

Aut. vsp. Nr. 1P20170100
2017-07-11

PIRKIMO SUTARTIS NR. 41.16-64

2017 m. liepos 11 d.
Vilnius

Lietuvos bankas (toliau – **Užsakovas**), atstovaujamas Organizacijos tarnybos Informacinių technologijų departamento direktoriaus Andriaus Ženčiaus, veikiančio pagal Prekių, paslaugų ir darbų pirkimo bei kitų sutarčių rengimo, įforminimo ir saugojimo Lietuvos banke taisyklių, patvirtintų Lietuvos banko valdybos pirmininko 2015 m. gruodžio 22 d. įsakymu Nr. V 2015/(1.7-260603)-02-245, 14.1 papunkčio nuostatas, ir UAB “Critical Security” (toliau – **Paslaugų teikėjas**), kaip Lietuvos banko supaprastinto mažos vertės apklausos žodžiu būdu Lietuvos banko numizmatinių vertybių pardavimo sistemos įsilaužimų testavimo paslaugų pirkimo laimėtoja (supaprastinto mažos vertės pirkimo pažyma 2017-07-04 Nr. V 2017/(1.138.16.E-2602)-308.16-144), atstovaujama direktoriaus Miroslov Lučinskij, veikiančio pagal įmonės įstatus, toliau kartu arba atskirai vadinamos Šalimis, sudaro šią pirkimo sutartį (toliau – Sutartis):

I. SUTARTIES DALYKAS

1. **Paslaugų teikėjas** suteikia Lietuvos banko numizmatinių vertybių pardavimo sistemos įsilaužimų testavimo paslaugas (toliau – paslaugos), atitinkančias Sutarties priede pateiktoje techninėje specifikacijoje nustatytus reikalavimus, Sutartyje numatytais sąlygomis ir terminais, o **Užsakovas** už suteiktas paslaugas atsiskaito Sutartyje nustatyta tvarka ir sąlygomis.

II. SUTARTIES KAINA IR MOKĖJIMO TVARKA

2. Paslaugų kaina:

Eil. Nr.	Paslaugų pavadinimas	Kaina Eur
1	2	3
1.	Lietuvos banko numizmatinių vertybių pardavimo sistemos įsilaužimų testavimo paslaugos	3000,00
	21 proc. PVM, Eur	630,00
	Iš viso, Eur su PVM	3630,00

3. Paslaugų kaina su pridėtinės vertės mokesčiu (PVM) (toliau – Sutarties kaina) yra 3630,00 Eur (trys tūkstančiai šeši šimtai trisdešimt eurų 00 ct).

4. Paslaugų kaina, nurodyta Sutarties 2 punkto lentelėje, negali būti keičiama visą Sutarties galiojimo laikotarpį, išskyrus tą atvejį, jeigu teisės aktais bus pakeistas PVM dydis. Tada kaina bus keičiama atitinkama dalimi, atsižvelgiant į kainos sudėtyje esančio PVM dalį. Kaina bus perskaičiuota taip, kaip nurodyta, ir tai nebus laikoma Sutarties sąlygų keitimu. Sutarties kaina dėl kainų lygio pasikeitimo neperskaičiuojama ir nebus keičiama.

5. Į paslaugų kainą įtraukti visi susiję mokesčiai ir rinkliavos, pristatymo **Užsakovui** (Žirmūnų g. 151, LT-09128 Vilnius) ir visos kitos su paslaugų teikimu susijusios išlaidos.

6. **Užsakovas** už kokybiškai suteiktas paslaugas sumoka **Paslaugų teikėjui** ne vėliau kaip per 7 kalendorines dienas nuo pakartotinio testavimo rezultatų ataskaitos gavimo ir paslaugų perdavimo akto pasirašymo dienos ir teisingos PVM sąskaitos faktūros gavimo dienos. Mokėjimo terminas pradedamas skaičiuoti nuo paslaugų perdavimo akto pasirašymo dienos ir teisingos PVM sąskaitos faktūros gavimo dienos, atsižvelgiant į tai, kuri iš šių datų vėlesnė. Paslaugų perdavimo akte ir PVM sąskaitoje faktūroje turi būti nurodytas Sutarties numeris. PVM sąskaita faktūra pateikiama „E.sąskaita“ informacinėje sistemoje.

