kad palaikomoje techninėje ar programinėje įrangoje nėra įdiegtas įtartinas, šnipinėjantis ar kokia kita kenkėjiška veikla užsiimantis programinis kodas, kuri nėra būtinas įrangos funkcionalumui užtikrinti. Paaiškėjus, kad įrangoje yra įdiegta įtartina, šnipinėjimo ar kokia kita kenkimo programinė įranga, tai būtų traktuojama kaip Sutarties reikalavimų nesilaikymas. Tokiu atveju įranga grąžinama tiekėjui arba keičiama nauja lygiaverte ar geresnių parametrų, tačiau saugumo reikalavimus atitinkančia įranga.

1.7.	Sprendimas turi veikti debesijos pagrindu, užtikrinant visų funkcijų prieinamumą per interneto naršyklę be papildomos kliento programinės įrangos diegimo. Papildomi sprendimo komponentai gali būti diegiami Perkančiosios organizacijos infrastruktūroje, jei to reikalauja sprendimo architektūra ar integracijos poreikiai. Nuotoliniu būdu valdomoje įrangoje ar sistemose slaptažodžių valdymui neturi būti diegiami agentai.
1.8.	Į Sprendimo kainą turi būti įskaičiuota ne mažiau kaip 20 konsultavimo valandų eksploatavimo klausimais visu sutarties galiojimo laikotarpiu.
1.9.	Pagal Perkančiosios organizacijos poreikį Įrangos tiekėjas turės suteikti ne mažiau kaip žemiau išvardintus paslaugas:
1.9.1.	Atlikti sprendimo projektavimo darbus: suprojektuoti ir nubraižyti privilegijuotų paskyrų sprendimo pajungimo schemas, atitinkančias gerąsias gamintojo ir kibernetinio saugumo praktikas.
1.9.2.	Atlikti sprendimo pradinį konfigūravimą pagal suderintą projektavimo dokumentaciją ir pagal geriausias gamintojo ir kibernetinio saugumo praktikas.
1.9.3.	Atlikti trečių šalių prisijungimo sprendimo konfigūravimą.
1.9.4.	Atlikti sprendimo atnaujinimą į naujausią stabilią versiją.
1.9.5.	Sukonfigūruoti sistemos žurnalinių įrašų siuntimą į centralizuotą žurnalinių įrašų tarnybinę stotį.
1.9.6.	Atlikti techninės dokumentacijos ir administravimo vadovo parengimą – turi būti pateikta įdiegtos įrangos atliktų darbų techninė dokumentacija (pajungimo į tinklą schema, įdiegto sprendimo schemos, sistemos konfigūracijos ir taisyklių/profilių aprašymas bei kiti duomenys, reikalingi tolimesniam įrangos konfigūravimui ir eksploatavimui (IP adresai, valdymo programų vardai, prisijungimų vardai, slaptažodžiai ir pan.). Dokumentacija turi būti parengta lietuvių kalba ir pateikta elektroniniu formatu.
1.9.7.	Atlikti įrangos testavimą – pabaigus diegimo darbus Įrangos tiekėjas, kartu su Perkančiosios organizacijos atstovais, pagal iš anksto suderintus testavimo scenarijus, turės atlikti Įrangos veikimo testavimus (aukšto patikimumo, našumo savybių ir pan.) ir pateikti testų rezultatus elektroniniu formatu.
1.9.8.	Įdiegus sprendimą ir atlikus testavimą, suorganizuoti perkančiosios organizacijos darbuotojų (ne mažiau 4 darbuotojų) siūlomo Sprendimo administravimo ir naudojimo, ne trumpesnius nei 8 akademinių valandų mokymus. Visi mokesčiai, susiję su mokymais (pvz. mokymų kaina, transporto išlaidos, apgyvendinimo išlaidos ir kt.), turi būti įskaičiuoti į pasiūlymo kainą.
1.9.	Jeigu apibūdinant pirkimo objektą techninėje specifikacijoje ar kitose pirkimo dokumentuose galimai nurodytas konkretus modelis ar tiekimo šaltinis, konkretus procesas, būdingas konkretaus Įrangos tiekėjo tiekiamoms prekėms ar teikiamoms paslaugoms, ar prekių ženklas, patentas, tipai, konkreti kilmė ar gamyba, sertifikatai, standartai, protokolai, turi būti laikoma, kad kiekviena tokia nuoroda yra pateikta su žodžiais „arba lygiavertis“. Lygiavertiškumo įrodymas yra Įrangos tiekėjo pareiga.
