Dokumentų valdymo bendrojoje informacinėje sistemoje esamos LT ID integracijos pagrindu teikiamų asmens tapatybės nustatymo, kvalifikuoto elektroninio parašo ir elektroninio spaudo transakcijų paslaugų pirkimas (PPR-339)

I. BENDROJI INFORMACIJA

1. **Pirkėjas** – Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos.
2. **Pirkimo objektas** – esamos Dokumentų valdymo bendrosios informacinės sistemos (toliau – DBSIS) integracijos su LT ID infrastruktūrą pagrindu teikiamos fizinių asmenų autentifikavimo, nuotolinio kvalifikuoto elektroninio parašo ir kvalifikuoto elektroninio spaudo transakcijų paslaugos (toliau – Paslaugos), skirtos DBSIS naudotojų autentifikavimui ir ADOC-V1.0, PDF ir ASiC-E elektroninių dokumentų pasirašymui arba tvirtinimui.
3. DBSIS yra sukurta ir įdiegta integracinė sąsaja su valstybės įmonės Registrų centro valdoma LT ID infrastruktūra, kuriai naudoti būtina įsigyti Techninės specifikacijos 2 p. nurodytas Paslaugas. DBSIS ir LT ID infrastruktūros integracinė sąsaja yra realizuota vadovaujantis LT ID identifikavimo ir pasirašymo paslaugos serviso vadovu (nuoroda į dokumentą: https://ltid.lt/site_media/2025/04/LT-ID-identifikavimo-ir-pasirasymo-paslauga-v1.4.pdf).
4. Paslaugos turi būti teikiamos naudojant esamą DBSIS ir LT ID infrastruktūros integracinę sąsają, nereikalaujant papildomo DBSIS programinės įrangos pakeitimo, išskyrus būtinus konfigūravimo veiksmus.
5. Šiuo pirkimu nėra siekiama įsigyti naujos DBSIS integracinės sąsajos sukūrimo, esamos integracinės sąsajos keitimo ar DBSIS adaptavimo skirtingų kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų (toliau – Tiekėjai) infrastruktūroms paslaugų. Alternatyvių sprendimų integravimas, reikalaujantis esamos DBSIS architektūros ar integracinių komponentų keitimo, nėra šio pirkimo objektas, nes tai galėtų lemti papildomus techninius, saugumo ir finansinius kaštus bei veiklos tęstinumo rizikas.
6. **Pirkimo tikslas** – užtikrinti nepertraukiamą DBSIS naudotojų autentifikavimo, kvalifikuoto elektroninio parašo ir kvalifikuoto elektroninio spaudo paslaugų teikimą, išlaikant esamą DBSIS integracinę sąsają su patikimumo užtikrinimo paslaugų infrastruktūra.

II. NACIONALINIO SAUGUMO REIKALAVIMAI

7. Pirkimo objektui taikomi Lietuvos Respublikos viešųjų pirkimų įstatymo (toliau – VPĮ) 37 straipsnio 8 dalies reikalavimai, susiję su nacionaliniu saugumu: Pirkėjas, veikiantis srityse, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, ar valdantis ypatingos svarbos informacinę infrastruktūrą, reikalauja, kad Tiekėjo siūlomos Paslaugos nekeltų grėsmės nacionaliniam saugumui, kai sandorio pagrindu susidarytų aplinkybės, nurodytos Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 13 straipsnio 4 dalies 1 punkte.

   Laikoma, kad Tiekėjo siūlomos Paslaugos kelia grėsmę nacionaliniam saugumui, kai Lietuvos Respublikos Vyriausybė yra priėmusi sprendimą, patvirtinantį, kad ketinamas sudaryti sandoris neatitinka nacionalinio saugumo interesų vadovaujantis Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu, ir Tiekėjo pasiūlymas atmetamas.

   Vertinimas atliekamas iki pasiūlymų eilės nustatymo kreipiantis į kompetentingas institucijas dėl ekonomiškai naudingiausią pasiūlymą pateikusio Tiekėjo, įvertinus jo pasiūlymą, atitiktį pašalinimo pagrindams, kvalifikacijos reikalavimams bei VPĮ 37 straipsnio 9 dalies reikalavimams, susijusiems su nacionaliniu saugumu.