III. PASLAUGŲ SUTEIKIMO TERMINAS IR PRIĖMIMO TVARKA

7. **Paslaugų teikėjas** ne anksčiau kaip nuo 2017-07-10 ir ne vėliau kaip iki 2017-07-21 įsipareigoja atlikti paslaugas, atitinkančias techninėje specifikacijoje nustatytus reikalavimus ir per 5 darbo dienas po paslaugų atlikimo **Užsakovui** pateikti testavimo rezultatų ataskaitą, o pakartotinį aptiktų

pažeidžiamumą (spragų) testavimą atlikti po jų pašalinimo, bet ne vėliau kaip iki 2017-10-30 ir per 5 darbo dienas po paslaugų atlikimo pateikti **Užsakovui** pakartotino testavimo rezultatų ataskaitą.

8. Paslaugos arba jų dalys laikomos suteiktomis tik tada, kai **Užsakovas** pasirašo paslaugų perdavimo aktą, patvirtinantį, kad suteiktos paslaugos atitinka techninėje specifikacijoje nustatytus reikalavimus. Šalių atstovai pasirašo du vienodą juridinę galią turinčius paslaugų perdavimo akto egzempliorius, po vieną kiekvienai Sutarties Šaliai.

IV. ŠALIŲ ĮSIPAREIGOJIMAI

9. Užsakovas įsipareigoja:

9.1. po pirminės testavimo rezultatų ataskaitos gavimo, ne vėliau kaip iki 2017-10-15 pašalinti testavimo rezultatų ataskaitoje nurodytas Lietuvos banko numizmatinių vertybių pardavimo sistemos pažeidžiamumo spragas;

9.2. kai **Paslaugų teikėjas** Sutarties 7 punkte numatytais terminais suteikia paslaugas, patikrinti jas ir priimti kokybiškas paslaugas bei per 5 darbo dienas pasirašyti paslaugų perdavimo aktą;

9.3. užtikrinti, kad atsakingieji tarnautojai bendradarbiaus su **Paslaugų teikėjo** specialistais ar atstovais paslaugų teikimo klausimais;

9.4. sumokėti **Paslaugų teikėjui** už paslaugas Sutarties 6 punkte nustatyta tvarka ir terminais;

9.5. tinkamai vykdyti kitus įsipareigojimus, numatytus Sutartyje ir galiojančiuose Lietuvos Respublikos teisės aktuose.

10. Paslaugų teikėjas įsipareigoja:

10.1. Suteikti paslaugas vadovaujantis Sutarties nuostatomis ir 7 punkte nustatytais terminais, galiojančių teisės aktų reikalavimais ir juose nustatytais apribojimais. **Paslaugų teikėjo** suteiktos paslaugos turi atitikti pirkimo sąlygas, pasiūlymą ir Sutartį;

10.2. pateikti testavimo rezultatų ataskaitas taip, kaip numatyta Sutarties 7 punkte.

10.3. informuoti **Užsakovą** apie aplinkybes, išskyrus Sutarties 23 punkte nurodytas aplinkybes, trukdančias tinkamai suteikti paslaugas, raštu elektroniniu paštu IT-sutartys@lb.lt per 3 kalendorines dienas nuo šių aplinkybių atsiradimo dienos. Šis pranešimas neatleidžia **Paslaugų teikėjo** nuo Sutartyje nustatytų įsipareigojimų įvykdymo;

10.4. užtikrinti Sutarties vykdymo metu iš **Užsakovo** gautos ir su Sutarties vykdymu susijusios informacijos konfidencialumą, apsaugą, neatskleidimą ir užtikrinti, kad šių įsipareigojimų laikytųsi **Paslaugų teikėjo** specialistai ir paslaugoms teikti pasitelkti tretieji asmenys (jeigu pasitelkiami), išskyrus tuos atvejus, kai informaciją privaloma atskleisti pagal Lietuvos Respublikos įstatymus;

10.5. tinkamai vykdyti kitus įsipareigojimus, numatytus Sutartyje ir galiojančiuose Lietuvos Respublikos teisės aktuose.

