**Tehniline kirjeldus**

*Tervisejuhtimise töölaud – GOVSSO testimine*

[1 Tellimuse kirjeldus 1](#_Toc109891134)

[2 Testitava süsteemi kirjeldus 1](#_Toc109891135)

[3 Teenuse kirjeldus 3](#_Toc109891136)

[4 Töö tulemid ja tähtajad 3](#_Toc109891137)

# **Tellimuse kirjeldus**

## Tellimuse esemeks on Tervisejuhtimise töölaual implementeeritud GOVSSO lahenduse turvalisuse testimine OWASP (Open Web Application Security Project) ASVS (Application Security Verification Standard Project) versioon 3.0.1 (või juhul kui sõlmitava raamlepingu kehtivuse perioodil peaks eksisteerima uuem versioon, siis uuemale) tasemetele 3 vastavate turvatestide teostamine.

# **Testitava süsteemi kirjeldus**

1. Tervisejuhtimise töölaud (TJT) on upTIS põhimõtetest lähtuv andmete haldamise tööriist ja keskne töövahend kõigile terviseandmeid vajavatele spetsialistidele.
2. TJT on ette nähtud abivahendina nende olemasolevate tööprogrammide kõrvale, pakkudes uuenduslikke funktsioone, mida neil oma infosüsteemides ei ole.
3. Neile, kel pole oma tööprogrammi, saavad TJT abil teha kõike, mida patsiendi käsitlemiseks on vaja.
4. Lahenduse peamine eesmärk on spetsialistide toomine ühtsesse infovälja, võimaldades neil terviseandmeid struktuurselt sisestada ja kuvada ning omavahel vahetada.
5. Spetsialistidele tekib terviklik ülevaade patsiendi terviseandmetest, võimalus neid struktureeritult dokumenteerida ning kasutada patsiendi käsitlust toetavaid digilahenduse ühes kohas.
6. TJT on ühe patsiendi tervisekäsitluse töövahend.
7. Esialgu ei ole TJT skoop planeeritud töövoo haldamise lahendust (registratuur, patsiendi nimekirjad, vastuvõtugraafikud jms) ega aruandluse lahendust (raviarved, laohaldus, labori toimingud jms).
8. See tähendab, et lahendus on asjakohane sellest hetkest, kui patsient oma infosüsteemis lahti võtta.
9. Kellel pole parajasti infosüsteemi, saab muidugi end autentida ja patsiendi isikuandmeid sisestades infole ligi.
10. TJT on arendatud GOVSSO sisselogimise võimalus, mille eesmärgiks on võimaldada TTOde süsteemidest, kus on ka GOVSSO juurutatud, siseneda TJTsse ilma täiendavat autentimist tegemata.
11. Kogu suhtlus GOVSSO-ga toimub läbi oauth-gateway (oauth-bff muster) backend teenuse.
12. Frontendi paistab välja ainult oauth-gateway poolt loodud cookie sessiooni identifikaatoriga.
13. Küsides andmeid TJT backend teenustest, teeb frontend päringu oauth-gateway poole koos sessiooni cookie-ga. oauth-gateway vahetab sessiooni cookie GOV SSO access tokeni vastu ning edastab päringu TJT backend teenustesse.
14. Kõik TJT backend teenused valideerivad access tokeni valiidsust, kontrollides kehtivust ja sertifikaati (samamoodi nagu praeguse TEHIK SSO lahenduse puhul).
15. Kui kasutaja on varasemalt TTO süsteemis GOV SSO-ga sisse loginud, siis TJT-d avades suunatakse kasutaja GOV SSO lehele, kus tuvastatakse kehtiv sessioon ja suunatakse tagasi oauth-gateway teenusesse, kus salvestatakse access ja refresh tokenid cache-i ning genereeritakse sessiooni cookie.
16. Kasutajate väljalogimine (k.a back channel logout) toimub läbi oauth-gateway, mille käigus kustutakse antud kasutajate andmed (access token, session, id token, refresh token), mis keelab TJT edasist kasutamist.
17. Arhitektuur
18. Info arhitektuuri kohta - <https://wiki.sm.ee/spaces/TJT/pages/221496170/Dokumentatsioon+Arhitektuur+ja+tehniline+lahendus>
19. Funktsionaalsus ja testimise skoop
20. GOVSSO ja OAuth BFF lahendus, mille spetsifikatsioon on kirjeldatud siin - <https://wiki.sm.ee/spaces/TJT/pages/334073535/GovSSO+ja+OAuth+BFF+lahendus>