8. Pirkimo objektui taikomi VPĮ 37 straipsnio 9 dalies reikalavimai, susiję su nacionaliniu saugumu*: Tiekėjas privalo įrodyti, kad siūlomos paslaugos nekelia grėsmės nacionaliniam saugumui – paslaugų teikimas nėra vykdomas iš VPĮ 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.

   Pirkėjas pasiūlymo atitikčiai VPĮ 37 straipsnio 9 dalies reikalavimams patvirtinti **iš Tiekėjo reikalauja KARTU SU PASIŪLYMU PATEIKTI** užpildytą pirkimo dokumentą „Nacionalinio saugumo reikalavimų atitikties deklaracija“ (8 IA PD ATITIKTIES DEKLARACIJA)**, o iš ekonomiškai naudingiausią pasiūlymą pateikusio Tiekėjo reikalaus pateikti** (kartu su pasiūlymu šių dokumentų Tiekėjas pateikti neturi) – vieną ar kelis šiuos dokumentus**: juridinio asmens vadovo patvirtintą juridinio asmens steigimo dokumentų kopiją, Juridinių

asmenų registro išplėstinį išrašą su istorija, Juridinių asmenų dalyvių informacinės sistemos išrašą, asmens tapatybę patvirtinančio dokumento (tapatybės kortelės ar paso) kopiją, leidimo verstis atitinkama ūkine veikla patvirtinančio dokumento (pavyzdžiui, verslo liudijimo, individualios veiklos pažymėjimo ir pan.) kopiją, pažymą apie deklaruotą gyvenamąją vietą arba atitinkamus valstybės narės ar trečiosios šalies dokumentus, ar kitus Pirkėjui priimtinus dokumentus.

Pastabos:

**Jeigu Teikėjas ar jį kontroliuojantis asmuo yra nacionaliniam saugumui užtikrinti svarbi įmonė, valstybės įmonė, savivaldybės įmonė, taip pat valstybės valdoma bendrovė ir jų dukterinės bendrovės, išvardytos Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme, šiems subjektams aukščiau nurodytas reikalavimas (VPĮ 37 straipsnio 9 dalis) yra netaikomas.*

***Dokumentai, kuriuose nenurodytas jų galiojimo terminas, turi būti išduoti ar atspausdinti iš informacinės sistemos ne anksčiau kaip likus 3 (trims) mėnesiams iki tos dienos, kurią Pirkėjo prašymu Tiekėjas turi pateikti dokumentus.*

III. SĄVOKOS

9. Šioje techninėje specifikacijoje vartojamos sąvokos:

9.1. **LT ID infrastruktūra** – Registrų centro valdoma nuotolinio kvalifikuoto elektroninio parašo, spaudo ir autentifikavimo infrastruktūra.

9.2. **LT ID žiniatinklio paslaugos** – programinių sąsajų ir protokolų rinkinys, skirtas DBSIS integracijai su LT ID infrastruktūra, vykdant naudotojų autentifikavimo ir elektroninių dokumentų pasirašymo operacijas.

9.3. **LT ID aplikacija** – mobiliesiems iOS ir Android įrenginiams pritaikyta aplikacija, skirta naudotojų DBSIS inicijuotų autentifikavimo ir elektroninių dokumentų pasirašymo transakcijų patvirtinimui, aktyvuojant LT ID infrastruktūroje saugomus kvalifikuoto elektroninio parašo arba spaudo sertifikatus.

9.4. **LT ID parašas –** nuotolinė kvalifikuotos elektroninės atpažinties ir elektroninio parašo paslauga, skirtą fizinių asmenų tapatybės nustatymui (autentifikavimui) elektroninėje erdvėje ir elektroninių dokumentų pasirašymui kvalifikuotu elektroniniu parašu.

9.5. **LT ID spaudas** – nuotolinė kvalifikuoto elektroninio spaudo paslauga, skirta juridinio asmens vardu tvirtinti elektroninius dokumentus užtikrinant jų kilmę ir vientisumą naudojant kvalifikuotą elektroninio spaudo sertifikatą.