V. ŠALIŲ ATSAKOMYBĖ

11. **Paslaugų teikėjas**, laiku nesuteikęs paslaugų, sumoka **Užsakovui** 0,02 proc. delspinigius, skaičiuojamus nuo Sutarties kainos su PVM, už kiekvieną pradelstą kalendorinę dieną. Paslaugų perdavimo akte turi būti nurodytas pradelstų dienų skaičius ir apskaičiuotų delspinigių suma, kuria atsiskaitydamas už paslaugas **Užsakovas** mažins **Paslaugų teikėjo** pateiktoje PVM sąskaitoje faktūroje nurodytą mokėjimo sumą.

12. **Užsakovas**, laiku neatsiskaitęs už suteiktas paslaugas, sumoka **Paslaugų teikėjui** 0,02 proc. delspinigius, skaičiuojamus nuo laiku nesumokėtos sumos su PVM, už kiekvieną pradelstą kalendorinę dieną.

13. Jeigu **Paslaugų teikėjas** per 10 kalendorinių dienų nuo delspinigių mokėjimo pradžios nesuteiks paslaugų, tai **Užsakovas**, apie tai elektroniniu paštu m.lucinskij@sec-consult.com informavęs **Paslaugų teikėją** prieš 10 kalendorinių dienų, gali vienašališkai nutraukti Sutartį. Tokiu atveju **Paslaugų teikėjas** sumoka **Užsakovui** 300 Eur (trys šimtai eurų) baudą ir priskaičiuotus delspinigius. Baudą ir delspinigius **Paslaugų teikėjas** sumoka **Užsakovui** ne vėliau kaip per 10 darbo dienų nuo Sutarties nutraukimo dienos.

14. **Užsakovas**, pasirašęs Sutartį, bet vėliau ją vienašališkai nutraukęs ne dėl **Paslaugų teikėjo** kaltės ir apie tai elektroniniu paštu m.lucinskij@sec-consult.com informavęs **Paslaugų teikėją** prieš 10 kalendorinių dienų, arba **Paslaugų teikėjui** nutraukus Sutartį dėl Sutarties 18 punkte numatytų

aplinkybių, moka **Paslaugų teikėjui** 300 Eur (trys šimtai eurų) baudą ne vėliau kaip per 10 darbo dienų nuo Sutarties nutraukimo dienos. Ši bauda nemokama, jeigu Sutartis nutraukiama Viešųjų pirkimų tarnybos nurodymu.

15. **Paslaugų teikėjas**, pasirašęs Sutartį, bet vėliau ją vienašališkai nutraukęs ne dėl **Užsakovo** kaltės ir apie tai elektroniniu paštu IT-sutartys@lb.lt informavęs **Užsakovą** prieš 10 kalendorinių dienų, arba **Užsakovui** ją nutraukus dėl Sutarties 17.1 ir (arba) 17.2 papunktyje nurodytų aplinkybių, moka **Užsakovui** 300 Eur (trys šimtai eurų) baudą ne vėliau kaip per 10 darbo dienų nuo Sutarties nutraukimo dienos.

VI. SUTARTIES GALIOJIMO, KEITIMO IR NUTRAUKIMO SĄLYGOS

16. Sutartis įsigalioja Šalims pasirašius Sutartį ir galioja iki visiško pagal Sutartį prisiimtų įsipareigojimų įvykdymo arba iki Sutarties nutraukimo Sutartyje arba galiojančiuose Lietuvos Respublikos teisės aktuose nustatytais atvejais ir tvarka.

17. **Užsakovas** turi teisę nutraukti Sutartį vienašališkai, nesikreipdamas į teismą, apie tai elektroniniu paštu m.lucinskij@sec-consult.com pranešęs **Paslaugų teikėjui** prieš 10 kalendorinių dienų, jeigu:

17.1. **Paslaugų teikėjas** pažeidžia savo sutartinius įsipareigojimus ir, nepaisydamas **Užsakovo** raštu pateikto įspėjimo, nepradeda jų tinkamai vykdyti per Sutarties 13 punkte nustatytą laikotarpį;

17.2. padarytas esminis sutarties pažeidimas, apibrėžtas Sutarties 21 punkte.

18. **Paslaugų teikėjas** turi teisę nutraukti Sutartį vienašališkai, nesikreipdamas į teismą, apie tai elektroniniu paštu IT-sutartys@lb.lt pranešdamas **Užsakovui** prieš 10 kalendorinių dienų, jeigu **Užsakovas** ne dėl **Paslaugų teikėjo** kaltės vėluoja atlikti mokėjimą daugiau kaip 30 kalendorinių dienų, nepaisydamas **Paslaugų teikėjo** raštu pateikto įspėjimo.

