

Lisa 1 - Tehniline kirjeldus

Sisukord

I.	SKAIS1 arhitektuuridokument	2
1.	Sissejuhatus	2
2.	Süsteemi taust	2
3.	SKAIS1 komponentdiagramm	2
4.	Majutatavad teenuse komponendid	3
5.	Välised liidestused	3
6.	Süsteemi arhitektuuris kasutatavad tehnoloogiad/tarkvarad	3
7.	Tehnoloogia maatriks	4
8.	Teenuse tehniline kirjeldus	4
9.	Lokatsioonide näitlik loogiline arhitektuur	8
II.	SKAIS2 arhitektuuridokument	9
1.	Sissejuhatus	9
2.	Süsteemi taust	9
3.	Paigaldusvaade	9
4.	Rajadokument	14
5.	Süsteemi arhitektuuris kasutatavad tehnoloogiad	21
6.	Tehnoloogiate maatriks	21
7.	Tuleviku visioon	23
8.	Teenuse tehniline kirjeldus	23
III.	STAR arhitektuuridokument	29
1.	Sissejuhatus	29
2.	Süsteemi taust	29
3.	STAR komponentdiagramm	29
4.	Majutatavad teenuse komponendid	30
5.	Välised liidestused	31
6.	Süsteemi arhitektuuris kasutatavad tehnoloogiad/tarkvarad	31
7.	STAR2 ametniku rakenduse arhitektuur – mikroteenused	31
8.	Teenuse tehniline kirjeldus	33
9.	Nõuded mikroteenuste arhitektuuri tehnilisele ülesehitusele	38
10.	Toodangukeskkonna näitlik arhitektuur	38
IV.	Lisad	40
1.	Tehnilise kirjelduse lisad on:	40

I. SKAIS1 arhitektuuridokument

1. Sissejuhatus

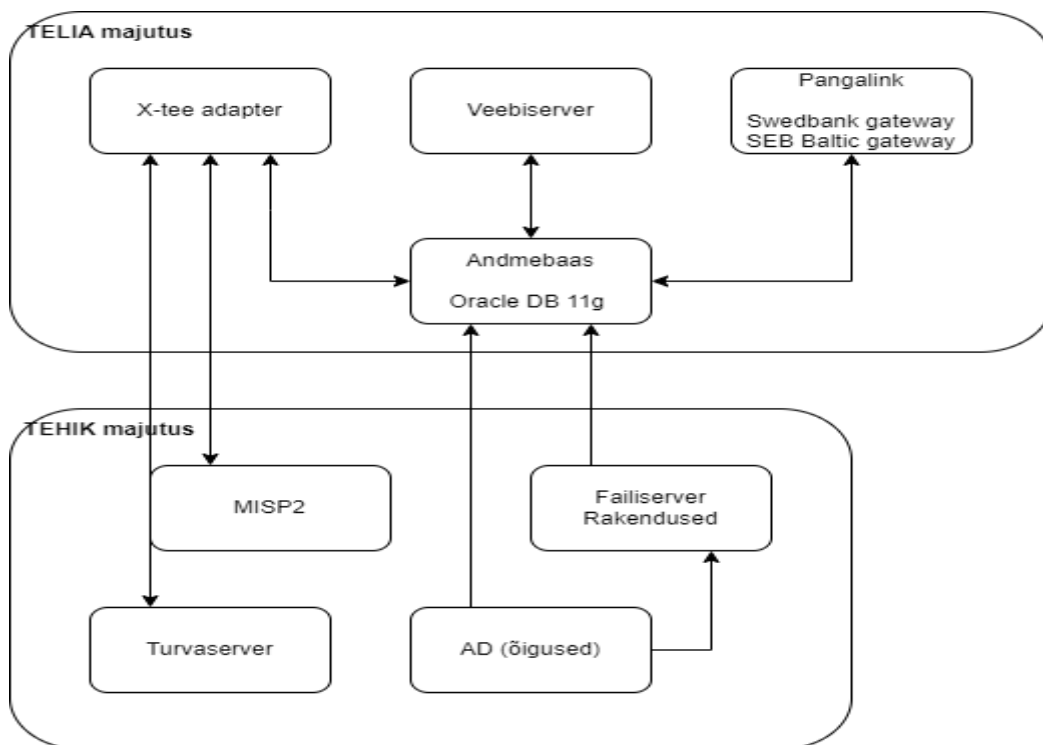
- 1.1. Antud dokument kirjeldab SKAIS1 infosüsteemi arhitektuuri, sisaldades antud süsteemi komponentide kirjeldust, nende omavahelist suhtlemist, paigaldusvaadet ning kirjeldust süsteemi ning teda ümbritsevate keskkondade vahel.

2. Süsteemi taust

- 2.1. Sotsiaalkindlustusameti infosüsteem (SKAIS) on riigi infosüsteemi kuuluv andmekogu, mida peetakse seadustest tulenevate Sotsiaalkindlustusameti avalike ülesannete täitmise eesmärgil. Täna kasutusel olev SKAIS koosneb tehniliselt neljast alaminfosüsteemist - SKAIS1, SKAIS2 ja EBS, mis moodustava omavahel kokkuseotuna ühe loogilise terviku ja mida vaadeldakse ühe tervikliku infosüsteemina.
- 2.2. SKAIS1 on liidestatud erinevate üleriigiliste infosüsteemidega. Andmebaasis on 3,4 miljoni isiku andmed.
- 2.3. Infosüsteemi SKAIS1 majutuskeskkond koosneb kolmest (test-, pre-live ja live keskkond) võrgu tasemele teineteisest lahusolevast keskkonnast. Kõiki keskkonnad on üles ehitatud sarnase arhitektuuri ja komponentidega va. testkeskkond, millel puudub vajadus teise dubleeriva öla järele. Allpool dokumendis on komponentide tasemel piisava detailsusega lahti kirjutatud SKAIS1 loogiline arhitektuuriline ülesehitus kirjeldamaks praeguse süsteemi toimimist ja võimaldamaks jätkusuutlikku arengut tulenevalt Sotsiaalkindlustusameti arenduse soovidest.

3. SKAIS1 komponentdiagramm

- 3.1. Järgnev skeem kirjeldab SKAIS1 infosüsteemis paiknevaid komponente ning nende vahelist suhtlust:



- 3.2. **Veebiportaal** (siseveeb) – Sotsiaalkindlustusameti ametnikele mõeldud veebirakendus, ligipääsetav ainult sisevõrgust.
- 3.3. **MISP2** – Veebirakendus, sisaldab sealhulgas Teenuseosutaja portaali.

- 3.4. **Turvaserver** – Liidestus X-Teega (asub füüsiliselt TEHIKus).
- 3.5. **Adapterserver** – Vahekomponent x-tee turvaserveri ja andmebaasi vahel.
- 3.6. **Andmebaas** – Oracle Database Enterprise Edition, SKAIS1 andmestik.

4. Majutatavad teenuse komponendid

- 4.1. Andmebaas
 - 4.1.1. Oracle Database 11g Enterprise Edition.
- 4.2. Veebiportaal (siseveeb)
 - 4.2.1. Sotsiaalkindlustusameti ametnikele mõeldud veebirakendused
 - 4.2.2. Tüüp: teenuseid pakkuv veebilehekülg
 - 4.2.3. Kasutatud protokoll: sisevõrgu veebileht, https
 - 4.2.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.
- 4.3. Adapterserver
 - 4.3.1. Kasutatakse x-tee teenuste vahendamiseks x-teele (ka MISP2 ja eesti.ee)
 - 4.3.2. Tüüp: sünkroonne ja asünkroonne teenus; süsteemne taustprotsess
 - 4.3.3. Kasutatud protokoll: integreeritud süsteemi osa
- 4.4. Digitempel
 - 4.4.1. Füüsiline krüptopulk pangalinkides maksefailide allkirjastamiseks/krüpteerimiseks.
 - 4.4.2. Tüüp: Daemon protsess
 - 4.4.3. Kasutatud protokoll: jdbc; https; PKCS11
- 4.5. Pangalink
 - 4.5.1. Pankadega andmevahetuse server.
 - 4.5.2. Tüüp: Daemon protsess
 - 4.5.3. Kasutused Swedbank ja SEB standard gateway tarkvara

5. Välised liidestused

- 5.1. Eesti.ee riigiportaal
 - 5.1.1. Pakutakse 16 avalikku veebiteenust
- 5.2. Sertifitseerimiskeskus
 - 5.2.1. digiallkirjade kehtivuskinnitus
 - 5.2.2. Tüüp: sünkroonne teenus
- 5.3. EESSI
 - 5.3.1. EL pädevate asutustevaheline andmevahetuskeskkond.
- 5.4. Pank
 - 5.4.1. Väljamaksete edastamine panka
 - 5.4.2. Tüüp: asünkroonne gateway
 - 5.4.3. Kasutatud protokoll: SOAP
- 5.5. X-tee
 - 5.5.1. Erinevate andmekogudega suhtlus
 - 5.5.2. SKAIS1 poolt x-teel pakutavaid erinevaid teenuseid on 67;
 - 5.5.3. SKAIS1 poolt x-teel tarbitavad erinevaid teenuseid on 82;
 - 5.5.4. Tüüp: sünkroonne/asünkroonne
 - 5.5.5. Kasutatud protokoll: SOAP

6. Süsteemi arhitektuuris kasutatavad tehnoloogiad/tarkvarad

- 6.1. Serverite operatsioonisüsteem
 - 6.1.1. Serverite operatsioonisüsteemi tarkvarad peavad olema kaetud tootjapoolse tarkvaratoega lepingu perioodi vältel.
 - 6.1.2. Operatsioonisüsteem: Red Hat Enterprise Linux 7 (RHEL) / Oracle Enterprise Linux 7 (OEL).
 - 6.1.3. Vajalikud litsentsid tagab Taitja.
- 6.2. Apache HTTP Server Versioon: 2.4.37

- 6.2.1. Konfiguratsioon ja nõuded: SSL, ID-Kaardi sertifikaadi tuvastamine (ssl konfiguratsioon).
- 6.2.2. Operatsioonisüsteem: Red Hat Enterprise Linux 7 (RHEL)
- 6.2.3. Vajalikud SSL sertifikaadid tagab Tellija.
- 6.3. Apache Tomcat Versioon: 9.0.82
 - 6.3.1. Konfiguratsioon ja nõuded: -
 - 6.3.2. Operatsioonisüsteem: Red Hat Enterprise Linux 7 (RHEL)
- 6.4. Oracle Database Enterprise Edition 11g Versioon: Oracle Database 11g Enterprise Edition 11.2.0.4.
 - 6.4.1. Konfiguratsioon ja nõuded: klasterdatud andmebaas.
 - 6.4.2. Operatsioonisüsteem: Oracle Enterprise Linux 7 (OEL).
 - 6.4.3. Andmebaasi eeldatav stardimaht (täna olemasolev andmestik) 1TB
 - 6.4.4. Tellija tagab 8 (kaheksa) Oracle Database Enterprise CPU litsentsi. Süsteemi arengust tingitud vajaduse korral tagab lisalitsentsid Tellija.
- 6.5. Oracle Partitioning
 - 6.5.1. Kasutatakse SKAIS1 Oracle andmebaasi partitsioneerimiseks.
 - 6.5.2. Tellija tagab 8 (kaheksa) litsentsi. Süsteemi arengust tingitud vajaduse korral tagab lisa-litsentsid Tellija.
- 6.6. IBM Websphere Application Server Community Edition Versioon: 2.1.1.6 Veebiteenuste server.
- 6.7. Konfiguratsioon ja nõuded:-
- 6.8. Operatsioonisüsteem: CentOS 5.8

7. Tehnoloogia maatriks

Rakendus	Java 8	SOAP	Apache Tomcat 6.x	Oracle 11g EE	Märkus
Veebirakendused	x	x	x		
SafeNet eToken	x				
X-tee adapter	x	x	x		
X-tee turvaserver		x			
Andmebaas				x	

8. Teenuse tehniline kirjeldus

- 8.1. Nõuded serveriruumile ja infrastruktuurile
 - 8.1.1. Täitja majutab Tellija infosüsteemi kahes füüsiliselt eraldi asukohas ja eraldi aadressidel paiknevas serveriruumis. Serveriruumid ja nendevahelised ühendused peavad paiknema Eesti Vabariigi territooriumil ja serveriruumide minimaalne nõutud geograafiline vahemaa on vähemalt 1 km.
 - 8.1.2. Serveriruumid peavad olema spetsiaalselt ehitatud serverite majutuseks ja vastama E-ITS turbeastmele H ning standardile ANSI/TIA-942 (Telecommunications Infrastructure Standard for Data Centers) tasemele Tier 3, mõõndusega, et varugeneraator ei pea olema dubleeritud.
 - 8.1.3. Täitja tagab SKAIS1 infosüsteemile turvatud (SSL) välise andmesideühenduse kiirusega vähemalt 100 Mbps (megabitti sekundis) ja serveriruumide vahel füüsilise, turvatud (VPN) dubleeritud ühenduse kiirusega vähemalt 1 Gbps (gigabitti sekundis).
 - 8.1.4. Andmesideühenduse (internetiteenuse) täitja peab olema Eesti Interneti SA poolt akrediteeritud.
 - 8.1.5. Serverite ja serveriruumide vaheline ühenduse kiirus peab olema piisav, et tagada teenustaseme nõuded. Tõrke korral peab olema tagatud teenuste üle viimine teise serveriruumi teenuse nõuetele vastava aja jooksul.

