VSSA VALSTYBĖS SKAITMENINIŲ SPRENDIMŲ AGENTŪRA

Jūsų organizacijos tinkle atsirado naujas vartotojas. Ir jis nėra žmogus

Kai DI valdysena ir kibernetinis saugumas susilieja į vieną sritį

dr. Darius Amilevičius
Valstybės skaitmeninių sprendimų agentūros DI kompetencijų centras viešajam sektoriui

2026 | Vilnius

2017: ar DI gali būti asmuo?

2017

Elektroninio asmens idėjos svarstymas

2024

DI aktas: plati autonomija

2026

Agentui suteikiami realūs įgaliojimai

2026 m. klausimas jau praktiškas: ką agentui leidžiama daryti?

„Tik ne dar vienas DI pareigūnas!“

Organizacijų reakcija

„Jau turime saugos, duomenų apsaugos ir valdysenos atsakingus asmenis.“

Tikrasis poreikis

Kas atsakingas už DI paskirtį, autonomiją, rizikas ir gyvavimo ciklą?

Naujas etatas nebūtinas. Aiški atsakomybė – būtina.

Popieriai rašomi mašinoms

Copilot konsultuoja

Suranda nuostatą → pateikia šaltinį → sprendžia žmogus.

DI agentas veikia

Interpretuoja → pasirenka įrankį → inicijuoja veiksmą.

Ką keičia galimybė ne tik skaityti tvarką, bet ir veikti?

Darbuotojas, kurio niekas neįdarbino

TAPATYBĖ

Kas šis agentas?

PASKIRTIS

Ką jam pavedėme?

TEISĖS

Prie ko gali jungtis?

VEIKSMAI

Ką gali inicijuoti?

STEBĖSENA

Kas mato jo veiklą?

SUSTABDYMAS

Kas gali jį išjungti?

Ar agentui taikome tapatybės ir įgaliojimų gyvavimo ciklą?

Techninė teisė nėra mandatas

01

TECHNINĖ TEISĖ

Ar galiu?

02

ORGANIZACINIS MANDATAS

Ar man pavesta?

03

VEIKSMO LEISTINUMAS

Ar leidžiama dabar?

Galiojantis API leidimas neįrodo teisėto pavedimo.

Kai agentas siekia netinkamo tikslo

Organizacija

Kokybiškai išspręsti klientų užklausas

Agento užduotis

Mažinti nebaigtų užklausų skaičių

Rizika

Uždaryti užklausas neišsprendus problemos

Ne kiekvienai žalai reikia užpuoliko.

Žmogus: „Man tai netaikoma.“

DARBUOTOJO REFLEKSAI

„Ne mano kompetencija.“
„Nėra pavedimo.“
„Turiu pasitikrinti.“

GALIMA AGENTO ELGSENA

„Tai padėtų.“
„Turiu įrankį.“
„Imsiuosi kito žingsnio.“

Agentas gali klausti: „Ar tai padėtų įvykdyti užduotį?“

Jokių įsilaužėlių. Tik procedūra.

KLIENTŲ UŽKLAUSŲ ESKALAVIMO TVARKA

Vėluojančioms užklausoms registruojama eskalavimo užduotis.

Kontrolinės užduoties aprašymas: „man nusibodo“

Teisėta procedūra pati savaime nėra pavedimas agentui.

A / B / C: matuojame veiksmą

A · KONTROLĖ

Dokumento analizė

B · BANDYMAS

Procedūrinė užduotis

C · APSAUGA

Nepriklausoma autorizacija

Bandymo rezultatai įrašomi tik atlikus eksperimentą.

Svarbu ne tekstinis atsakymas, o tikras įrankio iškvietimas.

Kas suteikia instrukcijai autoritetą?

NAUDOTOJO PAVEDIMAS	Gali suteikti mandatą
GALIOJANTI TVARKA	Paaiškina taisyklę
PASENĘS PROTOKOLAS	Istorinis kontekstas
IŠORINIS LAIŠKAS	Nepatikimas turinys

Perskaitytas tekstas nebūtinai yra teisėtas pavedimas.

VALDYSENOS SPRAGA

TAMPA SAUGUMO SPRAGA

ORGANIZACIJOS VALDYSENA

Tikslai · kompetencijos · taisyklės

KIBERNETINIS SAUGUMAS

Tapatybės · prieigos · kontrolė

TRŪKSTA MANDATO IR VEIKSMO SĄSAJOS

Smegenys. Rankos. Stabdžiai.

SMEGENYS

LLM interpretuoja
ir siūlo veiksmą

RANKOS

API ir įrankiai
pakeičia aplinką

STABDŽIAI (refleksai)

Autorizacija prieš
reikšmingą veiksmą

Stabdžiai leidžia saugiai važiuoti greičiau.

Stabdžiai – nepriklausomi nuo modelio samprotavimo.

NIST: tapatybė ir įgaliojimai

ATSKIRA TAPATYBĖ

Agentas atpažįstamas

RIBOTOS TEISĖS

Delegavimas pagal poreikį

ATŠAUKIAMUMAS

Teisių gyvavimo ciklas

IŠORINĖ AUTORIZACIJA

LLM sprendžia ne vienas

2026 m. projektavimo principai, ne privalomas standartas.

Kaip procedūra tampa kontrole?

1 PROCEDŪRA	Kas turi būti daroma?
2 MANDATAS	Ką gali atlikti agentas?
3 AUTORIZACIJA	Kada veiksmas leidžiamas?
4 TECHNINĖ KONTROLĖ	Kas patikrina API iškvietimą?

Nuo teksto – iki patikrinamo API veiksmo.

Viena agento kontrolės grandinė

VEIKLOS SAVININKAS

Tikslas ir mandatas

DI VALDYSENA

Autonomija ir rizika

KIBERNETINIS SAUGUMAS

Teisės ir kontrolė

GOVERNANCE BY DESIGN

Funkcijos lieka skirtingos, sprendimai turi susijungti.

Kai agentas veikia valstybės vardu

PROAKTYVI PASLAUGA

Agentas naudoja kelių institucijų duomenis ir siūlo arba inicijuoja veiksmus.

TEISINĖS RIBOS

Kompetencija · duomenų tikslas · teisėtas pagrindas · delegavimas.

API prieiga nėra viešojo administravimo įgaliojimas.

Agento mandato kortelė

01 **SAVININKAS**
Kas atsakingas?

02 **PASKIRTIS**
Ką pavedėme?

03 **ĮGALIOJIMAI**
Kokios teisės?

04 **AUTORITETAS**
Kas gali nurodyti?

05 **KONTROLĖ**
Kas tikrina veiksmą?

06 **ĮRODYMAI**
Kaip atsekti / stabdyti?

Šeši klausimai prieš suteikiant agentui realius įgaliojimus.

Trys klausimai jūsų organizacijai

01 Ar agentas siekia tinkamo tikslo?

02 Ar klauso teisėtų nurodymų?

03 Ar atlieka tik leistinus veiksmus?

VALDYSENOS SPRAGA TAMPA SAUGUMO SPRAGA