9.6. **Paketinis pasirašymas** – LT ID infrastruktūros funkcionalumas, leidžiantis vienos transakcijos metu perduoti pasirašymui daugiau nei vieną DBSIS sugeneruotą elektroninio dokumento santrauką (angl. *hash*).

9.7. **Transakcija** - paslaugos apskaitos vienetas – viena sistemos API užklausa, nepriklausomai nuo jos paskirties (autentifikavimo, kvalifikuoto elektroninio parašo ar kvalifikuoto elektroninio spaudo inicijavimo), vykdoma per tą pačią DBSIS integracinę sąsają su LT ID infrastruktūra.

IV. FUNKCINIAI IR TECHNINIAI REIKALAVIMAI

10. Perkamos Paslaugos turi būti suderinamos su esama DBSIS integracija su LT ID infrastruktūra ir nereikalauti DBSIS programinių pakeitimų, išskyrus konfigūravimą, užtikrinant šias funkcijas:

10.1. naudotojų autentifikavimą;

10.2. nuotolinio kvalifikuoto elektroninio parašo ir kvalifikuoto elektroninio spaudo operacijų inicijavimą ir valdymą;

10.3. elektroninių dokumentų pasirašymą ADOC, PDF ir ASiC-E formatais;

10.4. dokumentų tvirtinimą kvalifikuotu elektroniniu spaudu.

11. DBSIS naudotojai turi turėti galimybę inicijuoti naudotojų autentifikavimo, elektroninių dokumentų pasirašymo ir elektroninių dokumentų tvirtinimo kvalifikuotu elektroniniu spaudu transakcijas per LT ID žiniatinklio paslaugas.

12. DBSIS generuoja pasirašomų elektroninių dokumentų santraukas (hash), kurios perduodamos LT ID infrastruktūrai kvalifikuoto elektroninio parašo arba kvalifikuoto elektroninio spaudo sukūrimui.

13. LT ID žiniatinklio paslaugos turi:

13.1. palaikyti naudotojų autentifikaciją, elektroninį parašą ir elektroninį spaudą;

13.2. palaikyti paketinio elektroninių dokumentų pasirašymo funkcionalumą, leidžiantį vienos transakcijos metu perduoti iki 25 (dvidešimt penkių) DBSIS sugeneruotų elektroninių dokumentų duomenų santraukų (angl. *hash*) pasirašymui;

13.3. užtikrinti saugų HTTPS duomenų perdavimą;

13.4. palaikyti SHA-256, SHA-384 ir SHA-512 algoritmus dokumentų santraukoms kurti;

13.5. veikti naudojant REST architektūros stilių arba SOAP protokolą;

13.6. grąžinti klaidas naudojant standartinius HTTP protokolo kodus.

14. LT ID aplikacijoje turi būti sudaryta galimybė:

14.1. rodyti ir konfigūruoti autentifikavimo ir pasirašymo užklausų pranešimus;

14.2. rodyti DBSIS pavadinimą;

14.3. pateikti naudotojui aiškią sesijos ir operacijos kilmės informaciją;

14.4. atvaizduoti DBSIS sugeneruotą 4 skaitmenų autentifikavimo arba elektroninio dokumento pasirašymo užklausos patvirtinimo kodą, leidžiantį naudotojui įsitikinti sesijos autentiškumu.

15. Paslaugos turi būti teikiamos vadovaujantis:

15.1. 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentu (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB;

15.2. Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymu;

15.3. Lietuvos Respublikos kibernetinio saugumo įstatymu (toliau – KSĮ);

15.4. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 18 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

15.5. Elektroniniu parašu pasirašyto elektroninio dokumento specifikacija ADOC-V1.0, patvirtinta Lietuvos vyriausiojo archyvaro 2009 m. rugsėjo 7 d. įsakymu Nr. V-60 „Dėl Elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos ADOC-V1.0 patvirtinimo“;

15.6. kitais Lietuvos Respublikos teisės aktais, reglamentuojančiais elektroninio parašo naudojimą, elektroninio parašo paslaugų teikimą, valstybės informacinių išteklių valdymą ir kibernetinio saugumo užtikrinimą.