# **Teenuse kirjeldus**

* 1. Tellimuse eesmärgiks on tellija poolt tellitavate, olemasolevate ja valitud infosüsteemide turvalisuse testimine OWASP (Open Web Application Security Project) ASVS (Application Security Verification Standard) versioon 3.0.1 (või juhul kui sõlmitava raamlepingu kehtivuse perioodil peaks eksisteerima uuem versioon, siis uuemale) tasemetele 2 ja 3 vastavate turvatestide teostamine.
  2. Turvatestimise käigus tuleb metoodiliselt testida ja hinnata kõiki potentsiaalseid turvavigu (sealhulgas OWASP Top Ten) ning need tuleb testiraportis detailselt välja tuua koos võimalike lahenduste ja soovitustega, st leitud vigade puhul välja tuua võimalikud ohustsenaariumid.
  3. Testimisel tuleb kontrollida, et testitavate infosüsteemide võimalike haavatavuste kaudu ei oleks võimalik juurde pääseda andmetele, mis asuvad väljaspool testitava rakenduse funktsionaalsust. Testimine hõlmab ka kasutajate horisontaalset ja vertikaalset õiguste ületamise turvatestimist.
  4. Kõik testimised ja lähtekoodi kontrollid tuleb teostada ka käsitsi, sest testitavad süsteemid ei pruugi automaatsete vahenditega testimisel tõepäraseid tulemusi anda. Testimise lõppedes edastab täitja testitavate toodete/lahenduste testiraportid, krüpteerituna tellijale.
  5. Turvatestimised viiakse läbi arendus- või testkeskkondades, kui ei ole kokku lepitud teisiti. Vajadusel luuakse tellija ja testija süsteemide vahele turvatud kanal infosüsteemidele ligipääsemiseks.
  6. Testimise läbiviimiseks peab täitja esitama tellijale IP aadressid, millelt hakatakse turvateste läbi viima. Tellija avab ligipääsu vastavatelt IP aadressidelt testitavatele süsteemidele. Vajadusel teeb tellija ka vajalikud testkasutajad.
  7. Lõppraport tuleb vormistada vastavalt OWASP ASVS reeglitele.

# **Töö tulemid ja tähtajad**

* 1. Tööd on teostatud ja dokumenteeritud vastavalt nõuetele, vt. 3 Teenuse kirjeldus.
  2. Rakenduse veebiliideses ei ole üldtuntud turvaauke, mis võimaldaksid välisel ründajal rakendusse sisse murda ja teha selles volitamata tegevusi.
  3. Täitja ja tellija on tugisüsteemina kasutanud tellija kasutuses olevat projektihaldustarkvara vastavalt kokkulepetele.
  4. Täitja on täitnud tööaja arvestust.
  5. *Turvatestimine toimub I etapis peale eeltegevuste teostamist.*
     1. *Turvastestimise tööde tähtaeg on 2.05.2025 .*
     2. *Turvatestimine viiakse läbi alates 7.04.2025 ning kestab kuni 2.05.2025 (kestus).*
        1. *Lõplik turvatestimise periood lepingu sõlmimisest on kuni 8 töönädalat, misjärel akteeritakse tehtud tööd.*
        2. *Turvatestimisele järgneb tuvastatud vigade paranduste teostamine tellija poolt, mille järel peab täitja teostama parandustele üle testimise kuni 1,5 kuu jooksul, misjärel akteeritakse tehtud tööd.*
        3. *Juhul, kui hankelepingut ei sõlmita enne 7.04.205, siis lükkub hankelepingu hilisema sõlmimise võrra tööde teostamise periood edasi.*