- 8.1.6. Täitja serveriruumid peavad olema ühendatud tellija serveriruumidega läbi VPN ühenduse kiirusega vähemalt 1Gb/s. Tellija serveriruumid asuvad serverimajutuskeskustes kahes erinevas lokatsioonis Eesti Vabariigis.
- 8.1.7. Täitja peab kasutama riistvara, millel töötab ainult Tellija infosüsteem. Pakutaval riistvaral ei tohi töötada samal ajal kolmandate osapoolte infosüsteemid. Samuti ei tohi olla kolmandatel osapooltel ligipääse pakutavale riistvarale ja operatsioonisüsteemile.
- 8.2. SKAIS1 infosüsteemi majutus- ja tugiteenuste üldised (miinimum) nõuded
- 8.2.1. Täitja kohustub tagama SKAIS1 infosüsteemi kasutamise võimaluse veebikeskkonnas ning lepingu kehtivuse perioodil kindlustama keskkondade nõuetekohase (hankedokumentis ja teenusepassis kirjeldatud) funktsioneerimise.
- 8.2.2. Täitja tagab SKAIS1 infosüsteemi järgmised majutus- ja tugiteenused:
- 8.2.2.1. Serverite, võrgu- ja salvestusseadmete ressursid.
 - 8.2.2.2. Andmebaaside administreerimine ja monitooring.
 - 8.2.2.3. Infrastruktuuri administreerimine ja monitooring.
 - 8.2.2.4. Muudatuste haldus.
 - 8.2.2.5. Konsultatsioonid ja parendusettepanekud.
 - 8.2.2.6. Muud ühekordsed tegevused ehk lisatööd.
 - 8.2.2.7. Teenuse lõpetamisega seotud tööd lepingu lõppemisel.
- 8.2.3. Infosüsteem peab olema majutatud kahes serveriruumis põhimõttel primary site ja failover site. Täitja peab kirjeldama, mis vahenditega tagatakse vajaduse korral teenuste üle viimine teise serveriruumi vastavalt käideldavusnõuetele.
- 8.2.4. SKAIS1 infosüsteemi Oracle andmebaaside vaheliseks andmete reaajas sünkroniseerimiseks peab Täitja kasutama Oracle Data Guard tarkvara. Oracle Active Data Guard tarkvara võetakse kasutusele vajadusepõhiselt, mille kasutuselevõtu tingimused lepatakse eraldi kokku teenuseosutajaga.
- 8.2.5. Lepingu lõppedes kooskõlastatakse andmete uude majutuskeskkonda migreerimise ja seejärel hävitamise protsess Tellija ja Täitja vahel. Andmete ülekolimise ja hävitamise järgselt vormistab majutusteenuse osutaja akti, millega kinnitatakse, et andmed on hävitatud.
- 8.2.6. Teenuse osutaja vahetumisel vormistatakse andmete ülekolimise (migratsiooni) läbiviimise järgselt kolmepoolne üleandmis-vastuvõtu akt (andja, vastuvõtja, omanik).
- 8.2.7. Teenuse lõppedes, uude keskkonda andmete migratsiooni ettevalmistamine ja läbiviimisel abi osutamine (Täitja pädevuse ulatuses) on majutusteenuse osa ja ei ole eraldi tasustatav.
- 8.3. Nõuded andmete hoidmisele
- 8.3.1. Kõik infosüsteemis töödeldavad andmed (andmebaasis ja rakendusserverites) peavad paiknema keskses andmesalvestusmassiivis, mille andmemahut on lihtsasti juurde tellitav. Andmesalvestusmassiiv peab võimaldama andmete kloonimist töökeskkonnast töökeskkonna-eelsesse ja testkeskkonda. Andmesalvestusmassiivi mis tahes komponendi rike ei tohi põhjustada andmekadu.
- 8.3.2. Täitja peab maandama andmesalvestusmassiivi riknemise riski, mis võib Tellijale tähendada ulatuslikku teenusekatkestust. Täitja kirjeldab pakkumuses, kuidas ja mis vahenditega (sh SAN seadmed ja andmesalvestusmassiivid) on tagatud mainitud riskide maandamine.
- 8.4. X-tee turvaserverid
- 8.4.1. SKAIS1 infosüsteemis on kasutusel x-tee versioon 6 raamistik.
- 8.4.2. X-tee turvaserverite töökeskkonna, toodangueelse keskkonna ja testkeskkonna tagab Tellija (asuvad Tellija juures).
- 8.4.3. Infosüsteemi osade ühtlustamise ja edasiarenduste raames peab Täitjal olema valmidus x-tee turvaserveri majutus- ja haldusteenuse osutamiseks sarnaselt SKAIS2 alaminfosüsteemile.

8.5. Muudatuste haldus

- 8.5.1. Arendusmuudatuste paigalduse õigus on ainult Täitjal, kui ei lepita kokku teisiti.
- 8.5.2. Arendusmuudatused valmistab ette Arendaja ja edastab paketeeritult koos paigaldusjuhendiga paigaldamiseks toodangu- ja toodangueelsesse keskkonda. Paigalduspakettide, juhendite jm vajaliku informatsiooni edastamiseks ja paigaldustega seotud tegevuste dokumenteerimiseks, kasutatakse Tellija tööde/projektide juhtimise keskkonda Jira.
- 8.5.3. Teenusetäitja paigaldab arendusmuudatusi lepingu raames vastavalt teenuse passile.
- 8.5.4. Toodangukeskkonda ja toodangueelsesse keskkonda tehakse üldjuhul kuni 4 arendusmuudatuse tarnet ja 4 veaparandustarnet kuus. Testkeskkonda tehakse üldjuhul kuni 12 arendusmuudatuse tarnet ja 12 veaparandustarnet kuus. Arendusmuudatusi töökeskkonda viiakse sisse väljaspool aktiivset tööaega.
- 8.5.5. Teenusetäitja peab vastavalt tellimusele käivitama parandusskripte vigade tuvastamiseks ja parandamiseks.
- 8.5.6. Arendusmuudatuste paigalduse aja kooskõlastab Täitja Tellijaga.
- 8.5.7. Täitja poolt arendusmuudatuse paigalduse ebaõnnestumisel vastutab Täitja süsteemi taastamise (rollback) eest.
- 8.5.8. Täitja uuendab toodangueelse ja testkeskkonna andmeid toodangukeskkonna andmetega Tellija tellimusel kui tarnejuhend seda ette näeb, kuid mitte rohkem kui punktis 10.5.4 kirjeldatud tarnete arv.
- 8.5.9. Teenusetäitja tagab Tellija tellimisel arenduspartneritele ligipääsu test- ja toodangueelsele keskkonnale (andmebaasile, rakendusserverile) 2 tööpäeva jooksul.
- 8.5.10. Teenusetäitja tagab Tellija tellimisel arenduspartneritele ligipääsu sulgemise test- ja toodangueelsele keskkonnale esimesel võimalusel, kuid mitte hiljem kui 2 tööpäeva jooksul.
- 8.5.11. Täitja peab kindlustama Tellija tellimisel (andme)halduritele / rakenduse administraatoritele lugemisõigustes (read only) ligipääsud kõikide SKAIS2 keskkondade serverite operatsioonisüsteemi konfiguratsioonifailidele ja andmebaasidele.

8.6. Varundamine ja teenuse taastamine

- 8.6.1. Täitja teeb majutuskeskkonnas olevatest süsteemidest regulaarselt varukoopiaid selliselt, et oleks tagatud teenuse passis sätestatud tingimuste täitmine. Täitja peab pakkumises kirjeldama, et milliste vahendite ja meetoditega tehakse varukoopiaid.
- 8.6.2. Varukoopiaid tehakse rakendusi seiskamata st, et Tellija infosüsteemide käideldavus ei ole varukoopiate tegemise ajal mõjutatud. Varundust teostatakse väljaspool infosüsteemi tööaega.
- 8.6.3. Varukoopiad tuleb salvestada töökeskkonnast eraldi asuvatele andmekandjatele, mis asuvad erinevas füüsilises lokatsioonis. Varukoopiad ja nende allika vaheline andmevahetus peab olema krüpteeritud.
- 8.6.4. Täitja on kohustatud hoidma töökeskkonna varundatud andmeid järgnevalt:
 - 8.6.4.1. Vähemalt kahe viimase kuukoopia.
 - 8.6.4.2. Vähemalt neli viimast nädalakoopiat.
 - 8.6.4.3. Vähemalt viis viimast tööpäevakoopiat.
- 8.6.5. Kuukoopiad on planeeritud kopeerida täiendavalt andmesaatkonda. Ajakava ning täpne tehniline lahendus töötatakse välja ja realiseeritakse koos eduka Täitjaga töö käigus 2020/21.aastal.
- 8.6.6. Andmekadu põhjustavat intsidenti käsitletakse kui erakorralist intsidenti. Erakorralise intsidendi korral on lubatud teenuse järjestikune seisak kuni 4 tundi ja summaarne seisak kuni 4 tundi nädalas ja kuni 6 tundi kalendrikuus. Pärast intsidendi lahendamist ja/või andmete taastamist esitab Täitja Tellijale detailse raporti, kus toob välja intsidendi põhjuse, mis põhjustas andmekadu ning meetmed selliste juhtumite vältimiseks või esinemise tõenäosuse vähendamiseks tulevikus.

8.6.7. Täitja töötab pärast iga keskkonna käivitamist ühe kuu jooksul välja vastava keskkonna taasteplaani ja esitab selle Tellijale ülevaatamiseks ja kinnitamiseks. Taasteplaani peab sisaldama tegevuskava ja süsteemi üldist arhitektuuri kirjeldust visuaalsel kujul. Olulised infrastruktuuri komponendid (serverid, võrguseadmed jne) peavad olema kirjalikult lahti seletatud.

8.6.8. Täitja testib taasteplaani ajakohasust, kui toimub muudatus Tellija infosüsteemiga seotud infrastruktuuris, kuid mitte harvemini kui üks kord aastas. Täitja kooskõlastab Tellijaga testi läbiviimise aja ning esitab Tellijale pärast testi läbiviimist raporti, kus märgib ära taasteplaani vastavuse tegelikule olukorrale ja plaanist leitud puudused. Puudused tuleb kõrvaldada Tellijaga kokkuleppel mõistliku aja jooksul ning seejärel korraldada uus taasteplaani test.

8.7. Monitooring

8.7.1. Täitja tagab tsentraliseeritud tehnilise toe teenuse, mis on avatud 24 tundi ööpäevas ja seitse päeva nädalas, mille kaudu sooritatakse mitmesuguseid süsteemiga seotud järelevalve, muudatuste ja veahalduse menetlustoiminguid.

8.7.2. Tehnilise toe teenuseid osutatakse osana majutusteenustest, kus kõik süsteemihoiatused saadetakse tsentraliseeritud 24 tundi toimivale tehnilisele toele (sh võrgu, serveri ja rakenduse hoiatused).

8.7.3. Kõik keskkonnad peavad olema Täitja poolt monitooritud kogu lepinguperioodi vältel.

8.7.4. Täitja võimaldab Tellijale ja Tellija poolt nimetatud arendajale juurdepääsu monitooringuinfole või edastab monitooringuteated Tellija poolt etteantud meiliaadressile.

8.7.5. Täitja installeerib vajadusel või Tellija palvel serveritesse täiendavad monitooringuagendid, mis koguvad infot serverite ja rakenduste seisundi kohta. Tellijal on kasutusel monitooringu süsteem Prometheus ja Grafana.

8.7.6. Täitja monitoorib serverites asuvate infosüsteemide tööd vähemalt järgmiste komponentide osas:

8.7.6.1. Andmesideühenduse olemasolu Tellija serverite ja infosüsteemide vahel.

8.7.6.2. Serverite riistvaraliste komponentide töökorras olek.

8.7.6.3. Serverite protsessorite ja mälu kasutus.

8.7.6.4. Kõvaketaste täituvus.

8.7.6.5. Süsteemi load (UNIX süsteemide puhul).

8.7.6.6. Andmebaasisüsteemi töökorras olek.

8.7.6.7. Andmebaasile eraldatud ressursside olemasolu.

8.7.6.8. Varukoopiate tegemise õnnestumine.

8.7.6.9. Monitooringusüsteemi töökorras olek.

8.7.7. SKAIS1 infosüsteemi rakenduste monitooring

8.7.7.1. Täitja poolset SKAIS1 rakenduse monitooringut ei nõuta. Täitjal peab olema valmisolek integreerida oma keskkonda Tellija poolt kasutatavad rakenduse monitooringu vahendid (agendid vms).

8.7.8. Teenuse tehniline tugi

8.7.8.1. Täitja peab tagama kasutajatoe (ühtne kontaktpunkt, telefoni number, e-mail ja/või avalik portaal) vastavalt Teenuse passis toodud nõuetele.

8.7.8.2. Täitja peab teavitama Tellijat kriitilistest ja keskmise taseme vigadest koheselt ja asuma teenuse nõutud tingimustele vastavust taastama.

8.7.8.3. Kui tõrget ei ole võimalik teenuse passis nõutud aja jooksul lahendada, peab Täitja esitama põhjendused ja lahendustettepanekud.

8.7.8.4. Kriitilise taseme tõrkeks loetakse olukorda, kus SKAIS1 toodangukeskkonna tervikuna või oluliste komponentide, sh andmevahetused teiste infosüsteemidega, kasutamine ei ole võimalik.

8.7.8.5. Keskmise taseme tõrkeks loetakse olukorda, kus SKAIS1 toodangukeskkonna kasutamine on oluliselt häiritud.

8.7.8.6. Madala taseme tõrkeks loetakse olukorda, kus SKAIS₁ toodangukeskkonna kasutamine on võimalik, kuid on häiritud.

8.7.9. Aruandlus ja infovahetus

8.7.9.1. Taitja esitab majutusteenuse osutamise kohta igakuiselt ülevaate eelmise kuu kohta, mis sisaldab vähemalt järgmist informatsiooni:

8.7.9.1.1. Süsteemi komponentide käideldavus vastavalt teenuste passi nõuetele.

8.7.9.1.2. Perioodi vältel toimunud intsidendid koos algus- ja lõpuajaga, juurpõhjusega (kui on selgunud) ning kirjeldusega, kuidas neid edaspidi vältida.

