NUMERIŲ PERKĖLIMO CENTRINĖS DUOMENŲ BAZĖS ADMINISTRAVIMO PASLAUGŲ SUTARTIES PRIEDAS NR. 6

PASLAUGŲ SAUGUMO UŽTIKRINIMO PRIEMONĖS IR REIKALAVIMAI

1. Patalpos

NPCDB įranga talpinama saugiose patalpose (viena patalpa skirta pagrindinei įrangai, antra – avarinio atstatymo įrangai sumontuoti) su perimetro bei tūrio apsauga bei sienų vibracijos davikliais ir aplinkos parametrus užtikrinančia įranga. Patalpos yra specialiai pritaikytos kompiuterinei įrangai ir atitinka Konkurso sąlygų reikalavimus:

a) Patalpos ir įėjimas į patalpas yra nuolat (24 val. per parą, 7 d. per savaitę) stebimi vaizdo kameromis, vaizdo duomenys saugomi 3 mėnesius;

b) Patalpos turi įėjimo kontrolę, perimetro ir tūrio apsaugą, įskaitant sienų vibracijos daviklius;

c) Patalpos nėra pastatų rūsiuose, pusrūsiuose ir viršutiniuose aukštuose. NPCDB skirtos patalpos yra antruose pastatų aukštuose iš trijų;

d) Pagrindas, ant kurio bus sumontuota NPCDB, bus įrengtas 30 centimetrų aukščiau patalpos grindų;

e) Patalpose yra įrengta priešgaisrinė apsauga;

f) Patalpose yra sumontuota dubliuota tikslios oro temperatūros ir drėgmės palaikymo įranga (kondicionavimo ir klimato kontrolės sistema);

g) Papildoma atsarginė elektros tiekimo sistema (nenutrūkstamo tiekimo šaltinis ir dyzelinis generatorius, įrengtas atskiroje patalpoje). Elektros energija į patalpą yra teikiama dviem nepriklausomais ir iš skirtingų pastočių ateinančiais elektros įvadais su automatiniais rezerviniais įrenginiais, taip pat yra įrengti dubliuojantys nepertraukiamos srovės tiekimo įrengimai, užtikrinantys elektros energijos tiekimą nemažiau nei 12 val., nutrūkus pagrindiniam elektros tiekimui;

h) Siūlomos dvi atskiros patalpos: vienoje bus sumontuota pagrindinė įranga, kitoje – avarinio atstatymo įranga. Įrengimai, užtikrinantys rezervines NPCDB duomenų kopijas, bus įrengti avarinio atstatymo įrangos vietoje, t. y. kitoje patalpoje nei pagrindinė NPCDB;

i) Patekti į patalpą galės tik asmenys, kuriems bus suteiktos teisės patekti į šias patalpas, jų apsilankymai bus registruojami įėjimo į patalpą žurnale.

2. NPCDB saugumo užtikrinimo būdai

Pagrindiniai būdai, kaip užtikrinti NPCDB ir joje esančios informacijos/ duomenų saugumą yra šie:

- vartotojų identifikavimo ir autentifikavimo mechanizmas;
- rolių ir vartotojų teisių priskyrimo modulis;
- vartotojų teisių prieiti prie duomenų valdymas;
- vartotojų veiksmų, dirbant NUMLEX sistemoje, registravimas;
- registravimas visų veiksmų numerio rėžių importavimo metu;
- sistemos duomenų bazės atsarginių kopijų darymas ir galimybė atstatyti duomenis, pasinaudojant kopijomis;
- galimybė koduoti asmeninius ir/ar susijusius duomenis;
- pagal nutylėjimą yra numatyta, kad vienam vartotojui gali būti viena sesija (šis parametras yra konfigūruojamas).

Kliento autorizacijai naudojamas vartotojo profilis (angl. user profile). Vartotojo profilis nustato Kliento teises prieiti prie sistemos resursų ir funkcijų: duomenų bazės lentelių, bylų, modulių, ataskaitų ir kt. Klientas gali turėti daugiau kaip vieną profilį.

Taip pat Klientams yra priskiriamos atitinkamos rolės, nustatančios teises ir prieigas prie sistemos resursų bei funkcijų. Klientams yra siūlomos šios 2 pagrindinės roles:

- Pažengęs vartotojas;
- Paprastas vartotojas.

Pagal poreikį šios rolės gali būti pakeistos. Taip pat, atsižvelgiant į kiekvieno projekto specifiką, gali būti apibrėžtos rolės ir tinklo ekspertams bei klientų aptarnavimo specialistams.

3. Prieigos prie tinklo būdai

NPCDB palaiko šiuos saugios prieigos prie tinklo būdus:

- HTTPS;
- VPN.

HTTPS

HTTPS (angl. Hypertext Transfer Protocol Secure) yra plačiai naudojamas ryšio protokolas saugiam komunikavimui per kompiuterinį tinklą. HTTPS – HTTP protokolo praplėtimas, palaikantis šifravimą. Duomenys perduodami HTTP protokolui „įpakuojami“ į SSL arba TLS protokolą, tuo pačiu užtikrinamas duomenų saugumas. SSL (angl. Secure Socket Layer – apsaugotų sluoksnių protokolas) – kriptografinis protokolas, užtikrinantis saugų domenų perdavimo Interneto tinklais. Šio protokolo naudojimo metu sudaromas saugus sujungimas tarp kliento ir tarnybinės stoties.