2.	**Specialieji reikalavimai:**

2.1. Sistemos paskirtis	Sistema skirta privilegijuotų paskyrų (administratorių) valdymui, užtikrinanti naudotojų prisijungimų kontrolę prie resursų bei saugų slaptažodžių maskavimą ir valdymą. Sistema turi leisti ne mažiau kaip: - valdyti privilegijuotų naudotojų teises ir prieigas; - užtikrinti privilegijuotų naudotojų teisių stebėseną; - užtikrinti privačių SSH raktų saugumą; - užtikrinti saugią prieigą prie valdomų resursų; - valdyti trečiųjų šalių prieigą prie resursų; - užtikrinti privilegijuotų naudotojų veiksmų atsekamumą.
2.2. Sistemos suderinamumas	Sistema turi pilnai veikti debesijos paslaugų pagrindu ir užtikrinti vartotojų prieigą „VPN-less“ principu, t. y. be poreikio naudoti virtualaus privataus tinklo (VPN) ryšį.
2.3. Naudotojų autentifikavimas Sistemos web portale	Turi palaikyti lokalių naudotojų ir Microsoft Active Directory naudotojų prisijungimus į Sprendimo web portalą.
2.4. Naudotojų, valdomos įrangos, privačių raktų, sesijų skaičiai	Sistema turi leisti ja naudotis: - ne mažiau kaip 8 naudotojų (administratorių); - leisti naudoti ir stebėti ne mažiau kaip 10 aktyvių sesijų vienu metu; - ne mažiau kaip 1000 įrenginių; - ne mažiau 30000 privačių raktų / slaptažodžių. - Ne mažiau nei 10 valdomų sisteminių vartotojų (Windows OS ir Unix/Linux OS); - neribojamas politikų ir nustatymų skaičius.
2.5. Naudotojų valdymas	Sistema turi leisti valdyti naudotojų paskyras ne mažiau kaip nurodytose sistemose ar lygiaverčiose: - operacinėse sistemose: Windows, Linux; - duomenų bazėse: Microsoft SQL, Microsoft SQL Cluster Service, MySQL, PostgreSQL; - infrastruktūros valdymo sprendimuose: DELL iDRAC, HP iLO, Cisco CIMC; - tinklo (maršrutizatoriai, komutatoriai ir ugniasienės) ir saugos sprendimuose: Cisco, Juniper, HPE, PaloAlto, Fortinet; - moduliuose: Microsoft Services, Scheduled tasks, IIS application Pool, registries, Microsoft domain accounts; - direktorijose: Active Directory; - virtualios infrastruktūros sprendimuose: VMware vSphere, VMware ESXi, VMware vCenter Vmware Vcloud; - WEB aplikacijose.
2.6. Palaikomi protokolai	Sistema be papildomų modulių / licencijų turi palaikyti ne mažiau kaip šiuos protokolus: - SSH; - RDP; - HTTP/HTTPS
2.7. Valdymas	Sistema turi užtikrinti ne mažiau kaip šiuos reikalavimus:

	- visi siūlomi moduliai (jei siūloma Sistema sudaryta iš atskirų modulių) turi būti tarpusavyje suderinami; - visi sistemos komponentai turi būti prijungti prie Sistemos centralizuoto valdymo; - sistema turi leisti naudoti specializuotus (t. y. programiškai aprašytus) vykdomuosius automatizacijos scenarijus (angl. scripts) nestandartiniams prisijungimams valdyti.
2.8. Sistemos patikimumas	Sistema turi užtikrinti ne mažiau kaip šiuos reikalavimus: - Tiekėjas privalo užtikrinti, kad siūlomas debesijos (cloud-based) PAM sprendimas veiktų aukšto pasiekiamumo (High Availability, HA) architektūroje, kuri garantuoja nenutrūkstamą paslaugos veikimą ir duomenų prieinamumą; - Tiekėjas privalo naudoti sertifikuotą ir patikimą debesijos infrastruktūrą , užtikrinančią SLA ne mažesnį kaip 99,9 % paslaugos pasiekiamumą; - Duomenų centrai turi būti geografiškai paskirstyti (multi-zone arba multi-region) siekiant užtikrinti atsparumą infrastruktūros sutrikimams; - PAM sprendimas turi turėti aukšto pasiekiamumo (HA) mechanizmus, įskaitant automatinį apkrovos balansavimą, paslaugų replikaciją ir automatinį atsistatymą po gedimo (failover); - Tiekėjas turi pateikti visas reikalingas licencijas siūlomam HA funkcionalumui užtikrinti ir jos turi galioti visą garantinį laikotarpį.