8.7.9.1.3. Perioodi vältel tehtud plaanilised tööd.

8.7.9.1.4. Muudatuste logi.

8.7.9.1.5. Tellija poolt perioodi jooksul esitatud pöördumiste staatus, mis sisaldab ka lahendamata pöördumisi eelmistest perioodidest.

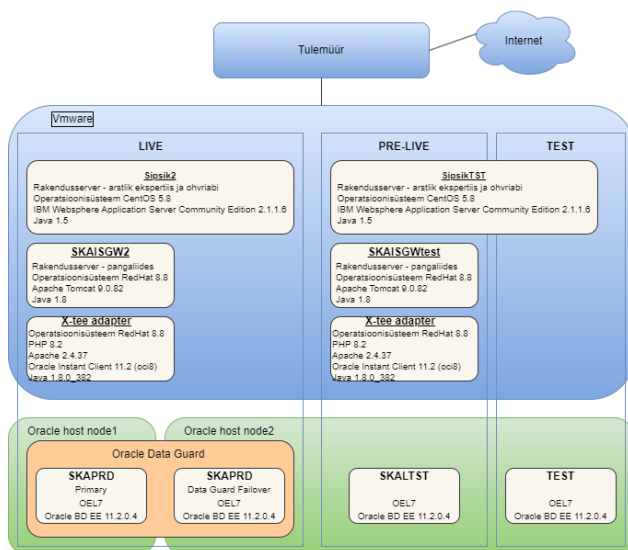
8.7.9.1.6. Taitja poolsed ettepanekud infosüsteemi ja majutuse parendamiseks ning teostamiskava.

8.7.9.2. Aruandlus peab olema Tellija kontaktisikutele kättesaadavaks tehtud veebi kaudu või e-kirja teel.

8.7.9.3. Taitja peab võimaldama Tellijal tellida tellimustööna täiendava tasu eest ühekordseid raporteid nt andmebaasi detailseid koormusraporteid.

8.7.9.4. Taitja ja Tellija vaheline töökeel on eesti keel.

9. Lokatsioonide näitlik loogiline arhitektuur



II. SKAIS2 arhitektuuridokument

1. Sissejuhatus

- 1.1. Antud dokument kirjeldab juba valminud SKAIS2 infosüsteemi arhitektuuri, sisaldades antud süsteemi komponentide kirjeldust, omavahelist suhtlemist ja suhestumist, paigaldusvaadet ning kirjeldust loodava süsteemi ning teda ümbritsevate keskkondade vahel.

2. Süsteemi taust

- 2.1. Sotsiaalkindlustusameti infosüsteem (SKAIS2) on riigi infosüsteemi kuuluv andmekogu. Aastaks 2018 oli välja arendatud elatisabi ja riigile üle läinud elatisnõuete sissenõudmise; puude raskusastme ja puudest tulenevate lisakulude ning püsiva töövõimetuse tuvastamise funktsionaalsus.
- 2.2. Aastatel 2018–2020 lisandusid SKAIS2 infosüsteemi Pereküsitiste pakkumuste sündmuspõhine teenus, Tehniliste abivahendite taotlemise ja soodustingimustel eraldamise infosüsteem, Isa täiendava vanemahüvitise puhkuse planeerimise võimalus, Vanemahüvitiste- ning Kogumispensioni täiendavate sissemaksete funktsionaalsus.
- 2.3. Aastatel 2021–2023 lisandus Pensioniõigusliku staaži andmete kogumise teenus ja uuenesid Digitemeldamise -, Dokumentide haldamise -, Rahvastikuregistriga liidestumise – ja Arstliku-ekspertiisi teenused.
- 2.4. SKAIS2 on liidestatud erinevate üleriigiliste infosüsteemidega. Süsteemis on 1,6 miljoni isiku andmed.

3. Paigaldusvaade

- 3.1. Järgnevalt kirjeldatakse süsteemi komponentide paigaldust ja omavahelist suhtlust. Infosüsteem on laias laastus jagatud kaheks:
 - 3.1.1. sisevõrgus paiknevad süsteemi osad
 - 3.1.2. välisvõrgust ligipääsetavad süsteemi osad
- 3.2. Välisvõrgus asub Sotsiaalkindlustusameti iseteeninduse rakendus, mis suhtleb sisevõrgus olevate komponentidega üle standardse HTTPS protokolliga. Ligipääs sisevõrgus olevatele komponentidele on määratud välisvõrgus asuva serveri(te) IP aadressi(de) näol.
- 3.3. Rakendusserveritele (*Apache Tomcat*¹) paigaldatud komponendid (Ametniku portaali) on paljundatavad (hetkel kasutatav sessiooni *sticky-session* asendub tulevikus Redis² andmebaasil põhineva sessiooni haldusega). Süsteem võimaldab lisada N arv lisa servereid, koormust juhib rakendusserverite ette paigaldatud koormusjaotur Apache³ mod_proxy⁴.
- 3.4. Uuemad (pärast 2018 arendatud) komponendid on arendatud mikroteenuste⁵ põhimõtteid jälgides ning väldivad kasutaja sessiooni oleku hoidmist rakendusserveris. Valitud lahendus võimaldab rakenduse komponente paljundada ja lõppkasutajale märkamatu (katkestuste vabalt) vahetada.
- 3.5. Andmebaasi ühendusi hallatakse rakendusesisese *Connection Pooli* abil. Infosüsteem töötab läbivalt UTF-8 kodeeringus.
- 3.6. Süsteemi aluseks olev andmebaas on paigaldatud kahte erinevasse serveriruumi (*active/passive site*), kus ainult üks on aktiivses olekus.

¹ Apache Tomcat — <http://tomcat.apache.org/>

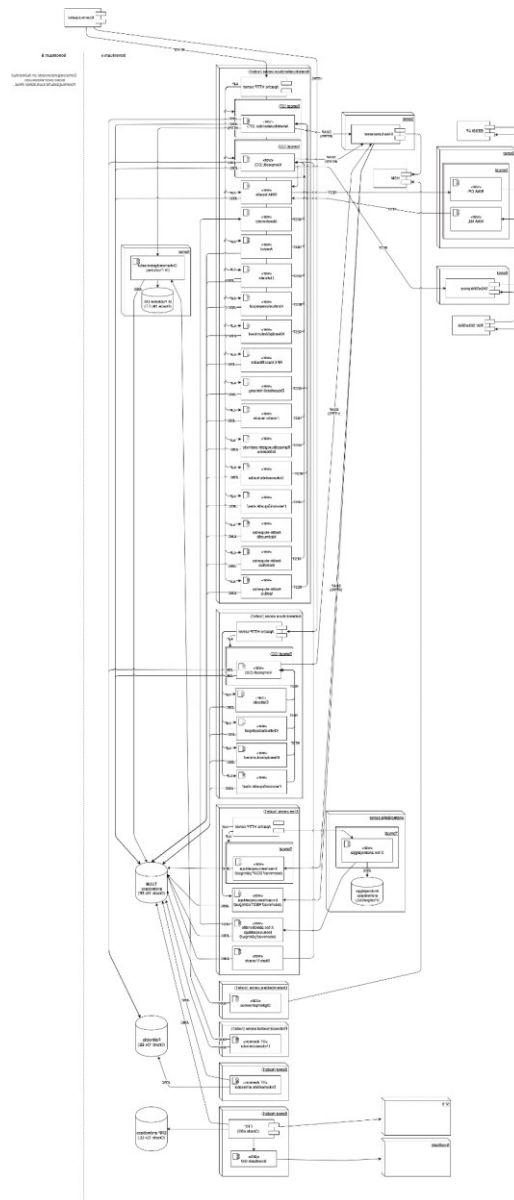
² Redis — <https://redis.io/>

³ Apache HTTP Server — <https://httpd.apache.org/>

⁴ mod_proxy — https://httpd.apache.org/docs/2.4/mod/mod_proxy.html

⁵ Mikroteenuste arhitektuur — <https://microservices.io/>

- 3.7. Java rakendused on klasterdatud 2 aktiivse õlga (*node*) vahel, mis on paigutatud erinevatesse serveriruumidesse (st. 1 õlg serveriruumi peale).
- 3.8. SKAIS2 integreerub erinevate väliste infosüsteemidega:
- 3.8.1. infovahetus teiste riigi andmekogudega toimub üle X-tee6 kasutades HTTP(S) REST ja SOAP 7 protokolle.
 - 3.8.2. Infovahetus SKAIS1-ga toimub üle andmebaasiühenduste (JDBC ja DBLink8)
 - 3.8.3. Euroopa Liidu ühtse sotsiaalkindlustuse infovahetus (EESSI9) käib läbi Sotsiaalkindlustusameti RINA rakenduse kasutades HTTP protokolle, vahetades REST sõnumeid.
 - 3.8.4. Väljamakseid teostatakse kasutades Eesti pankade poolt pakutavaid teenuseid.



3.8.5. Ametniku portaal – Sotsiaalkindlustusameti ametnikele mõeldud veebirakendus.

⁶ X-tee andmevahetuse platform — <https://www.x-tee.ee/home>

⁷ SOAP protokoll — <https://www.w3.org/TR/soap/>

⁸ Oracle Database Links: https://docs.oracle.com/cd/E18283_01/server.112/e17120/ds_conceptso02.htm

⁹ Electronic Exchange of Social Security Information — <https://ec.europa.eu/social/main.jsp?catId=869&langId=en>

- 3.8.6. **Komposiit** - ajutine veebirakendus, mis pakendab endas erinevate valdkondade mikroteenuseid (failihaldus, finants (arvestus), iseteenindus, isik, kogumispension, maksude deklareerimine, otsus/hüvitis, pakkumus, perehüvitis, parameeter, sotsiaalmaksu hüvitamine, teavitused, tööülesanded, universaalmenetlus, vanemahüvitis, x-tee väljuvad päringud). Ajutine lahendus kuni toodangus võetakse kasutusele *Kubernetes*¹⁰.
- 3.8.7. **RINA Facade** – EESSI RINA liidestus. Integratsiooni komponent. Vahendab EESSI RINA ja SKAIS2 vahelist suhtlust üleeuroopaliste sotsiaalkindlustuse juhtumite menetlemiseks SKAIS2 kaudu. Eraldi käivitav Java (*Spring Boot*¹¹) rakendus.
- 3.8.8. **Abivahendid** – Tehniliste abivahendite ärimoodul. Haldab riigi poolt toetatud, soodustingimustel teostatud, abivahendite tehingute registreerimisi ja neist tulenevaid äriprotsesse. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.9. **Arestid** – Kolmandate osapoolte (*kohtutäiturid*) poolt Sotsiaalkindlustusametile edastatud arestiaktide alusel kinnipidamiste teostamine ja haldus. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.10. **Elatisabi** – Elatisabi teenuse ärimoodul. Haldab riigi poolt pakutavaid Elatisabi teenuseid ja neist tulenevaid äriprotsesse. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.11. **Kindlustuslepingud** – Kindlustusandjate poolt riigile üleantud pensioni II samba lepingute haldusmoodul. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.12. **Kliendipöördumised** – Kliendipöördumiste ja -suhtluse ärimoodul. Kliendipöördumiste ärimoodulis hallatakse kogu kliendiga toimuvat suhtlust, kus suhtluse algatajaks võib olla nii klient kui ka Sotsiaalkindlustusameti töötaja. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.13. **RFK klassifikaator** – Rahvusvahelise funktsioneerimisvõime, vaeguste ja tervise klassifikatsiooni (ICF¹²) haldusmoodul. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.14. **Ekspertarsti hinnang** – Sotsiaaltoetuste aluseks olev, isiku puude - ja toimetuleku hindamise moodul. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.15. **Finants facade** – SKAIS1s määratud pensionite, toetuste ja hüvitiste finantsarvestuse teostamise integratsioonimoodul. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.16. **Rahvastikuregistri andmete töötlemine** – Rahvastikuregistriga liidestumise ja rahvastikuregistrist saadud andmete töölemise teenus. Vastutab rahvastikuregistriga liidestuste eest (*sh. Isikuandmete muudatused/ Isiku detailandmed/ Isiku viibimiskoht/ Isiku dokumendid*) . Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.17. **Dokumentide hoidla** – SKAIS2 põhiteenus isikuga seotud dokumentide hoidmiseks. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.18. **Pensioniõiguslik staaž** – Pensioni määramiseks alusandmete, Pensioniõiguslike staažide, kogumise ja haldamise moodul. Eraldi käivitav Java (*Spring Boot*) rakendus.