NPCDB sistemos internetinė vartotojo sąsaja (angl. WEB GUI) yra pasiekiama per HTTPS. Taip pat, kad būtų užtikrintas dar didesnis saugumas, tikrinamas IP, iš kurio yra jungiamasi. Leidžiama jungtis tik iš sistemoje numatytų vietų.

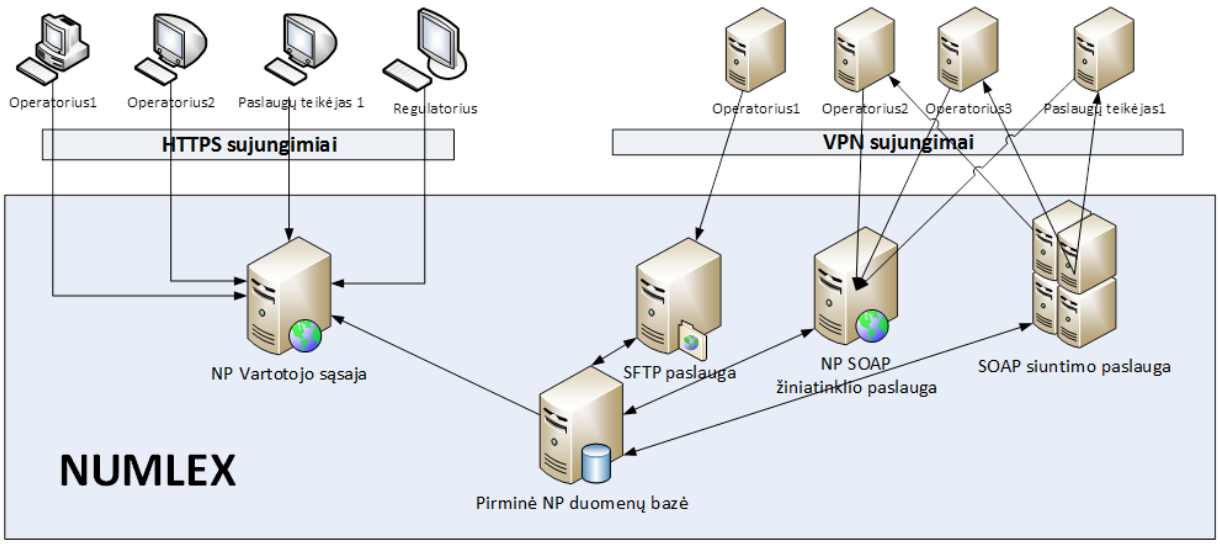
VPN

VPN (angl. Virtual Private Network, VPN) yra tinklo ryšys, sukurtas kito tinklo (pvz., interneto) išorėje arba viduje. Taip dažniausiai vadinamas saugus tinklo ryšys arba tunelis nesaugaus interneto ryšio viduje. Šiame tunelyje VPN pagalba vyksta duomenų, kuriuos vartotojo kompiuteris pateikia interneto svetainėms ar programinei įrangai, besijungiančiai prie interneto apsauga – šifravimas. Tokiu būdu duomenų gavėjas mato gaunamus duomenis ne iš vartotojo, bet iš VPN serverio.

Prisijungimui prie NPCDB sistemos naudojamas IPSec (angl. Internet Protocol Security). IPSec – tai protokolų rinkinys ir kartu standartas, sukurtas IETF (angl. Internet Engineering Task Force) grupės. Jis yra paremtas galingomis šiuolaikinėmis duomenų kodavimo technologijomis ir suteikia saugumo mechanizmus jau IP lygyje. Tai yra didelis privalumas tinklo vartotojui, kuriam nereikia rūpintis tunelio sukūrimu ar valdymu.

VPN yra rekomenduojamas SOAP saityno paslaugos sąsajai tarp NPCDB sistemos ir operatorių sistemų (angl. „back office“ systems). VPN yra tinkamas įvairių dydžių kompanijoms.

Prisijungimas prie NPCDB sistemos yra saugus, nes vykdomas per koduotą kanalą (HTTPS arba VPN).



1 pav. *Saugus prisijungimas prie NPCDB per HTTPS ir VPN koduotus kanalus*

Šalių rekvizitai:

Administratorius	**Klientas**
Viešoji įstaiga „Numerio perkėlimas“: Jogailos g. 9, LT- 01116 Vilnius Įmonės kodas: 303386211 Duomenys kaupiami ir saugomi Juridinių asmenų registre AB SEB bankas A/s Nr.: LT47 7044 0600 0798 0315 Banko kodas: 70440 Tel.: (8 699) 23 530, faks.: (8 699) 00 111 El. paštas: info@numerioperkelimas.lt Jolita Kurtinaitienė VšĮ “Numerio perkėlimas” direktorė	
_____	_____
A.V.	A.V.