

AUTENTIFIKACIJOS SPRENDIMO LICENCIJŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

1. Pirkimo tikslas – įsigyti **Keleto faktorių autentifikacijos sprendimo licencijas** su 36 mėn. gamintojo palaikymu.
2. Licencijos turi atitikti 1 lentelėje numatytus reikalavimus.
3. Tiekėjai, teikdami pasiūlymus, turi užpildyti siūlomų licencijų atitikimą reikalavimams 1 lentelės stulpelyje *Siūloma charakteristika*.
4. Licencijų tiekėjas turi būti siūlomų licencijų gamintojo atstovas, įgaliotas pateikti (parduoti), siūlomas licencijas arba turi būti sudaręs sutartį su tokiu atstovu, turinčiu išvardintas teises. Pasiūlyme turi būti pateiktos licencijų gamintojo pažymos, patvirtinančios, kad tiekėjas yra siūlomų licencijų gamintojo atstovas, įgaliotas pateikti (parduoti) siūlomas licencijas arba turi būti sudaręs sutartį su tokiu atstovu, turinčiu išvardintas teises (turi būti pateikta skaitmeninė kopija).

1 lentelė. Keleto faktorių autentifikacijos sprendimo licencijos – 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.	Fortinet FortiAuthenticator licencijos ir FortiCare kontraktai: FAC-VM-100-UG – 12 vnt. FortiAuthenticator-VM 100 users license upgrade FC2-10-0ACVM-248-02-36 – 2 vnt. FortiAuthenticator - VM License 3 Year 24x7 FortiCare Contract (1 - 1100 USERS) Fortinet FortiToken licencijos: FTM-ELIC-100 – 6 vnt. Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 100 users. FTM-ELIC-50 – 2 vnt. Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 50 users. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf

			https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortitoken.pdf
2.	Sprendimo architektūra	Sprendimas turi būti suderinamas su VMware virtualia perkančiosios organizacijos infrastruktūra. Turi būti pateikta visa (pagal gamintojo rekomendacijas) programinė įranga ir visos licencijos, reikalingos šioje lentelėje įvardintam funkcionalumui ir jo palaikymui užtikrinti.	Sprendimas suderinamas su VMware virtualia perkančiosios organizacijos infrastruktūra. Pateikiama visa (pagal gamintojo rekomendacijas) programinė įranga ir visos licencijos, reikalingos šioje lentelėje įvardintam funkcionalumui ir jo palaikymui užtikrinti.
3.	Suderinamumas	Siūlomas sprendimas turi būti pilnai suderinamas su perkančiosios organizacijos šiuo metu naudojamomis Fortinet FortiAuthenticator ir FortiToken sistemomis, integruotis į šiuo metu naudojamas išvardintas Fortinet sistemas bei išplėsti naudojamų licencijų kiekį.	Siūlomas sprendimas pilnai suderinamas su perkančiosios organizacijos šiuo metu naudojamomis Fortinet FortiAuthenticator ir FortiToken sistemomis, integruosis į šiuo metu naudojamas išvardintas Fortinet sistemas bei išplės naudojamų licencijų kiekį.
4.	Funkcionalumas	Siūlomas sprendimas turi užtikrinti ne mažiau kaip šiuos funkcionalumus: 1. Turi veikti kaip dviejų faktorių naudotojų tapatybės nustatymo serverio Fortinet FortiAuthenticator plėtinys; 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;	Siūlomas sprendimas užtikrina šiuos funkcionalumus: 1. Veiks kaip dviejų faktorių naudotojų tapatybės nustatymo serverio Fortinet FortiAuthenticator plėtinys; 2. Integruosis su įvairiomis IT sistemomis, siekiant pakeisti tapatybės nustatymą statinių slaptažodžių pagalba į tapatybės nustatymą vienkartinių slaptažodžių pagalba; 3. Turi integruotą duomenų bazę; 4. Veiks kaip RADIUS serveris; 5. RADIUS serveris palaiko: • 802.1X, • EAP; 6. Valdymas realizuotas per HTTPS sprendimą; 7. Leidžia naudoti kelių lygių administratorius,