¹⁰ Kubernetes konteinerite orkestratsioon — <https://kubernetes.io/>

¹¹ *Spring Boot* Java rakenduste raamistik — <https://spring.io/projects/spring-boot>

¹² ICF (International Classification of Functioning, Disability and Health) - <https://www.who.int/standards/classifications/international-classification-of-functioning-disability-and-health>

- 3.8.19. **Arstlik-ekspertiis küsimustik** – Arstliku-ekspertiisi taotluse juures kasutatav küsimustiku haldamise moodul. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.20. **Arstlik-ekspertiis menetlus** – Arstliku-ekspertiisi menetlemise moodul (*hetkel kasutatakse puudeotsuste edastamiseks STAR-i süsteemi*). Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.21. **Arstlik-ekspertiis taotlus** – Arstliku-ekspertiisi taotlemise moodul. Antud mooduli kaudu saavad kodanikud esitada iseteenindusest puude hindamise ja sotsiaaltoetuste taotlusi. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.22. **Protsessimootor** - kasutatakse virtuaalmasinas eraldiseisva protsessina (*jar*). Teostab süsteemis defineeritud ja järjekorda seatud taustaprotsesside jooksutamist. Jõudluse tõstmiseks on võimalik paigaldada mitu protsessimootorit.
- 3.8.23. **Dokumendi generaator** - vahend (*Oracle BI Publisher*¹³) menetlusprotsesside käigus koostatavate dokumentide koostamiseks ja automaatseks genereerimiseks. Liidestatud teiste süsteemidega kasutades *Oracle BI Publisher Java Integration API*'t. BI Publisheri kasutus on tasapisi asendumas ärimoodulite endi sees genereeritud dokumentidega.
- 3.8.24. **X-tee turvaserver** – X-tee liidestus. Installeeritud vastavalt turvaserveri installeerimisjuhendile: http://x-road.ee/docs/est/turvaserveri_kasutusjuhend.pdf.
- 3.8.25. **X-tee andmejälgija** – X-tee andmejälgija liidestus. Installeeritud vastavalt andmejälgija paigaldamise juhendile: <https://github.com/e-gov/AJ/blob/master/doc/Rakendusjuhend.md#tarkvara-paigaldamine>
- 3.8.26. **HSM** - (*hardware security module*) riistvaraline turvamoodul PKI infrastruktuuris turvaliselt saladuste krüpteerimiseks ja signatuuride kinnitamiseks.
- 3.8.27. **X-tee teenusetäitja** - Installeeritud eraldiseisvana virtuaalmasinasse (*Apache + Tomcat*). Vahendab SKAIS2 poolt pakutavaid x-tee teenuseid välistele süsteemidele, mis on loodud kasutades SOAP protokollit. Liidestus X-Tee turvaserveriga, pakub andmeid.
- 3.8.28. **X-road teenusetäitja** - Vahendab SKAIS2 poolt pakutavaid x-tee teenuseid välistele süsteemidele, mis on loodud kasutades REST protokollit. Liidestus X-Tee turvaserveriga, pakub andmeid. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.29. **Abivahendite X-tee teenusetäitja** – Installeeritud eraldiseisvana virtuaalmasinasse Java (*Spring Boot*) rakendusena. Vahendab SKAIS2 pakutavaid abivahendite X-tee teenuste otspunkte. Liidestus X-tee turvaserveriga, pakub andmeid.
- 3.8.30. **"Tuum" Andmebaas** – Oracle Database 19c Enterprise Edition, hoitakse ja töödeldakse kogu SKAIS2 andmestikku. Kasutusel 36 schemat (*skais_assignment, skais_benefit, skais_client_inquiry, skais_dashboard, skais_disability_application, skais_disability_proceeding, skais_disability_question, skais_doctor_assessment, skais_document_management, skais_finance, skais_fin_facade, skais_funded_pension, skais_funded_pension_payments, skais_isik, skais_maintenance_allowance, skais_notification, skais_pakkumus, skais_parental_benefit, skais_pension_seniority, skais_perehyvitis, skais_population_reg_proc, skais_proceeding, skais_rfk_classifier, skais_rinafacade, skais_signing, skais_social_tax_benefit, skais_system,*

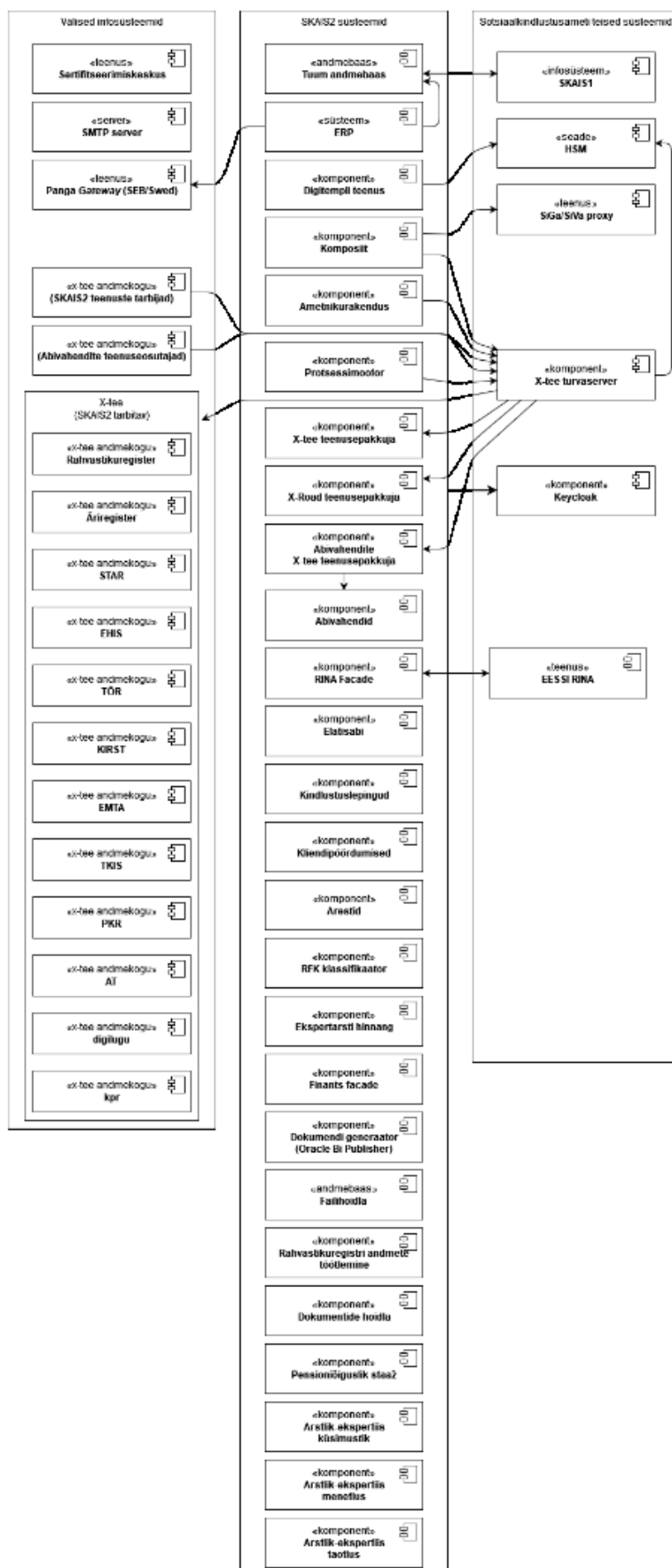
¹³ Oracle Business Intelligence Publisher — <https://www.oracle.com/middleware/technologies/bi-publisher.html>

skais_tax_declaration, skais_technicalaid, skais_technicalaidxroad, skais_withholdings, skais_xroad, skais_xroad_provider, skais2, skais2sys, skais2valine).

- 3.8.31. **Failihoidla** – *Oracle Database 19c Enterprise Edition* hoidmaks äriprotsesside poolt loodud ja süsteemi kasutajate poolt üleslaetud dokumente.
- 3.8.32. **Dokumentide arhivaator** – *Daemon* komponent (*jar*) operatiivbaasi salvestatud dokumentide liigutamiseks arhiivi (*failihoidla andmebaasi*).
- 3.8.33. **Digitempli teenus** – Äriteenuste poolt loodud otsuste ja maskefailide allkirjastamise (*digitembeldamise*) teenus. Allkirjastatud failid saavad asutuse digitempli ASiCe formaadis. Eraldi käivitav Java (*Spring Boot*) rakendus.
- 3.8.34. **ERP** - *Oracle E-Business Suite*¹⁴ paigaldatuna eraldi serverile. Haldab/töötleb SKAIS2 raamatupidamisinfot (maksed panka või muudesse maksekanalitesse (kojukanne), pangast tagasiside jne). ERPi taga on erinevad liidestused pankadega. SKAIS2 integratsioon ERPiga on tehtud läbi vahetabelite. Skais2 lisab read tabelitesse, kus ERP need üles korjab. Pärast tagasisidet pangast kirjutab ERP read tabelisse, kus SKAIS2 need jälle üles korjab ja oma ärilistesse tabelitesse laiali salvestab.
- 3.8.35. **Swedbank GW** – ERP Liidestus Swedbank'i maksete liidesega. Vahendab väljamaksete infot ERP ja Swedbank'i vahel.

¹⁴ *Oracle E-Business Suite* — <https://www.oracle.com/applications/ebusiness/>

4. Rajadokument



4.1. "Tuum" Andmebaas

- 4.1.1. Oracle Database 19c Enterprise Edition.
- 4.1.2. Tüüp: Andmebaas
- 4.1.3. Kasutatud protokoll: JDBC
- 4.1.4. Käideldavus: kõrgkäideldav active-passive klaster kahel ölal.

4.2. Iseteeninduse portaal (brauseri rakendus)

- 4.2.1. Sotsiaalkindlustusameti klientidele mõeldud veebirakendus.
- 4.2.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
- 4.2.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST).
- 4.2.4. Käideldavus: Brauseris töötav kasutajaliides.

4.3. Ametniku portaal

- 4.3.1. Sotsiaalkindlustusameti ametnikele mõeldud veebirakendus.
- 4.3.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
- 4.3.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST)
- 4.3.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.4. Elatisabi

- 4.4.1. Elatisabi teenuse ärimoodul
- 4.4.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
- 4.4.3. Kasutatud protokoll: HTTP(S) REST, Angular.
- 4.4.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.5. Kliendipöördumised

- 4.5.1. Kliendipöördumiste ja -suhtluse ärimoodul
- 4.5.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
- 4.5.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST)
- 4.5.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.6. Kindlustuslepingud

- 4.6.1. Kindlustusandjate poolt riigile üleantud pensioni II samba lepingute haldusmoodul
- 4.6.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
- 4.6.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST)
- 4.6.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.7. Arestid

- 4.7.1. Arestide (kinnipidamiste) teostamise ja halduse ärimoodul
- 4.7.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
- 4.7.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST)
- 4.7.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.8. RFK klassifikaator

- 4.8.1. Rahvusvahelise funktsioneerimisvõime, vaeguste ja tervise klassifikatsiooni haldusmoodul.
- 4.8.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
- 4.8.3. Kasutatud protokoll: AMQP, HTTP(S) (REST)
- 4.8.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.9. Ekspertarsti hinnang

- 4.9.1. Isiku puude - ja toimetuleku hindamise ärimoodul
- 4.9.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
- 4.9.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST)
- 4.9.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.10. Finants facade

- 4.10.1. SKAIS1s määratud pensionite, toetuste ja hüvitiste finantsarvestuse teostamise integratsioonimoodul.
- 4.10.2. Tüüp: sisemisi teenuseid pakkuv veebirakendus.

- 4.10.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST)
- 4.10.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.
- 4.11. **Komposiit**
 - 4.11.1. Ajutine mikroteenuse komponentide konteiner (Apache Tomcat)
 - 4.11.2. Tüüp: Avalike ja sisevõrgu teenuseid pakkuvate rakenduste konteiner.
 - 4.11.3. Kasutatud protokoll: HTTP(S) (REST)
- 4.12. **SiGa/SiVa proxy**
 - 4.12.1. TEHIKu sisene proxy teenus, mis vahendab RIA poolt pakutud SiGa/SiVa teenust.
 - 4.12.2. Tüüp: sisemisi teenuseid pakkuv veebirakendus.
 - 4.12.3. Kasutatud protokoll: HTTP(S) (REST)
 - 4.12.4. Käideldavus: k8s klastrisse ja koormusjaoturi taha paigaldatud mikroteenus.
- 4.13. **Protsessimootor**
 - 4.13.1. Kasutuses eraldiseisva protsessina virtuaalmasinas täitmaks süsteemis defineeritud ja järjekorda seatud taustaprotsesse või üle Oracle AQ saabunud sõnumeid. Töötab eraldiseisva(te) protsessi(de)na Daemon protsesside jooksutamiseks.
 - 4.13.2. Tüüp: sünkroonne ja asünkroonne teenus; süsteemne taustaprotsess.
 - 4.13.3. Kasutatud protokoll: AMQP, HTTP(S) (REST), JDBC
- 4.14. **Digitempli teenus**
 - 4.14.1. Digitembeldamise teenus, digitembeldab etteantud faile, lisab failid failihoidlasse. Sisemiselt kasutab digitembeldamise APIt. Signeerimiseks kasutab majutuskohas olevat võrgu HSM seadet.
 - 4.14.2. Tüüp: sisemisi teenuseid pakkuv veebirakendus.
 - 4.14.3. Kasutatud protokoll: AMQP, JDBC
 - 4.14.4. Käideldavus: klastrisse paigaldatud mikroteenus
- 4.15. **Failihoidla**
 - 4.15.1. Süsteem (Andmebaas + Java API) hoidmaks dokumendi generaatori poolt loodud, süsteemi kasutajate poolt üleslaetud ja protsessi mootori poolt loodud dokumente. Paigaldatud eraldiseisvasse virtuaalmasinasse.
 - 4.15.2. Tüüp: Teenus (API), Andmebaas.
 - 4.15.3. Kasutatud protokoll: JDBC; HTTPS
- 4.16. **Rahvastikuregistri andmete töötlemine**
 - 4.16.1. Rahvastikuregistri andmete pärimise ja töötlemise teenus
 - 4.16.2. Tüüp: sisemisi teenuseid pakkuv veebirakendus.
 - 4.16.3. Kasutatud protokoll: AMQP, HTTP(S) (REST), JDBC
 - 4.16.4. Käideldavus: klastrisse paigaldatud mikroteenus
- 4.17. **Dokumentide hoidla**
 - 4.17.1. Isikuga seotud dokumentide haldamise ärimoodul
 - 4.17.2. Tüüp: avalikke ja sisemisi teenuseid pakkuv veebirakendus.
 - 4.17.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST), JDBC
 - 4.17.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.
- 4.18. **Pensioniõiguslik staaž**
 - 4.18.1. Pensioniõiguslike staažide, kogumise ja haldamise ärimoodul
 - 4.18.2. Tüüp: avalikke ja sisemisi teenuseid pakkuv veebirakendus.
 - 4.18.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST), JDBC
 - 4.18.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.
- 4.19. **Arstlik-ekspertiis küsimustik**
 - 4.19.1. Arstliku-ekspertiisi taotluse juures kasutatav küsimustiku haldamise moodul
 - 4.19.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
 - 4.19.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST), JDBC
 - 4.19.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.20. Arstlik-ekspertiis menetlus

- 4.20.1. Arstliku-ekspertiisi menetlemise ärimoodul
- 4.20.2. Tüüp: sisemisi teenuseid pakkuv veebirakendus.
- 4.20.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST), JDBC
- 4.20.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.21. Arstlik-ekspertiis taotlus

- 4.21.1. Puude tuvastamise ja sotsiaaltoetuste taotlemise ärimoodul
- 4.21.2. Tüüp: avalikke teenuseid pakkuv veebirakendus.
- 4.21.3. Kasutatud protokoll: AJP, AMQP, HTTP(S) (REST), JDBC
- 4.21.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.22. Dokumendi generaator

- 4.22.1. Vahend menetlusprotsesside käigus koostatavate dokumentide genereerimiseks. Liidestatakse teiste süsteemidega kasutades Oracle BI Publisher Java Integration API'sid.
- 4.22.2. Tüüp: sünkroonsed teenused API tarbijatele, veebileht administreerimiseks.
- 4.22.3. Vastaspool: liidese tarbijaks on Ametniku portaali ja protsessimootori.
- 4.22.4. Kasutatud protokoll: Oracle BI Publisheri põhine, ühenduse hoidmiseks kasutatakse Oracle poolt pakutud API't. Port millelt ühendus luuakse, konfigureeritav süsteemis (by default 7001).
- 4.22.5. Lisa: Rakendus vajab oma repositooriumi hoidmiseks andmebaasi.