2.9. Sistemos saugumas	Siūloma Sistema turi užtikrinti ne mažiau kaip: - turi būti suderinama su ne mažiau kaip šiuo autentifikacijos sprendimu: LDAP; - turi būti kelių faktorių autentifikavimas (angl. MFA). Funkcionalumas turi leisti integruoti su trečių šalių MFA sprendimais, kurie veikia naudodami nuo laiko priklausomus vienkartinius slaptažodžius (angl. time based onetime password). Aparatinio autentifikavimo FIDO2 palaikymas; - komunikacijos tarp sistemos komponentų turi būti atliekamos šifruotais ryšio kanalais; - turi būti galimybė slėpti privilegijuotų naudotojų valdomų paskyrų slaptažodžius; - turi leisti naudotojui prisijungti prie valdomų paskyrų nepateikiant slaptažodžio; - turi užtikrinti saugumą: slaptažodžiams, įrašytoms sesijoms, audito pranešimams ir t.t.; - turi panaikinti naudotojo sesiją į Sistemos web portalą po nustatyto neaktyvumo laiko; - turi būti galima nurodyti iš kokių IP adresų galima jungtis prie slaptažodžių spintos (Vault); - turi gebėti aptikti kenksmingus veiksmus ir atakas susijusias su privilegijuotomis paskyromis.
2.10. Integracijos	Siūloma Sistema turi integruotis su ne mažiau kaip:

	- LDAP / Active Directory direktorijomis privilegijuotų naudotojų teisių priskyrimui bei pakeitimui; - turi leisti naudoti aplikacijų programines sąsajas (API); - API turi palaikyti pagrindines programavimo kalbas .NET, JAVA arba lygiavertes; - API turi būti apsaugotas SSL/TLS; - turi būti integruojamas su SSO (angl. single sign on) sistemomis; - turi siųsti el. pašto pranešimus; - turi integruotis su HSM; - turi palaikyti integraciją su IT užklausų valdymo sistema (angl. ITSM).
2.11. Ataskaitos ir auditas	Siūloma Sistema turi užtikrinti ne mažiau kaip: - turi pateikti paskyras, naudotas prisijungimams nurodytu laiko intervalu; - turi turėti galimybę pateikti paskyrų panaudojimo ir stebėsenos duomenis; - turi gebėti generuoti ataskaitas nurodytais laiko intervalais ar pagal pageidavimą; - turi leisti suformuoti šias ataskaitas: • prieigos ataskaitą, • privilegijuotų naudotojų veiksmų ataskaitą, • privilegijuotų paskyrų suvestinę ataskaitą, • valdomų aplikacijų suvestinę ataskaitą; - turi leisti sugeneruoti ataskaitas bent csv formatu; - turi leisti generuoti atskaitas apie prieigą prie valdomų sistemų; - turi leisti sugeneruoti ataskaitas apie prieigos prašymus; - turi leisti sugeneruoti atskaitas apie nesėkmingas slaptažodžių užklausas ir nesėkmingus prisijungimus; - audito informaciją turi būti galima eksportuoti į išorines sistemas ataskaitų generavimui ir analizei; - turi leisti siųsti ataskaitas arba nuorodas į jas el. paštu.