19. Sutartis gali būti nutraukta raštišku Šalių susitarimu.

20. Sutarties nutraukimas Sutarties 13, 14 ir 15 punktuose numatytais atvejais neatleidžia Šalių nuo šiuose punktuose numatytų įsipareigojimų įvykdymo ir baudų sumokėjimo.

21. Sutarties 7, 10.1, 10.2 punktų sąlygos laikomos esminėmis ir dėl jų pažeidimo Sutartis gali būti vienašališkai **Užsakovo** nutraukta dėl esminio pirkimo sutarties pažeidimo.

22. Sutarties sąlygos jos galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias Sutarties sąlygas, kurias pakeitus nebūtų pažeisti Viešųjų pirkimų įstatymo 17 straipsnyje nustatyti principai ir tikslai. Sutarties sąlygų keitimu nebus laikomas Sutarties sąlygų koregavimas joje numatytomis aplinkybėmis, jeigu šios aplinkybės nustatytos aiškiai, nedviprasmiškai ir buvo numatytos pirkimo dokumentuose. Tais atvejais, kai Sutarties sąlygų keitimo būtinybės nebuvo įmanoma numatyti rengiant pirkimo dokumentus ir sudarant Sutartį, Šalys gali keisti tik neesmines Sutarties sąlygas. Sutarties pakeitimai turi būti įforminami raštu dokumentais, pasirašytais **Paslaugų teikėjo** ir **Užsakovo** įgaliotųjų asmenų, ir jie bus neatskiriamos Sutarties dalys.

VII. NENUGALIMA JĖGA (*FORCE MAJEURE*)

23. Šalys neatsako už savo įsipareigojimų pagal Sutartį nevykdymą, jeigu tokio nevykdymo arba netinkamo vykdymo priežastis buvo nenugalimos jėgos (*force majeure*) aplinkybės. Nenugalima jėga yra suprantama taip, kaip ją apibrėžia Lietuvos Respublikos teisės aktai.

24. Šalis, negalinti tinkamai vykdyti savo sutartinių įsipareigojimų dėl nenugalimos jėgos aplinkybių, per 3 kalendorines dienas nuo to momento, kai sužinojo arba turėjo sužinoti apie šių aplinkybių atsiradimą, privalo raštu pranešti apie tai kitai Šaliai. Neįvykdžiusi šios pareigos Šalis privalo atlyginti dėl to atsiradusius tiesioginius nuostolius.

25. Nenugalimos jėgos aplinkybėms užsitęsus ilgiau nei 30 kalendorinių dienų, bet kuri Šalis turi teisę vienašališkai nutraukti Sutartį, apie tai raštu pranešusi kitai Šaliai.

VIII. ŠALIŲ GINČŲ SPRENDIMO TVARKA

26. Visi ginčai, susiję su Sutartimi, sprendžiami derybomis, o nepavykus taip išspręsti ginčo, jis nagrinėjamas Lietuvos Respublikos civilinio proceso kodekso nustatyta tvarka.

IX. KITOS SUTARTIES SĄLYGOS

27. Kitos paslaugų tiekimo sąlygos, kurios nėra aptartos Sutartyje, numatytos pirkimo sąlygose ir privalomos abiem Šalims.

28. **Paslaugų teikėjas** neturi teisės perduoti Sutartimi apibrėžtų teisių ir pareigų tretiesiems asmenims.

29. Sutartis sudaryta dviem egzemplioriais lietuvių kalba, po vieną kiekvienai iš Šalių. Abu egzemplioriai turi vienodą juridinę galią.

30. Sutartis sudaryta vadovaujantis Lietuvos Respublikos teise. Sutartis arba atskiros jos nuostatos turi būti aiškinamos vadovaujantis Lietuvos Respublikos teise.