4.23. ERP

- 4.23.1. Oracle E-Business Suite paigaldatuna eraldi serverile. Haldab/töötleb SKAIS2 raamatupidamisinfot—maksed pankasse või muudesse maksekanalitesse (kojukanne), pangast tagasisideid jne. SKAIS2 integratsioon ERPiga on teostatud läbi vahetabelite. SKAIS2 lisab read tabelitesse, kus ERP need üles korjab. Pärast tagasisidet pangast kirjutab ERP read tabelisse, kus SKAIS2 need üles korjab ja oma ärilistesse tabelitesse laiali salvestab.

4.24. Turvaserver

- 4.24.1. X-tee turvaserver, vajalik X-tee kaudu andmete vahetamiseks.
- 4.24.2. Kasutatud protokollid: HTTP(S) REST ja SOAP.

4.25. Dokumentide arhiveerija

- 4.25.1. Daemon protsess, eesmärgiga arhiveerida operatiivbaasi salvestatud dokumente failihoidlasse.
- 4.25.2. Tüüp: Daemon protsess.
- 4.25.3. Kasutatud protokoll: JDBC.

4.26. Pank

- 4.26.1. Väljamaksete edastamine pankasse.
- 4.26.2. Tüüp: asünkroonne gateway.
- 4.26.3. Kasutatud protokoll: SOAP.

4.27. X-tee

- 4.27.1. Suhtlus erinevate andmekogudega.
- 4.27.2. SKAIS2 poolt pakutavad teenused:

Teenus	Selgitus
EAFmakseteatised	Teenus võtab kohtutäiturilt vastu täitemenetluseaegse elatisabi maksekorraldused.
EAFmakseraport	Teenus väljastab kohtutäituritele täitemenetluseaegse elatisabi maksekorralduste staatused. Info selle kohta, kas Sotsiaalkindlustusameti poolt on maksekorralduse põhjal väljamakse teinud või tagastab veateate, miks maksekorraldust ei ole võimalik täita.

Teenus	Selgitus
TKToovoimPuueHyvitised	Teenus väljastab Töötukassale päritava isiku kohta info, milliseid hüvitisi ja töövõimetusi on määratud isikule Sotsiaalkindlustusametis. Lisaks väljastatakse ka rahaliste väljamaksete, kinnipidamiste ja tulumaksu info.
TKToovoimPuueHyvitisedMassTeenus	Teenus võtab vastu Töötukassast isikukoodide loetelu, kelle kohta Töötukassa soovib hüvitiste infot.
TKToovoimPuueHyvitisedMassTeenusVastus	Teenus väljastab Töötukassale päritavate isikute kohta info, milliseid hüvitisi ja töövõimetusi on määratud isikule Sotsiaalkindlustusametis
TVHTaotlusYksUks	Teenus võtab vastu Töötukassast puude määramise taotluse andmed.
calculateContributionV2	Arvutab etteantud abivahendite müügi tehingu ridadele riigi poolt teenuseosutajale hüvitatavate osamaksete suurused.
calculatelsoLimitParametersV2	Arvutab isikule müüdava abivahendi ISO koodi alusel talle määratud abivahendi soodustuse kasutamise piirmäärad.
cancelTransactionRowV2	Tühistab eelnevalt registreeritud abivahendi müügi- või renditehingu.
changeContribution	Teenus abivahendite teenuseosutajatele osamaksete muutmiseks
checkJustificationV2	Kontrollib isiku õigustatust soodustingimusel abivahendi soetamiseks.
correctTransaction	Teenus abivahendite teenuseosutajatele tehingute korrigeerimiseks.
courierDelivery	Teenus väljastab kojukande teenuseosutajale rahaliste hüvitiste väljamaksete info.
courierDeliveryAnnulation	Teenus väljastab kojukande teenuseosutajale tühistatud rahaliste hüvitiste väljamaksete info.
courierDeliveryReply	Teenus võtab vastu kojukande teenuseosutajalt teostatud väljamaksete info - kas õnnestus raha kliendile viia või mitte.
createTransactionV2	Registreerib uue abivahendi müügi- või renditehingu.
endRental	Lõpetab kehtiva abivahendi rendi perioodi
findUsage	Teenus väljastab Eesti.ee jaoks SKAIS2 poolt pakutavate isikustatud Xtee teenuste kasutamise infot.
incomeTaxExemptionV1	Teenus pensionikeskusele isiku tulumaksuarvestuse vaba jääk
isikutePuuded	Tagastab Kaitseressursside ametile isikute puude info
nonResidencePersons	Teenus väljastab etteantud perioodis Sotsiaalkindlustusametile teavitatud välisriikide maksuresidentsuse andmed (<i>sh. riigi, perioodi, tõendi staatuse ja registreerimise aja kohta</i>)
providerValidity	Valideerib et vastaval teenuseosutajal on õigus teostada soodustingimustel abivahendi müüki.
requestTransactionEvents	Teenus abivahendite teenuseosutajatele tehtud tehingute sündmuste pärimiseks.
requestTransactions	Teenus abivahendite teenuseosutajatele tehtud tehingute pärimiseks
star1Tulud	Teenus väljastab kohalikele omavalitsustele päritava isiku kohta info, milliseid hüvitisi on Sotsiaalkindlustusameti poolt

Teenus	Selgitus
	isikule määratud. Millised on olnud hüvitiste väljamaksed ja kinnipidamised.
starPuue2	Teenus väljastab kohalikele omavalitsustele, milliseid puuded on isikule määratud.
taituri_vmaksed	Teenus väljastab kohtutäituritele Sotsiaalkindlustusameti poolt isikutele teostatud väljamaksete info.
tlvisikuPuudeInfo	Teenus väljastab Tallinna linnavalitsusele päritava isiku kohta info, mis liiki puue on isikule määratud.

4.27.3. SKAIS2 poolt tarbitavad teenused:

Andmekogu	Teenus	Selgitus
arireg	lihtandmed_v1	Äriregister - Lihtandmete päring
arireg	detailandmed_v3	Äriregister - Ettevõtja detailandmete päring
at	teadaandeLiigid_v2	Ametlikud teadaanded – Teenusega tagastatakse teadaande liikide kirjeldused.
at	otsiTeadaanne	Ametlikud teadaanded – Teenusega tagastatakse teadaannete info.
digilugu	hl7	Terviseinfosüsteem – Teenusega päritakse Arstliku-eksperiisi taotluse juurde isiku viimase viie aasta arstivisiite.
ehis	sotsList1V2	Eesti hariduse infosüsteem - Õppuri andmed peretoetuste jaoks
ehis	sotsList2	Eesti hariduse infosüsteem - Õppurite andmed toitjakaotuspensionide jaoks
kirst	kindlustatus	Haigekassa infosüsteem - Kontrollipäring isiku kindlustatuse kohta
kirst	kindlustusalus	Haigekassa infosüsteem – kindlustusaluse info edastamine haigekassale
kirst	tvI_loetelu2	Haigekassa infosüsteem – Päring isiku töövõimetuslehtede kohta
kpr	liitumise_kontrollimine	Pensionikeskus – Päring kontrollimaks, kas isik on liitunud pensioni II sambaga.
kpr	maksekohustused	Pensionikeskus – Päring kontrollimaks kas isik on lõpetanud maksed pensioni II sambasse.

tsd	skaSotsmaks	Maksu- ja tolliamet – Päring isiku sotsiaalmaksu andmete kohta
EMTA	PublicNonResidencyInquiry	Maksu- ja tolliamet – Päring isiku residentsuse kohta.
pkrr	STAR1_TULUD	Pensionikindlustuse register – Päring kohalikele omavalitsustele makstud tulude kohta.
pkrr	taituri_vmaksed	Pensionikindlustuse register – Päring isikule tehtud väljamaksete küsimine.
rr	RR456	Rahvastikuregister – Päring isikukoodi alusel isiku andmete kohta (dokumendid, suhted ja hooldusõigused)
rr	RR67_muutus	Rahvastikuregister – masspäring isikuandmete muudatuste kohta vastavalt edastatud ajavahemikule.
rr	RRisikuandmeteMuudatused	Rahvastikuregister – uuenenud masspäring isikuandmete muudatuste kohta vastavalt edastatud ajavahemikule.
rr	RRisikuViibimiskoht	Rahvastikuregister – Päring isiku viibiiskoha kohta.
star	KontrolliToimetulekuToetuseSaamist	STAR - Päring kohalike omavalitsuste infosüsteemist kontrolimaks isiku toimetulekutoetuse saamist.
star	starPuudeotsusedV1	STAR – proaktiivne teenus, saadetakse kõik puudeotsused. Kohalikelomavalitsustel on vajalik teada isikutele määratud puuded haldusalas elavate isikute abivajaduse hindamiseks.
tkis	EkspertiisArvamusV2	Eesti töötukassa töövõime hindamise tuvastamise ekspertiisi andmeid välistele asutustele
tkis	TootuArvelolekV2	Töötuna arveloleku andmestik vanamahusitise alusandmete jaoks
tkis	TVHOtsusV1	Töövõime hindamise tuvastamise otsus
tkis	TVHTaotlusNimekiriV1	Töövõime hindamise tuvastamise taotluste nimekiri

tor	TORIK	Töötamise informatsiooni küsimine Töötamise registrist.
tor	TOOTREG_AMETNIK	Töötamise register - Töötamise andmete muutmise teenus.
tor	uploadMime	Töötamise register - Masspäring etteantud isikukoodide alusel isikute töötamise kohta
tor	downloadMime	Töötamise register - Masspäringu vastus eelnevalt küsitud isikute töötamise kohta.

4.27.4. Tüüp: sünkroonne

4.27.5. Kasutatud protokoll: SOAP

4.28. X-Road

4.28.1. Suhtlus erinevate andmekogudega.

4.28.2. SKAIS2 poolt pakutavad teenused:

Teenus	Selgitus
search-persons-latest-contacts	Teenusega antakse STAR'ile teada isiku viimased kontaktandmed.
teavitaSynnitahtaegV1	Teenusega võetakse, tervise teenuse osutajatelt (nt. haiglad), vastu informatsiooni eeldatava(te) sünnitähataegade kohta.
tyhistaSynnitahtaegV1	Teenusega võetakse, tervise teenuse osutajatelt (nt. Haiglad) vastu informatsiooni perinataalsurmade kohta.

4.28.3. Tüüp: sünkroonne

4.28.4. Kasutatud protokoll: HTTP(S) REST

5. Süsteemi arhitektuuris kasutatavad tehnoloogiad

- 5.1. **Apache HTTP Server** — Versioon: 2.4. Konfiguratsioon ja nõuded: SSL, koormusjaotur (mod_proxy_balancer), sticky session. Operatsioonisüsteem: RedHat / CentOS / Oracle Enterprise Linux.
- 5.2. **Apache Tomcat** — Versioon: 9.0.x Konfiguratsioon ja nõuded: klasterdamine Tomcat rakendusserverite tasemel (SimpleTcpCluster). Operatsioonisüsteem: RedHat / CentOS.
- 5.3. **Oracle BI Publisher** — Versioon: *Oracle Business Intelligence* (12.2.x). Konfiguratsioon ja nõuded: Repositoorium Oracle 19c EE; rakendusserver: Oracle WebLogic (kaasas by default installatsiooni paketis). Operatsioonisüsteem: Oracle Linux.
- 5.4. **Oracle 19c EE** — Versioon: *Oracle Database 19c Enterprise Edition* 19.13. Konfiguratsioon ja nõuded: klasterdatud andmebaas. Operatsioonisüsteem: RedHat / CentOS / Oracle Enterprise Linux.
- 5.5. **Oracle Database Advanced Queuing** — kasutatakse erinevate enne 2018 tarnitud komponentide vahel asünkroonseks suhtluseks.
- 5.6. **Rabbit MQ** — Versioon: 3.8.16. Kasutatakse erinevate komponentide vahel asünkroonseks suhtluseks.