		7. Turi leisti naudoti kelių lygių administratorius, turinčius skirtingas teises.	turinčius skirtingas teises.
5.	Naudotojų, kodų generatorių kiekis	Siūlomas sprendimas: 1. Turi leisti dirbti ne mažiau kaip 1200 naudotojų, išskaidant šiuos naudotojus į dvi sistemas, kurių kiekvienoje būtų po 600 naudotojų; 2. Turi būti galimybė, esant poreikiui, plėsti iki ne mažiau kaip 3000 naudotojų. 3. Turi būti pateikta ne mažiau kaip 700 vnt. vienkartinių kodų generatorių (programinių), kurių galiojimo trukmė būtų ne mažesnė kaip 36 mėn. Kodų generatoriai turi veikti savarankiškai be papildomų perdavimo terpių kaip internetas/GSM. 4. Vienkartinius kodų generatorius (programinius) turi būti leidžiama išskaidyti į 6 sistemas po 100 vnt. programinių kodų generatorių ir 2 sistemas po 50 vnt. programinių kodų generatorių.	Siūlomas sprendimas: 1. Leis dirbti 1200 naudotojų, išskaidant šiuos naudotojus į dvi sistemas, kurių kiekvienoje būtų po 600 naudotojų; 2. Galimybė, esant poreikiui, plėsti iki 3000 naudotojų. 3. Pateikiama 700 vnt. vienkartinių kodų generatorių (programinių), kurių galiojimo trukmė 36 mėn. Kodų generatoriai veikia savarankiškai be papildomų perdavimo terpių kaip internetas/GSM. 4. Vienkartinius kodų generatorius (programinius) leidžiama išskaidyti į 6 sistemas po 100 vnt. programinių kodų generatorių ir 2 sistemas po 50 vnt. programinių kodų generatorių.
6.	Sprendimo patikimumas	Naudojamas ir plečiamas sprendimas turi veikti aukšto patikimumo (angl. HA) konfigūracijoje, kuri užtikrintų nepertraukiamą sistemos veikimą dviejuose duomenų centruose. HA funkcionalumas turi būti užtikrintas sistemos funkcionalu, o ne platformos ar trečių šalių sprendimais. Naudojama ir plečiama sistema turi palaikyti ne mažiau kaip šias aukšto patikimumo funkcijas: • Sutrikus pagrindinio įrenginio darbui, sistema automatiškai persijungia į žemesnį prioritetą turintį įrenginį;	Naudojamas ir plečiamas sprendimas veikia aukšto patikimumo (angl. HA) konfigūracijoje, kuri užtikrina nepertraukiamą sistemos veikimą dviejuose duomenų centruose. HA funkcionalumas užtikrintas sistemos funkcionalu, o ne platformos ar trečių šalių sprendimais. Naudojama ir plečiama sistema palaiko 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.	• Konfigūracija tarp įrenginių sinchronizuojama; • Prievadų stebėjimas; • Įrenginių susijungimui į aukšto patikimumo sistemą naudojamas slaptažodis ar lygiavertė saugumo priemonė užtikrinanti, kad į telkinį susijungtų tik numatytieji įrenginiai Tarp aukšto patikimumo konfigūracijoje naudojamų virtualių įrenginių automatiškai sinchronizuojama ši informacija: • informacija apie kodų generatorius; • informacija apie naudotojus; informacija apie naudotojų susiejimą su kodų generatoriais.
7.	Vienkartiniai kodų generatoriai	Naudojamas ir plečiamas sprendimas turi palaikyti ne mažiau kaip: 1. Aparatinius vienkartinių kodų generatorius. Šie kodų generatoriai turi veikti 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	Naudojamas ir plečiamas sprendimas palaiko: 1. Aparatinius vienkartinių kodų generatorius. Šie kodų generatoriai veikia 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 nurodytos operacinės sistemos: - Windows OS, - iOS, - Android. 3. Programiniai vienkartiniai kodų generatoriai veikia be jokio išorinio ryšio t. y. be interneto/GSM ar panašių perdavimo terpių;