31. Prie Sutarties pridama techninė specifikacija, kuri yra neatskiriama Sutarties dalis (Sutarties priedas).

X. ŠALIŲ ADRESAI IR REKVIZITAI

Užsakovas

Lietuvos bankas
Gedimino pr. 6, LT-01103 Vilnius
Tel.: 268 0029, faks. 268 0038
Sąsk. LT41 1010 0000 0012 3456
Lietuvos banke
Įmonės kodas 188607684
PVM mokėtojo kodas LT 886076811

Organizacijos tarnybos
Informacinių technologijų departamento
direktorius

Andrius Ženčius



Paslaugų teikėjas

UAB "Critical Security"
Mokyklos g. 40-1, Vilnius
Tel.: 671 84203
Sąsk. LT157300010098571865
AB Swedbank banke
Įmonės kodas 300646885
PVM mokėtojo kodas LT 100004541418

Direktorius

Miroslav Lučinskij



TECHNINĖ SPECIFIKACIJA

Paslaugų teikėjas privalo atlikti naujai sukurtos Lietuvos banko numizmatinių vertybių pardavimo sistemos ir su ja susijusios techninės įrangos įsilaužimų testavimo paslaugas nurodytas šios techninės specifikacijos lentelėje (toliau – paslaugos).

Eil. nr.	Rodiklis
1.	Sistemos išorinio tinklo perimetro patikrinimas (patikrinimas atliekamas turint minimalias žinias apie Sistemos informacinių technologijų (toliau – IT) infrastruktūrą, imituojant potencialaus įsilaužėlio iš interneto veiksmus):
1.1.	informacijos apie tiriamą objektą surinkimas iš viešai prieinamų šaltinių
1.2.	perimetro tinklo mazgų, pasiekiamų iš interneto nustatymas
1.3.	perimetro tinklo mazguose veikiančių operacinių sistemų nustatymas ir atitinkamų, šiai dienai žinomų, pažeidžiamumų patikrinimas
1.4.	perimetro tinklo mazguose veikiančių tarnybų nustatymas ir atitinkamų, šiai dienai žinomų, pažeidžiamumų patikrinimas bei konfigūracijos analizė
1.5.	jei aptinkama iš interneto pasiekiamų tarnybų, reikalaujančių vartotojo tapatybės nustatymo, tuomet atliekamas išorinės paslaugos slaptažodžių auditas; taip turi būti tikrinama, ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti
1.6.	nustačius pažeidžiamumus atliekamas įsilaužimo testas (pvz.: ribotos išorinės prieigos išnaudojimas siekiant padidinti savo teises Sistemoje)
1.7.	išorinio patikrinimo vertinimo apimtis: kompiuterių tinklo segmentai priklausantys Sistemai
2.	Sistemos portalo ir jame veikiančių naudotojų programų komponentių, kurias naudoja naudotojai interneto naršyklės pagalba, patikrinimas:
2.1.	sisteminių paslaugų (angl. services) konfigūracijos patikrinimas
2.2.	automatizuota pažeidžiamumų paieška
2.3.	automatizuotos paieškos rezultatų patikrinimas
2.4.	atliekant portalo technologinių pažeidžiamumų vertinimą turi būti patikrintas atsparumas šiems pagrindiniams pažeidžiamumams:
2.4.1.	XSS (angl. cross-site scripting) ir CSRF (angl. cross-site request forgery)
2.4.2.	įvairios injekcijos (pvz., SQL, XML, LDAP ir PHP instrukcijų injekcijos)
2.4.3.	perduodamų duomenų perėmimo galimybės ir manipuliavimas jais
2.4.4.	sisteminių paslaugų konfigūracijos patikrinimas: darbinės direktorijos (katalogo) pakeitimas/manipuliavimas, tarnybos teisių padidinimas, informacijos atskleidimas per klaidų pranešimus
2.4.5.	„Input Validation“, „SQL injection“, „Buffer overflow“ ir manipuliuojant pateikiamais duomenimis ar duomenų paketais ir įvertinant kaip į iškraipytus duomenis reaguoja programinė įranga
2.4.6.	Denial of Service“ atakos
3.	Sistemos programų komponentių, prieinamų naudotojams interneto naršyklės pagalba, išeities tekstų patikrinimas:
3.1.	atliekant trūkumų paiešką turi būti patikrinti visi Sistemoje (portale) naudotojams prieinami naudotojų tapatybės nustatymo programinės komponentės ir jų sąajos su kitose sistemose esančiomis programinėmis komponentėmis, kurie priklauso Sistemai
3.2.	turi būtų atliktas Sistemos programinių komponentių, prieinamų išoriniams naudotojams Sistemos portale, išeities tekstų patikrinimas pagal „white-box“ principą
3.3.	trūkumų turi būti ieškoma tomis teisėmis ir sąlygomis, kuriomis dirba Sistemos naudotojai
3.4.	turi būti patikrinti dažniausiai pasitaikantys programavimo trūkumai
3.5.	programų logikos ir jų išnaudojimo galimybių vertinimas