6. Tehnoloogiate maatriks

Rakendus	Java	SOAP / REST	Apache Tomcat 9	Sõnumi- vahetus	Andmebaas	Märkus
Ametniku portaal	11	SOAP + REST	Jah	Oracle AQ + RabbitMQ	Oracle 19c EE	<i>Suhtlus X-teega kasutab SOAP liidestust, muu suhtlus käib REST ja asünkroonse sõnumivahetuse abil.</i>
Komposiit	11	REST	Jah	RabbitMQ	Oracle 19c EE	
Abivahendite teenus	11	REST			Oracle 19c EE	
Arestid	11	REST		RabbitMQ	Oracle 19c EE	
Arstlik-ekspertiis küsimustik	11	REST		RabbitMQ	Oracle 19c EE	
Arstlik-ekspertiis menetlus	11	REST		RabbitMQ	Oracle 19c EE	
Arstlik-ekspertiis taotlus	11	REST		RabbitMQ	Oracle 19c EE	
Dokumendi hoidla	11	REST		RabbitMQ	Oracle 19c EE	
Finants facade	11	REST		RabbitMQ	Oracle 19c EE	
Ekspertarsti hinnang	11	REST		RabbitMQ	Oracle 19c EE	
Elatisabi	11	REST		RabbitMQ	Oracle 19c EE	
Kliendipöördumised	11	REST		RabbitMQ	Oracle 19c EE	
Kindlustuslepingud	11	REST		RabbitMQ	Oracle 19c EE	
Pensioniõiguslik staaž	11	REST		RabbitMQ	Oracle 19c EE	
Rahvastikuregistri andmete töötlemine	11	REST		RabbitMQ	Oracle 19c EE	
RFK klassifikaator	11	REST		RabbitMQ	Oracle 19c EE	
Digitempli teenus	11			RabbitMQ	Oracle 19c EE	
Dokumentide arhivaator	11				Oracle 19c EE	
X-tee teenustäitja (sisenevad)	11	SOAP	Jah		Oracle 19c EE	

Rakendus	Java	SOAP / REST	Apache Tomcat 9	Sõnumi-vahetus	Andmebaas	Märkus
X-road teenustäitja (sisenevad)	11	REST		RabbitMQ	Oracle 19c EE	
Abivahendite x-tee teenustäitja (sisenevad)	11	SOAP + REST			Oracle 19c EE	
X-tee andmejälgija	11	SOAP			PostgreSQL	
RINA Facade	11	REST		RabbitMQ	Oracle 19c EE	
Protsessimootor	11	SOAP		Oracle AQ	Oracle 19c EE	
X-tee turvaserver		SOAP				
Failihoidla	11				Oracle 19c EE	
TUUM Andmebaas					Oracle 19c EE	

7. Tuleviku visioon

7.1. Läbiviidud arhitektuurianalüüsi käigus loodi tänaste probleemide adresseerimiseks uus arhitektuuriline visioon, millega kaasnevad tähtsamad muudatused on:

7.1.1. 2018 arendatud olemasolevate rakenduste (ametrnikurakendus, X-tee teenustäitja ja protsessimootori "monoliidid") kõrvale on hakatud arendama igale valdkonnale eraldi koodibaasi ja rakendusi. Uuemad äriteenused on arendatud jälgides mikroteenuste arhitektuuri põhimõtteid. Tasapisi on olemasolevatest teenuste monoliidist välja tõstetud funktsionaalselt iseseisvaid tükke ning need realiseeritud eraldi mikroteenustena. Kavas on seda mustrit jätkata ning edasistes arendustes monoliidi osakaalu järk-järgult veelgi vähendada.

7.1.2. Rakenduste paigaldusel võetakse kasutusele konteinerlahendused (Kubernetes). Uute rakenduste loomisel võetakse kohe arvesse, et neid saaks paigaldada ka konteinerina.

7.1.2.1. NB: täna (02.2024) ei ole Kubernetes veel toodangus. Täna teenustäitjaga käivad läbirääkimised Kubernetesi klastri seadistuse ning halduse vastutuste piiride üle.

7.1.2.2. Seni tarnitud komponentide liigutamisega Kubernetesi konteinerplatvormile on plaanis alustada 2025 aastal.

7.1.2.3. SKAIS2 rakenduse kolimine Kubernetesi klastrisse toimub järk-järgult üksikute ärikomponentide kaupa, kuni lõpuks on kõik SKAIS2 komponendid Kubernetesi klastris.

7.1.3. Suurem rõhk *continuous integration*'ile ja automaattestimisele.

7.1.3.1. Seniste tarneprotsesside optimeerimine ja automatiseerimine.

7.1.3.2. Keskkonna konfiguratsioonide ühtlustamine ja versioneerimine.

8. Teenuse tehniline kirjeldus

8.1. Nõuded serveriruumile ja infrastruktuurile

8.1.1. Täitja majutab tellija infosüsteemi kahes füüsiliselt eraldi asukohas ja eraldi aadressidel paiknevas serveriruumis. Serveriruumid ja nende vahelised ühendused peavad

- paiknema Eesti Vabariigi territooriumil ja serveriruumide minimaalne nõutud geograafiline vahemaa vähemalt 1 km.
- 8.1.2. Serveriruumid peavad olema spetsiaalselt ehitatud serverite majutuseks ja vastama E-ITS turbeastmele H ning standardile ANSI/TIA-942 (Telecommunications Infrastructure Standard for Data Centers) tasemele Tier 3, mõõndusega, et varugeneraator ei pea olema dubleeritud.
- 8.1.3. Täitja tagab SKAIS2 infosüsteemile turvatud (SSL) välise andmesideühenduse kiirusega vähemalt 100 Mbps (megabitti sekundis) ja serveriruumide vahel füüsilise, turvatud (VPN) dubleeritud ühenduse kiirusega vähemalt 1 Gbps (gigabitti sekundis).
- 8.1.4. Andmesideühenduse (internetiteenuse) täitja peab olema Eesti Interneti SA poolt akrediteeritud.
- 8.1.5. Serverite ja serveriruumide vaheline ühenduse kiirus peab olema piisav, et tagada teenustaseme nõuded. Tõrke korral peab olema tagatud teenuste üle viimine teise serveriruumi teenuse nõuetele vastava aja jooksul.
- 8.1.6. Täitja serveriruumid peavad olema ühendatud tellija serveriruumidega läbi VPN ühenduse kiirusega vähemalt 1Gb/s. Tellija serveriruumid asuvad serverimajutuskeskustes kahes erinevas lokatsioonis Eesti Vabariigis.
- 8.1.7. Täitja tagab eraldatud turvadomeenid süsteemi tuumale, Ametnikurakendusele, Avalikule rakendusele ja eBS rakendusele. Täitja kirjeldab pakumises vastavat tehnilist lahendust.
- 8.1.8. Täitja peab kasutama riistvara, millel töötab ainult tellija infosüsteem. Pakutaval riistvaral ei tohi töötada samal ajal kolmandate osapoolte infosüsteemid. Samuti ei tohi olla kolmandatel osapooltel ligipääse pakutavale riistvarale ja operatsioonisüsteemile.
- 8.2. SKAIS2 infosüsteemi majutus- ja tugiteenuste üldised (miinimum) nõuded
- 8.2.1. Täitja kohustub tagama SKAIS2 infosüsteemi kasutamise võimaluse veebikeskkonnas ning lepingu kehtivuse perioodil kindlustama keskkondade nõuetekohase (hankedokumentis ja teenusepassis kirjeldatud) funktsioneerimise.
- 8.2.2. Täitja tagab SKAIS2 infosüsteemi järgmised majutus- ja tugiteenused:
- 8.2.2.1. Serverite, võrgu- ja salvestusseadmete ressursid.
 - 8.2.2.2. Andmebaaside administreerimine ja monitooring.
 - 8.2.2.3. Rakenduste administreerimine ja monitooring.
 - 8.2.2.4. Infrastruktuuri administreerimine ja monitooring.
 - 8.2.2.5. X-tee turvaserverite (x-tee v6) administreerimine, versiooniuuendused ja sellega kaasnevad tööd, kaasa arvatud riistvaralist turvalist allkirjastamist võimaldavat (SSCD) seadet. Majutaja tagab tehnilise võimekuse osutada teenust vastavalt kehtivatele x-tee nõuetele. SKAIS2 tarkvaras kasutatakse digitembeldamist, mille tehnilises realisatsioonis kasutatakse RIA soovitude mõttes vähemalt keskklassi SSCD seadet (HSM), mis tagab vähemalt 20 päringut/s. HSM seadme tagab Täitja majutusteenuse koosseisus.
 - 8.2.2.6. Muudatuste haldus.
 - 8.2.2.7. Konsultatsioonid ja parendusettepanekud.
 - 8.2.2.8. Muud ühekordsed tegevused ehk lisatööd.
 - 8.2.2.9. Teenuse lõpetamisega seotud tööd lepingu lõppemisel.
- 8.2.3. Infosüsteem peab olema majutatud kahes serveriruumis põhimõttel primary site ja failover site. Täitja peab kirjeldama, mis vahenditega tagatakse vajaduse korral teenuste üle viimine teise serveriruumi vastavalt käideldavusnõuetele.
- 8.2.4. SKAIS2 infosüsteemi Oracle andmebaaside vaheliseks andmete reaajas sünkroniseerimiseks peab Täitja kasutama Oracle Data Guard tarkvara. Oracle Active Data Guard tarkvara võetakse kasutusele vajadusepõhiselt, mille kasutuselevõtu tingimused lepatakse eraldi kokku teenuseosutajaga.

- 8.2.5. eBS infosüsteemi Oracle andmebaaside vaheliseks andmete reaajas sünkroniseerimiseks peab Taitja kasutama Oracle Data Guard tarkvara.
- 8.2.6. Vältimaks SKAIS2 infosüsteemi ülekoormamist ei tohi Oracle BI Publisher aruandluskeskkond andmeid pärida aktiivsest SKAIS2 infosüsteemi andmebaasist.
- 8.2.7. Lepingu lõppedes kooskõlastatakse andmete uude majutuskeskkonda migreerimise ja seejärel hävitamise protsess Tellija ja Taitja vahel. Andmete ülekolimise ja hävitamise järgselt vormistab majutusteenuse osutaja akti, millega kinnitatakse, et andmed on hävitatud.
- 8.2.8. Teenuse osutaja vahetumisel, vormistatakse andmete ülekolimise (migratsiooni) läbiviimise järgselt kolmepoolne üleandmis-vastuvõtu akt (andja, vastuvõtja, omanik).
- 8.2.9. Teenuse lõppedes, uude keskkonda andmete migratsiooni ettevalmistamine ja läbiviimisel abi osutamine (täitja pädevuse ulatuses) on majutusteenuse osa ja ei ole eraldi tasustatav.
- 8.3. Nõuded andmete hoidmisele
 - 8.3.1. Kõik infosüsteemis töödeldavad andmed (andmebaasis ja rakendusserverites) peavad paiknema keskses andmesalvestusmassiivis, mille andmemahut on lihtsasti juurde tellitav. Andmesalvestusmassiiv peab võimaldama andmete kloonimist töökeskkonnast töökeskkonna-eelsesse ja testkeskkonda. Andmesalvestusmassiivi mis tahes komponendi rike ei tohi põhjustada andmekadu.
 - 8.3.2. Taitja peab maandama andmesalvestusmassiivi riknemise riski, mis võib Tellijale tähendada ulatuslikku teenusekatkestust. Taitja kirjeldab pakkumuses, kuidas ja mis vahenditega (sh SAN seadmed ja andmesalvestusmassiivid) on tagatud mainitud riskide maandamine.
- 8.4. X-tee turvaserverid
 - 8.4.1. SKAIS2 infosüsteemis on kasutusel x-tee versioon 6 raamistik.
 - 8.4.2. Taitja tagab eraldi x-tee turvaserverid töökeskkonna, toodangueelse keskkonna ja testkeskkonna tarbeks. Testkeskkond on liidestatud X-tee testkeskkonnaga; toodangueelne ja toodangukeskkond on liidestatud X-tee töökeskkonnaga.
 - 8.4.3. Taitja tagab x-tee ligipääsu dubleeritud serveriruumis, sealhulgas olukorras, kus primaarne serveriruum ei ole kasutatav ja töökeskkond on üle kolitud.
 - 8.4.4. Taitja osutab Tellijale turvaserverite administreerimisteenust.
 - 8.4.5. Taitja peab omama x-tee turvaserveri logimise lahendus, mis võimaldab väljastada regulaarselt logiandmed tellijale.
- 8.5. Muudatuste haldus
 - 8.5.1. Arendusmuudatuste paigalduse õigus on ainult täitjal, kui ei lepita kokku teisiti.
 - 8.5.2. Arendusmuudatused valmistab ette täitja ja edastab paketeeritult koos paigaldusjuhendiga paigaldamiseks toodangu-, toodangueelsesse ja testkeskkonda. Paigalduspakettide, juhendite jm vajaliku informatsiooni edastamiseks ja paigaldustega seotud tegevuste dokumenteerimiseks, kasutatakse tellija tööde/projektide juhtimise keskkonda Jira.
 - 8.5.3. Teenusetäitja paigaldab arendusmuudatusi lepingu raames vastavalt teenuse passile ja tarne juhendile.
 - 8.5.4. Toodangukeskkonda ja toodangueelsesse keskkonda tehakse üldjuhul kuni 4 arendusmuudatuse tarnet ja 4 veaparandustarnet kuus. Testkeskkonda tehakse üldjuhul kuni 12 arendusmuudatuse tarnet ja 12 veaparandustarnet kuus. Arendusmuudatusi töökeskkonda viiakse sisse väljaspool aktiivset tööaega.
 - 8.5.5. Teenusetäitja peab vastavalt tellimusele käivitama parandusskripte vigade tuvastamiseks ja parandamiseks.
 - 8.5.6. Arendusmuudatuste paigalduse aja kooskõlastab täitja tellijaga.
 - 8.5.7. Taitja poolt arendusmuudatuse paigalduse ebaõnnestumisel vastutab täitja süsteemi taastamise (rollback) eest.