2.12. Slaptažodžių prieigos	- Siūlomo sprendimo administravimas turi turėti aiškiai išskirtas teises, kurios leistų realizuoti - „keturių akių“ administravimo principą - vienas naudotojas suteikia super-administratoriaus teises, kitas tomis teisėmis pasinaudoja; - Sistema turi leisti privilegijuotam naudotojui užsakyti prieigą vėlesniam laikui; - Sistema turi audituoti kiekvieną slaptažodžio užklausą ir prieigos suteikimą;
2.13. Prisijungimo duomenų valdymas	Siūloma Sistema turi užtikrinti ne mažiau kaip šiuos funkcionalumus: - turi neleisti naudoti prieš tai buvusių slaptažodžių; - turi leisti naudoti keletą MS AD ar LDAP autentifikacijos valdymo sprendimų vienu metu; - turi leisti siųsti el. laiškus apie veiksmus su paskyromis;

	- turi užtikrinti unifikuotą prieigą prie nutolusių sistemų, neatskleidžiant prisijungimo duomenų privilegijuotam naudotojui, bent dviem būdais: • iš naudotojo kompiuterio per įgaliotąjį serverį (angl. proxy/jumphost) į sprendimo valdomą sistemą. - turi turėti funkcionalumą leidžiantį sugeneruoti ir patikrinti slaptažodžius pagal iš anksto nustatytas taisykles; - turi leisti periodiškai keisti valdomų įrenginių paskyrų (angl. account) slaptažodžius; - turi leisti pakeisti valdomų įrenginių paskyrų slaptažodį po panaudojimo; - turi identifikuoti privilegijuotas paskyras (pvz. administrator, root ir pan.) nurodytuose įrenginiuose; - turi leisti saugoti valdomų paskyrų slaptažodžių istoriją; - turi turėti funkcionalumą, leidžiantį įkelti valdomų įrenginių paskyrų sąrašą iš struktūrizuotos bylos; - turi turėti funkcionalumą valdomai paskyrai nurodyti viršesnę paskyrą, leidžiančią atstatyti slaptažodžius net jei valdoma paskyra yra blokuota ar slaptažodžiai nesutampa; - turi rinkti audito informaciją: • valdomose sistemose atliktus veiksmus, • paskyrų pakeitimus, • slaptažodžių panaudojimą, • slaptažodžių užklausas ir patvirtinimus, atmetimus.
2.14. Saugus trečių šalių valdymas	Siūloma Sistema turi užtikrinti ne mažiau kaip šiuos trečių šalių valdymo funkcionalumus: - ne mažiau nei 20 (dvidešimt) trečiųjų šalių licencijų, užtikrinant bent 3 (trijų) iš jų prisijungimą prie nutolusių sistemų vienu metu nenaudojant VPN sprendimo (VPN-less). Turi būti sprendimo plėtimo galimybė įsigyjant papildomas licencijas; - turi būti suteikta prisijungimų valdymo grafinė sąsaja veikianti žiniatinklio priemonėmis ir nereikalaujanti atskiro VPN; - neturi reikėti diegti papildomos programinės įrangos kompiuteryje, išskyrus interneto naršyklę (sprendimas turi palaikyti ne mažiau kaip šias naršykles: Google Chrome, Microsoft Edge, Mozilla Firefox). - trečioms šalims turi būti galimybė matyti apsaugotus išteklius, prie kurių suteikta teisė prisijungti; - sprendimas turi būti pagrįstas viešosios debesijos pagrindu (angl. SaaS); - ryšys tarp trečios šalies, perkančiosios organizacijos ir viešosios debesijos sprendimo turi būti perduodamas saugiais šifruotais kanalais; - turi būti galimybė generuoti ir siųsti kvietimus dėl prisijungimo prie sprendimo trečių šalių tiekėjams el. pašto pranešimais; - turi būti galimybė riboti prisijungimo prieigas laike;

	- jeigu galutinio ištekliaus techninės galimybės leidžia, turi būti galimybė slėpti prisijungimo prie apsaugoto ištekliaus prisijungimo slaptažodį; - sprendimas turi suteikti REST API sąsają vartotojų valdymo proceso automatizavimui.
2.15. Stebėsena ir kontrolė	Siūloma Sistema turi užtikrinti ne mažiau kaip šiuos funkcionalumus: - turi veikti kaip tarpinis taškas (angl. jump, proxy) prisijungimams prie valdomų sistemų; - turi veikti be papildomų agentų diegimo stebimose sistemose; - turi gebėti įrašyti veiksmus, vykdomus šiose sistemose: • Windows, • UNIX/Linux, maršrutizatoriuose ir komutatoriuose, • duomenų bazėse, • Perkančiosios organizacijos naudojamuose virtualizacijos platformų valdymo sprendimuose (VMware), • domeno valdikliuose. - stebėsena neturi paveikti valdomos sistemos greitaveikos; - turi būti galimybė stebėti valdomas sistemas nereikalaujant tinklo struktūros pakeitimų; - turi gebėti saugoti stebėsenos įrašus saugiame, šifruotame formate ir užtikrinti įrašų integralumą; - turi turėti detaliai pasirenkamą stebėsenos ir kontrolės audito mechanizmą ir sukauptų duomenų peržiūrą; - turi leisti atlikti vykdytų komandų paiešką įrašytose sesijose; - turi gebėti atvaizduoti įrašytas sesijas; - turi leisti matyti realiu laiku vykstančias sesijas ir jas nutraukti; - turi gebėti persiųsti detalią informaciją į SIEM sprendimus; - turi gebėti suspausti įrašus ilgalaikiam saugojimui; - turi išsaugoti visus naudotojo mygtukų paspaudimus; - turi būti funkcionalumas leidžiantis HTTP/HTTPS sesijas apsaugoti nuo prisijungimo duomenų patekimo į administratoriaus darbo vietą; - turi leisti privilegijuotiems naudotojams pasiekti valdomas sistemas šiais įrankiais: • aplikacija, gebančia komunikuoti MS RDP protokolu, • aplikacija, gebančia komunikuoti SSH protokolu.