		jokio išorinio ryšio t. y. be interneto/GSM ar panašių perdavimo terpių; 4. Leisti nustatyti, kad programinis vienkartinį kodų generatorius būtų naudojamas su PIN kodu; 5. Leisti nustatyti koks turi būti programinio vienkartinio kodų generatoriaus PIN kodo ilgis.	4. Leis nustatyti, kad programinis vienkartinį kodų generatorius būtų naudojamas su PIN kodu; 5. Leis nustatyti koks turi būti programinio vienkartinio kodų generatoriaus PIN kodo ilgis.
8.	Naudotojų savitarna	Naudojamas ir plečiamas sprendimas turi užtikrinti ne mažiau kaip šiuos funkcionalumus: 1. Turi būti savitarnos portalas, kuris vienkartinį kodų generatorių naudotojams naršyklės pagalba leistų atlikti ne mažiau kaip šiuos veiksmus, susijusius su vienkartinį kodų generatoriumi: • užpildyti prašymą gauti naują generatorių; • pranešti apie prarastą generatorių; • generatoriaus sinchronizavimas. 2. Turi leisti jungtis prie savitarnos portalo nenaudojant vienkartinį kodų generatoriaus.	Naudojamas ir plečiamas sprendimas užtikrina šiuos funkcionalumus: 1. Savitarnos portalas, kuris vienkartinį kodų generatorių naudotojams naršyklės pagalba leis atlikti šiuos veiksmus, susijusius su vienkartinį kodų generatoriumi: • užpildyti prašymą gauti naują generatorių; • pranešti apie prarastą generatorių; • generatoriaus sinchronizavimas. 2. Leis jungtis prie savitarnos portalo nenaudojant vienkartinį kodų generatoriaus.
9.	Integracijos	Naudojamas ir plečiamas sprendimas 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.	Naudojamas ir plečiamas sprendimas užtikrina integracijas 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.

10.	Ataskaitos ir auditas	Naudojamas ir plečiamas sprendimas 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.	Naudojamas ir plečiamas sprendimas užtikrina šiuos funkcionalumus: 1. Leis kaupti informaciją apie administratorių ir naudotojų atliekamus veiksmus, tapatybės nustatymo proceso įvykius; 2. Leis generuoti ataskaitas.
11.	Garantiniai įsipareigojimai, techninis aptarnavimas.	Visiems pateiktiems techniniams ir programiniams komponentams turi būti taikoma ne mažiau kaip 3 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 autorizoto 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	Visiems pateiktiems techniniams ir programiniams komponentams taikoma 3 metų (24 valandos per parą 7 dienos per savaitę 365 dienos per metus) gamintojo užtikrinta garantinė priežiūra įrangos eksploatavimo vietoje (pateikiami papildomi gamintojo serviso paketai, nurodomi pasiūlyme jų kodai ir pavadinimai). Garantinė priežiūra atliekama paties įrangos gamintojo arba jo autorizoto aptarnavimo atstovo. Garantiniu laikotarpiu teikiamas nemokamas garantinis aptarnavimas bei atnaujinimų teikimas (visą garantinį laikotarpį įranga leis naudoti visus šioje lentelėje įvardintus funkcionalumus). Perkančiajai organizacijai bus suteikta teisė kreiptis į gamintoją iškilus problemai (paslaugos tipas 24x7) internetu, elektroniniu paštu arba telefonu. Bus užtikrinta prieiga prie gamintojo internetiniame puslapyje esančių resursų, tarp jų ir programinės įrangos bibliotekų. Tiekėjas pateiks nuorodą į gamintojo internetinę prieigą, kuri įgalina naudojant produkto kodą ir/arba serijinį numerį patikrinti suteiktą gamintojo garantiją internetiniame puslapyje.

		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.	
--	--	--	--