- 8.5.8. Täitja uuendab toodanguelse ja testkeskkonna andmeid toodangukeskkonna andmetega tellija tellimisel kui tarnejuhend või arendusprotsessi etapp (näiteks andmemigratsiooni ettevalmistamine) seda ette näeb. Andmeuuenduse läbiviimise aeg ja maht lepitakse eraldi kokku.
 - 8.5.9. Teenusetäitja tagab tellija tellimisel arenduspartneritele ligipääsu test- ja toodanguelsele keskkonnale (andmebaasile, rakendusserverile) 2 tööpäeva jooksul.
 - 8.5.10. Teenusetäitja tagab tellija tellimisel arenduspartneritele ligipääsu sulgemise test- ja toodanguelsele keskkonnale esimesel võimalusel, kuid mitte hiljem kui 2 tööpäeva jooksul.
 - 8.5.11. Täitja peab tagama Tellija tellimisel (andme)halduritele / rakenduse administraatoritele ligipääsud kõikide SKAIS2 keskkondade serverite operatsioonisüsteemi konfiguratsioonifailidele ja andmebaasidele.
- 8.6. Varundamine ja teenuse taastamine
- 8.6.1. Täitja teeb majutuskeskkonnas olevatest süsteemidest regulaarselt varukoopiaid selliselt, et oleks tagatud teenuse passis sätestatud tingimuste täitmine. Täitja peab pakkumises kirjeldama, et milliste vahendite ja meetoditega tehakse varukoopiaid.
 - 8.6.2. Varukoopiaid tehakse rakendusi seiskamata st, et Tellija infosüsteemide käideldavus ei ole varukoopiate tegemise ajal mõjutatud. Varundust teostatakse väljaspool infosüsteemi tööaega.
 - 8.6.3. Varukoopiaid tuleb salvestada töökeskkonnast eraldi asuvatele andmekandjatele, mis asuvad erinevas füüsilises lokatsioonis. Varukoopiaid ja nende allika vaheline andmevahetus peab olema krüpteeritud.
 - 8.6.4. Täitja on kohustatud hoidma töökeskkonna varundatud andmeid järgnevalt:
 - 8.6.4.1. Vähemalt kahe viimase kuukoopia.
 - 8.6.4.2. Vähemalt neli viimast nädalakoopiat.
 - 8.6.4.3. Vähemalt viis viimast tööpäevakoopiat.
 - 8.6.5. Kuukoopiaid on planeeritud kopeerida täiendavalt andmesaatkonda. Ajakava ning täpne tehniline lahendus töötatakse välja ja realiseeritakse koos eduka Täitjaga töö käigus 2020/21.aastal.
 - 8.6.6. Andmekadu põhjustavat intsidenti käsitletakse kui erakorralist intsidenti. Erakorralise intsidendi korral on lubatud teenuse järjestikune seisak kuni 4 tundi ja summaarne seisak kuni 4 tundi nädalas ja kuni 6 tundi kalendrikuus. Pärast intsidendi lahendamist ja/või andmete taastamist esitab täitja tellijale detailse raporti, kus toob välja intsidendi põhjuse, mis põhjustas andmekadu ning meetmed selliste juhtumite vältimiseks või esinemise tõenäosuse vähendamiseks tulevikus.
 - 8.6.7. Täitja töötab pärast iga keskkonna käivitamist ühe kuu jooksul välja vastava keskkonna taasteplaani ja esitab selle Tellijale ülevaatamiseks ja kinnitamiseks. Taasteplan peab sisaldama tegevuskava ja süsteemi üldist arhitektuuri kirjeldust visuaalsel kujul. Olulised infrastruktuuri komponendid (serverid, võrguseadmed jne) peavad olema kirjalikult lahti seletatud.
 - 8.6.8. Täitja testib taasteplaani ajakohasust, kui toimub muudatus Tellija infosüsteemiga seotud infrastruktuuris, kuid mitte harvemini kui üks kord aastas. Täitja kooskõlastab Tellijaga testi läbiviimise aja ning esitab Tellijale pärast testi läbiviimist raporti, kus märgib ära taasteplaani vastavuse tegelikule olukorrale ja plaanist leitud puudused. Puudused tuleb kõrvaldada Tellijaga kokkuleppel mõistliku aja jooksul ning seejärel korraldada uus taasteplaani test.
- 8.7. Monitooring
- 8.7.1. Täitja tagab tsentraliseeritud tehnilise toe teenuse, mis on avatud 24 tundi ööpäevas ja seitse päeva nädalas, mille kaudu sooritatakse mitmesuguseid süsteemiga seotud järelevalve, muudatuste ja veahalduse menetlustoiminguid.
 - 8.7.2. Tehnilise toe teenuseid osutatakse osana majutusteenustest, kus kõik süsteemihoiatused saadetakse tsentraliseeritud 24 tundi toimivale tehnilisele toele (sh

- võrgu, serveri ja rakenduse hoiatused). Rakenduste ja teiste SKAIS2 komponentide monitooringuinfo hoitakse Graylog logihalduse keskkonnas. Graylog logihalduse keskkond (on-premise) on majutusteenuse osa.
- 8.7.3. Kõik keskkonnad peavad olema Täitja poolt monitooritud kogu lepinguperioodi vältel.
- 8.7.4. Täitja võimaldab Tellijale ja Tellija poolt nimetatud arendajale juurdepääsu monitooringuinfole või edastab monitooringuteated Tellija poolt etteantud meiliaadressile.
- 8.7.5. Täitja installeerib vajadusel või Tellija palvel serveritesse täiendavad monitooringuagendid, mis koguvad infot serverite ja rakenduste seisundi kohta. Tellijal on täna kasutusel monitooringu süsteem Prometheus ja Grafana.
- 8.7.6. Täitja monitoorib serverites asuvate infosüsteemide tööd vähemalt järgmiste komponentide osas:
- 8.7.6.1. Andmesideühenduse olemasolu Tellija serverite ja infosüsteemide vahel.
 - 8.7.6.2. Serverite riistvaraliste komponentide töökorras olek.
 - 8.7.6.3. Serverite protsessorite ja mälu kasutus.
 - 8.7.6.4. Kõvaketaste täituvus.
 - 8.7.6.5. Süsteemi load (UNIX süsteemide puhul).
 - 8.7.6.6. Andmebaasisüsteemi töökorras olek.
 - 8.7.6.7. Andmebaasile eraldatud ressursside olemasolu.
 - 8.7.6.8. Varukoopiate tegemise õnnestumine.
 - 8.7.6.9. Monitooringusüsteemi töökorras olek.
- 8.7.7. SKAIS2 infosüsteemi rakenduse monitooring
- 8.7.7.1. Täitja poolset SKAIS2 rakenduse monitooringut ei nõuta. Täitjal peab olema valmisolek integreerida oma keskkonda Tellija poolt kasutatavad rakenduse monitooringu vahendid (agendid vms).
- 8.8. Teenuse tehniline tugi
- 8.8.1. Täitja peab tagama kasutajatoe (ühtne kontaktpunkt, telefoni number, e-mail ja/või avalik portaal) vastavalt Teenuse passis toodud nõuetele.
 - 8.8.2. Täitja peab teavitama Tellijat kriitilistest ja keskmise taseme vigadest kohe ja asuma teenuse nõutud tingimustele vastavust taastama.
 - 8.8.3. Kui tõrget ei ole võimalik teenuse passis nõutud aja jooksul lahendada, peab Täitja esitama põhjendused ja lahendusettepanekud.
 - 8.8.4. Kriitilise taseme tõrkeks loetakse olukorda, kus SKAIS2 toodangukeskkonna tervikuna või oluliste komponentide, s.h andmevahetused teiste infosüsteemidega, kasutamine ei ole võimalik.
 - 8.8.5. Keskmise taseme tõrkeks loetakse olukorda, kus SKAIS2 toodangukeskkonna kasutamine on oluliselt häiritud.
 - 8.8.6. Madala taseme tõrkeks loetakse olukorda, kus SKAIS2 toodangukeskkonna kasutamine on võimalik, kuid on häiritud.
- 8.9. Aruandlus ja infovahetus
- 8.9.1. Täitja esitab majutusteenuse osutamise kohta igakuiselt ülevaate eelmise kuu kohta, mis sisaldab vähemalt järgmist informatsiooni:
 - 8.9.1.1. Süsteemi komponentide käideldavus vastavalt teenuste passi nõuetele.
 - 8.9.1.2. Perioodi vältel toimunud intsidendid koos algus- ja lõpuajaga, juurpõhjusega (kui on selgunud) ning kirjeldusega, kuidas neid edaspidi vältida.
 - 8.9.1.3. Perioodi vältel tehtud plaanilised tööd.
 - 8.9.1.4. Muudatuste logi.
 - 8.9.1.5. Tellija poolt perioodi jooksul esitatud pöördumiste staatus, mis sisaldab ka lahendamata pöördumisi eelmistest perioodidest.
 - 8.9.1.6. Täitja poolsed ettepanekud infosüsteemi ja majutuse parendamiseks ning teostamiskava.

- 8.9.2. Aruandlus peab olema tellija kontaktisikutele kättesaadavaks tehtud veebi kaudu või e-kirja teel.
- 8.9.3. Taitja peab võimaldama tellijal tellida tellimustööna täiendava tasu eest ühekordseid raporteid nt andmebaasi detailseid koormusraporteid.
- 8.9.4. Taitja ja tellija vaheline töökeel on eesti keel.

III. STAR arhitektuuridokument

1. Sissejuhatus

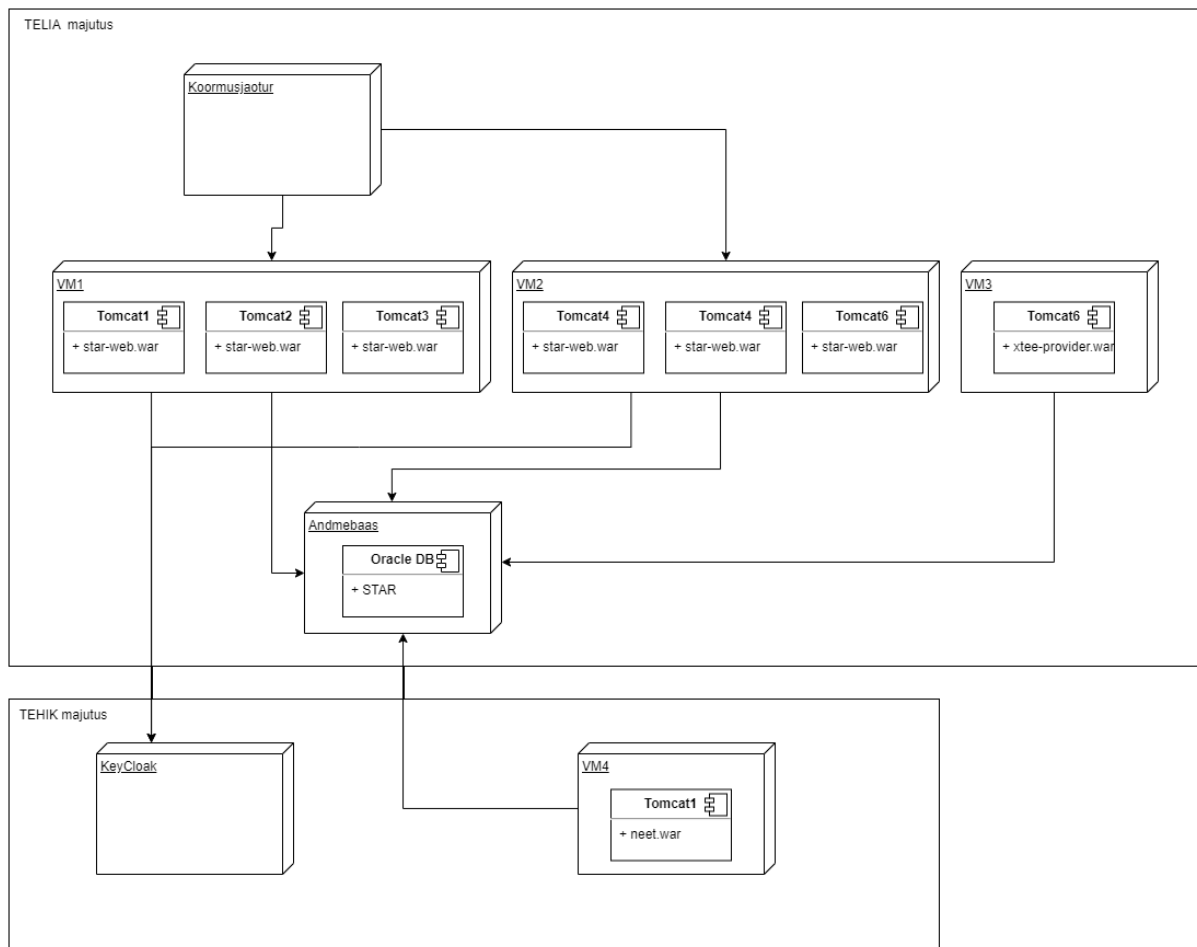
- 1.1. Antud dokument kirjeldab STAR infosüsteemi arhitektuuri, sisaldades antud süsteemi komponentide kirjeldust, nende omavahelist suhtlemist, paigaldusvaadet ning kirjeldust süsteemi ning teda ümbritsevate keskkondade vahel.