V. PASLAUGŲ LYGIO REIKALAVIMAI

16. Paslaugos turi būti pradėtos teikti kitą dieną po Sutarties įsigaliojimo dienos.

17. Paslaugos turi būti teikiamos nepertraukiamai 7 dienas per savaitę ir 24 valandas per parą.

18. Paslaugų prieinamumo per mėnesį lygis turi būti ne mažesnis kaip 99,5 proc.

19. Visi techninės priežiūros darbai turi būti iš anksto suderinti su Perkančiąja organizacija ir planuojami taip, kad minimaliai paveiktų paslaugų prieinamumą (pvz., tuo metu, kai DBSIS naudojimo aktyvumas yra mažiausias). Iš anksto su Perkančiąja organizacija suderinti techninės priežiūros darbai laikomi planine priežiūra ir nėra įtraukiami Techninės specifikacijos 18 punkte nurodytą Paslaugų prieinamumo per mėnesį rodiklį.

20. Identifikavus Paslaugų sutrikimus, šie turi būti šalinami tokia tvarka:

Aprašymas	Prioriteto lygis	Reakcijos laikas	Sprendimo laikas
Paslaugos visiškai arba iš dalies nepasiekiamos, todėl visi arba didžioji dauguma DBSIS naudotojų negali naudotis teikiamomis Paslaugomis	P1 Kritinis	30 min.	6 val.
Paslaugos visiškai arba iš dalies nepasiekiamos, arba veikia žymiai blogesniu atsakymo laiku ar	P2 Aukštas	30 min.	8 val.

funkcionalumu nei tikėtasi, todėl daugumai DBSIS naudotojų teikiamų Paslaugų prieinamumas mažėja ir gali turėti neigiamą poveikį			
Paslaugos visiškai arba iš dalies nepasiekiamos, arba veikia žymiai blogesniu atsakymo laiku ar funkcionalumu nei tikėtasi, todėl atskiriems DBSIS naudotojams ar jų grupėms (ribotam DBSIS naudotojų skaičiui) Paslaugų prieinamumas mažėja	P3 Vidutinis	30–60 min.	1 d. d.
Paslaugos veikia, nors jų funkcionalumas ribotas, tačiau turi minimalų poveikį DBSIS naudotojams ir neturi įtakos kritinėms operacijoms	P4 Žemas	30 min.–8 val.	3 d. d.

VI. KIBERNETINIO SAUGUMO REIKALAVIMAI

21. Tiekėjas privalo užtikrinti kibernetinių incidentų, galinčių turėti poveikį Paslaugų teikimui ir/arba DBSIS saugumui, valdymą ir apie juos pranešti Pirkėjui Sutartyje nustatytais ryšio kanalais (elektroniniu paštu ir (ar) kitomis priemonėmis):

21.1. apie didelį kibernetinį incidentą, atitinkantį KSĮ 18 str. 2 dalyje nurodytus kriterijus – nedelsiant, bet ne vėliau kaip per 24 (dvidešimt keturias) valandas nuo sužinojimo momento, pateikiant ankstyvąjį perspėjimą, kuriame pagal galimybes nurodoma, ar didelį kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti tarpvalstybinį poveikį;

21.2. apie kitą kibernetinį incidentą, neatitinkantį KSĮ 18 str. 2 dalyje nurodytų kriterijų – nedelsiant, bet ne vėliau kaip per 72 (septyniasdešimt dvi) valandas nuo sužinojimo momento, pateikiant ankstyvąjį perspėjimą, kuriame pagal galimybes nurodoma ar kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti poveikį Pirkėjo tinklams ir informacinėms sistemoms;

21.3. ne vėliau kaip per 1 (vieną) mėnesį nuo 24.1 ar 24.2 papunktyje nurodyto pranešimo apie kibernetinį incidentą pateikimo dienos pateikti galutinę ataskaitą, kurioje turi būti informacija, nurodyta KSĮ 18 straipsnio 4 dalies 4 punkte.

VII. APLINKOS APSAUGOS KRITERIJAI

22. Pirkimo objektui taikomas Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 „Dėl Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo patvirtinimo“, 4.4.3 papunktis.

_____