3.6.	naudotojų prieigos teisių prie informacijos išteklių programinėje įrangoje patikrinimas
3.7.	naudotojų autentifikavimo, identifikavimo, autorizavimo ir naudotojų sesijų valdymo saugumas ir perėmimo galimybių patikrinimas
3.8.	naudotojų teisių ir prieigos lygių portalo puslapiuose patikrinimas
3.9.	portale įgyvendintų elektroninių viešųjų paslaugų patikrinimas
3.10.	portale esančių sąsajų su kitose sistemose veikiančiomis elektroninėmis viešosiomis paslaugomis patikrinimas
3.11.	atliekant patikrinimus, turi būti laikomasi pasaulinės nepriklausomos organizacijos OWASP (<i>angl. Open Web Application Security Project</i>) teikiamų rekomendacijų (http://www.owasp.com , <i>OWASP Developer Guide</i> https://www.owasp.org/index.php/Category:OWASP_Guide_Project ; <i>OWASP Testing Guide v4</i> https://www.owasp.org/index.php/Category:OWASP_Testing_Project .)
4.	Reikalavimai Lietuvos banko numizmatinių vertybių pardavimo sistemos įsilaužimų testavimo ataskaitai:
4.1.	Atliktas Sistemos atsparumo įsilaužimui testavimas ir pateikta Sistemos atsparumo įsilaužimui testavimo/vertinimo ataskaita, saugos užtikrinimo išvados ir rekomendacijos pagal šias sritis:
4.1.1.	tikrintų objektų aprašymą
4.1.2.	patikrinimo metodiką: tikslus, metodus, scenarijus, naudotus įrankius
4.1.3.	aptiktų pažeidžiamumų/spragų aprašymą, kartu pateikiant pažeidžiamumų buvimo įrodymus, nurodant pažeidžiamumo kritiškumo lygį bei detales spragų pašalinimo rekomendacijas ir galimus sprendimus
4.1.4.	įsilaužimo scenarijų aprašymą – turi būti detalai aprašyta veiksmų seka, kaip gali būti išnaudotas vienas ar kitas saugos trūkumas (pateikiamas tik esant technologiniam pažeidžiamumui)
4.2.	Ataskaitoje turi būti:
4.2.1.	nustatytų saugos pažeidžiamumų apžvalga ir rekomendacijos (santrauka)
4.2.2.	detalus vertinimo eigos aprašas
4.2.3.	visų naudojamų technologinių patikrinimų (skenavimų) originalūs rezultatai (elektronine forma)
4.2.4.	Parengti dokumentai pateikiami lietuvių kalba popierine (2 egz.) ir elektronine (redaguojama) forma (Microsoft Word, Excel ir pan. / PDF, HTML, XML, CSV) įrašyti į kompaktinį diską (1 vnt.)
5.	Nustatytų, aptiktų pažeidžiamumų/spragų, Lietuvos bankui jas pašalinus, pakartotinis testavimas ir atskaitos apie pakartotinį testavimą pateikimas

Užsakovas

Lietuvos bankas
 Gedimino pr. 6, LT-01103 Vilnius
 Tel.: 268 0029, faks. 268 0038
 Sąsk. LT41 1010 0000 0012 3456
 Lietuvos banke
 Įmonės kodas 188607684
 PVM mokėtojo kodas LT 886076811

Organizacijos tarnybos
 Informacinių technologijų departamento
 direktorius

Andrius Ženčius

**Paslaugų teikėjas**

UAB "Critical Security"
 Mokyklos g. 40-1, Vilnius
 Tel.: 671 84203
 Sąsk. LT157300010098571865
 AB Swedbank banke
 Įmonės kodas 300646885
 PVM mokėtojo kodas LT 100004541418

Direktorius

Miroslav Lučinskij