2.16. Unix / Linux komandų valdymas	Siūloma Sistema turi užtikrinti ne mažiau kaip šiuos funkcionalumus: - turi leisti nurodyti, kokias komandas privilegijuoti naudotojai gali vykdyti Unix/Linux tipo sistemose; - turi leisti kontroliuoti naudojamas SSH komandas naudojant „baltuosius“ ir „juoduosius“ sąrašus; - turi leisti įrašyti visas CLI vykdytas komandas; - turi leisti įrašyti visą įvesties ir išvesties tekstą CLI sąsajoje.

2.17. SSH raktų valdymas	- Sistema turi leisti saugoti privačius SSH raktus apsaugotoje saugykloje; - Sistema turi leisti užtikrinti tokio lygio privačių SSH raktų apsaugą, kokia yra taikoma slaptažodžiams.
2.18. Microsoft Windows operacinių sistemų valdymas	Siūloma Sistema turi užtikrinti ne mažiau kaip šiuos funkcionalumus: - turi leisti kontroliuoti sistemas, neįtrauktas į domeną; - turi leisti fiksuoti naudotojų veiksmus stebimose Microsoft Windows aplikacijose; - turi leisti kontroliuoti lokalias administratorių paskyras.
2.19. Sesijos neaktyvumas	Siūloma Sistema turi užtikrinti ne mažiau kaip šiuos funkcionalumus: - turi panaikinti naudotojo sesiją į web portalą po nustatyto neaktyvumo laiko;
2.20. Grafinė sąsaja	Sistema turi turėti ne mažiau kaip: - grafinę naudotojų sąsają, pasiekiamą saugiu HTTPS protokolu interneto naršykle ir nereikalauti nesaugių trečių šalių technologijų, tokių kaip Flash, ActiveX ar JAVA.
2.21. Garantiniai įsipareigojimai, techninis aptarnavimas	Turi būti pateiktas 12 mėn. prenumeratos tipo (angl. subscription) sprendimas su ne mažiau kaip 12 mėnesių gamintojo užtikrinta garantija (pradedant skaičiuoti nuo licencijų aktyvavimo dienos). Garantijos metu turi būti nemokamai šalinami sprendimo gedimai, pateikiami programinės įrangos atnaujinimai (naujos versijos, klaidų pataisymai ir pan.) bei teikiama pagalba sprendžiant siūlomos programinės įrangos sutrikimus. Garantiniu laikotarpiu turi galioti visos licencijos ir jų užtikrinami funkcionalumai.
	Pirkėjui turi būti suteikta prieiga prie programinės įrangos kūrėjo/gamintojo klientų puslapio, kuriame galima rasti atsakymus į dažniausiai iškylančių Sistemos naudojimo klausimų duomenų bazę.
	Tiekėjas arba gamintojas visą sutarties laikotarpį privalo užtikrinti techninės pagalbos teikimą internetu, telefonu ir elektroniniu paštu darbo dienomis darbo valandomis (8x5 paslaugų teikimo režimu), be papildomo apmokestinimo.
2.22. Kvalifikaciniai rekalavimai	Tiekėjas turi atitikti: - Tiekėjas turi turėti privilegijuotų teisių valdymo (PAM) diegimo specialistą, kuris per pastaruosius 3 metus yra įgyvendinęs bent vieną PAM projektą, kurio vertė buvo ne mažesnė kaip 15 000,00 EUR be PVM. - Tiekėjas turi turėti sertifikuotą projektų vadovą, kuris per pastaruosius 3 metus vadovavo bent vienam privilegijuotų teisių valdymo diegimo projektui, kurio vertė buvo ne mažesnė kaip 15 000,00 EUR be PVM.