2. Süsteemi taust

- 2.1. Sotsiaalkindlustusameti infosüsteem STAR on riigi keskne andmeregister, mis on asutatud juhtumikorralduse põhimõttel läbiviidava sotsiaaltöö korraldamiseks ja mille põhikasutajateks on kohalike omavalitsuste sotsiaaltöö spetsialistid ja sotsiaalteenuseid osutavate ettevõtete esindajad. STAR-i peetakse seadustest tulenevate Sotsiaalkindlustusameti avalike ülesannete täitmise eesmärgil.
- 2.2. STARis on toimumas tehnoloogiline siirdumine monoliitrakendusest mikroteenustele põhinevale rakendusele. Siirdumine toimub väikeste sammudega ja paralleelselt on kasutusel monoliitrakendus (STAR₁) ja mikroteenustel põhinev rakendus (STAR₂). STAR₁ ja STAR₂ suhtlevad omavahel läbi API liidest. Kummalgi rakendusel on oma kasutajaliides.
- 2.3. STAR₁ koosneb kolmest eraldi paigaldatavast rakendusest:
- 2.4. Ametnikurakendus (star-web.war) - peamine rakendus. KOVi ja SKA menetluste äriloogika juhtimine;
- 2.5. X-tee provider (STARXteeProvider6.war) - pakub X-tee teenuseid välistele infosüsteemidele;
- 2.6. NGTS seire ankeet () - lihtne ankeedi rakendus Noortegarantii tugisüsteemi (NGTS) seire teostamiseks.
- 2.7. Andmeid hoitakse keskses Oracle 19c andmebaasis.
- 2.8. STAR₂ mikroteenused on veel algses arengu järgus. Valmis on tehtud kolmes küpsusastmes teenuseid:
- 2.9. Iseseisvad mikroteenused - Kogu vajalik funktsionaalsus on arendatud ühe mikroteenuse sisse. Mikroteenusel on oma andmebaas.
- 2.10. Hübridmikroteenus - Vajalik funktsionaalsus on arendatud mikroteenuse sisse. Mikroteenusel on oma andmebaas. Aga ta sõltub mingil määral STAR₁ andmetest ja äriloogikast.
- 2.11. Proxymikroteenused - Mikroteenus ei sisalda äriloogikat ega oma andmebaasi. Vajaliku äriloogika ja andmed asuvad STAR₁ rakenduses. Proxy mikroteenus vahendab STAR₁ loogikat ja andmeid.
- 2.12. Edasistes arendustest peavad hübrid ja proxy mikroteenused muutuma iseseisvateks mikroteenusteks.
- 2.13. Iseteeninduse broneeringute rakendus on osa Sotsiaalkindlustusameti iseteenindusest. Kuna Sotsiaalkindlustusameti iseteeninduse põhirakendus ei toeta mikrofrontende, siis broneeringute süsteem on arendatud eraldi iseseisva rakendusena. Iseteeninduse broneeringute rakendus baseerub mikroteenustel. STAR ja SKAIS infosüsteemidega toimub andmevahetus üle X-tee.
- 2.14. Infosüsteemi STAR majutuskeskkond koosneb kolmest võrgu tasemele teineteisest lahusolevast keskkonnast. Kõiki keskkonnad on üles ehitatud sarnase arhitektuuri ja komponentidega va. testkeskkond, millel puudub vajadus teise dubleeriva öla järele. Allpool dokumendis on komponentide tasemel piisava detailsusega lahti kirjutatud STAR loogiline arhitektuuriline ülesehitus kirjeldamaks praeguse süsteemi toimimist ja võimaldamaks jätkusuutlikku arengut tulenevalt Sotsiaalkindlustusameti arenduse soovidest.

3. STAR komponentdiagramm

3.1. Järgnev skeem kirjeldab STAR infosüsteemis paiknevaid komponente ning nende vahelist suhtlust.



3.2. **Veebiportaal** – Ametnikele mõeldud veebirakendus

3.3. **SSO ja KeyCloak** – Autentimislahendus süsteemi mõldimiseks.

3.4. **Turvaserver** – Liidestus X-Teega.

3.5. **Andmebaas** – Oracle Database Enterprise Edition, STAR andmestik.

4. **Majutatavad teenuse komponendid**

4.1. **Andmebaas**

4.1.1. Oracle Database 19c Enterprise Edition.

4.2. **Veebiportaal**

4.2.1. KOV ametnikele mõeldud veebirakendused

4.2.2. Tüüp: teenuseid pakkuv veebilehekülg

4.2.3. Kasutatud protokoll: https

4.2.4. Käideldavus: klastrisse ja koormusjaoturi taha paigaldatud virtualiseeritud masinad.

4.3. **Adapterserver**

4.3.1. Kasutatakse x-tee teenuste vahendamiseks x-teele

4.3.2. Tüüp: sünkroonne ja asünkroonne teenus; süsteemne taustprotsess

4.3.3. Kasutatud protokoll: integreeritud süsteemi osa

4.4. **Digitempel**

4.4.1. SSCD seade võimaldamaks turvalist allkirjastamist. SSCD seade peab võimaldama teostada 100 allkirjastamist minutis.

4.4.2. Tüüp: Daemon protsess

4.4.3. Kasutatud protokoll: jdbc; https;

4.5. **Turvaserver**

- 4.5.1. X-tee turvaserver, vajalik X-teel andmete vahetamiseks.
- 4.5.2. Kasutatud protokoll: soap

5. Välised liidestused

5.1. SSO (KeyCloak)

- 5.1.1. Autentimislahendus, liidestatud RIA TARA keskkonnaga, et pakkuda ID-kaardiga, Mobiil-ID ja SMART-ID sisselogimist
- 5.1.2. karbitoode: <https://www.keycloak.org/>

5.2. Sertifitseerimiskeskus

- 5.2.1. Digiallkirjade kehtivuskinnitus
- 5.2.2. Tüüp: sünkroonne teenus

5.3. Pank

- 5.3.1. Väljamaksete edastamine panka
- 5.3.2. Tüüp: asünkroonne gateway
- 5.3.3. Kasutatud protokoll: SOAP

5.4. X-tee

- 5.4.1. Erinevate andmekogudega suhtlus
- 5.4.2. Tüüp: sünkroonne/asünkroonne
- 5.4.3. Kasutatud protokoll: SOAP

6. Süsteemi arhitektuuris kasutatavad tehnoloogiad/tarkvarad

6.1. Serverite operatsioonisüsteem

- 6.1.1. Serverite operatsioonisüsteemi tarkvarad peavad olema kaetud tootjapoolse tarkvaratoega lepingu perioodi vältel.
- 6.1.2. Operatsioonisüsteem: Red Hat Enterprise Linux 7 (RHEL) / Oracle Enterprise Linux 7 (OEL).
- 6.1.3. X-tee turvaserveritel Ubuntu linux LTS (vastavalt RIA nõuetele).
- 6.1.4. Vajalikud litsentsid tagab Täitja.

6.2. Apache HTTP Server Versioon: 2.4.

- 6.2.1. Konfiguratsioon ja nõuded: SSL, ID-Kaardi sertifikaadi tuvastamine (ssl konfiguratsioon).
- 6.2.2. Operatsioonisüsteem: Red Hat Enterprise Linux 7 (RHEL)
- 6.2.3. Vajalikud SSL sertifikaadid tagab Tellija.

6.3. Apache Tomcat Versioon: 8.x

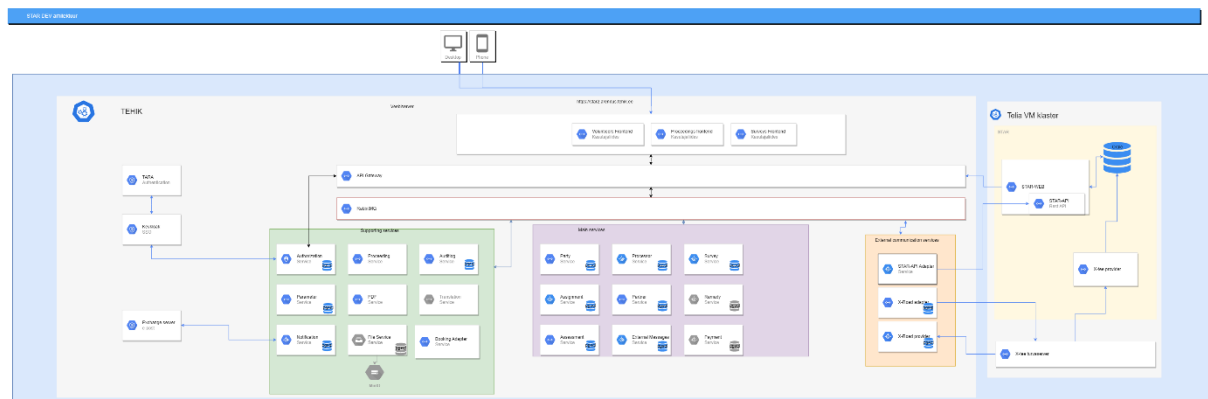
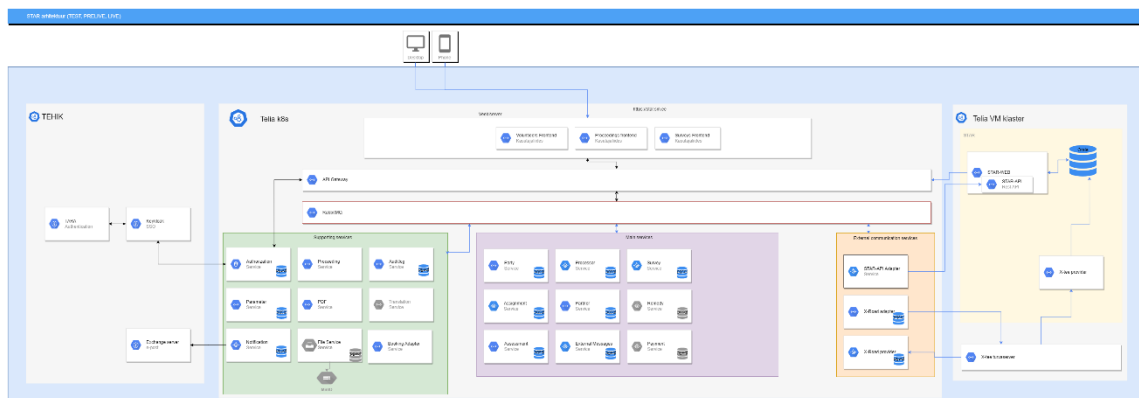
- 6.3.1. Konfiguratsioon ja nõuded: -
- 6.3.2. Operatsioonisüsteem: Red Hat Enterprise Linux 7 (RHEL)

6.4. Oracle Database Standard Edition 19c

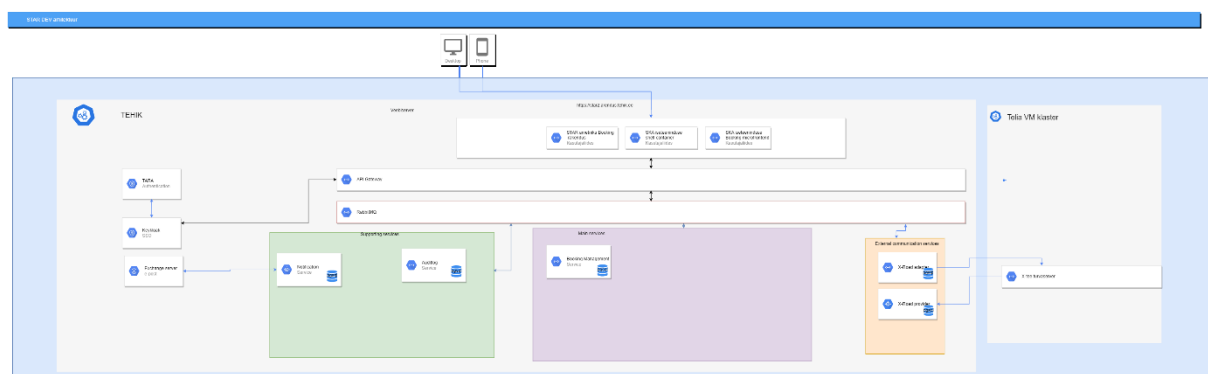
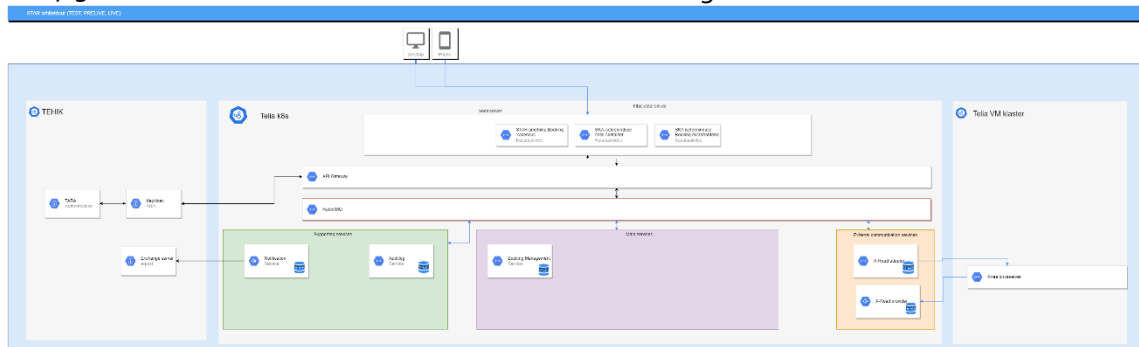
- 6.4.1. Konfiguratsioon ja nõuded: klasterdatud andmebaas.
- 6.4.2. Operatsioonisüsteem: Oracle Enterprise Linux 7 (OEL).
- 6.4.3. Andmebaasi eeldatav stardimaht (täna olemasolev andmestik) 1TB
- 6.4.4. Tellija tagab 2 (kaks) Oracle Database Standard CPU litsentsi. Süsteemi arengust tingitud vajaduse korral tagab lisalitsentsid Tellija.

7. STAR2 ametniku rakenduse arhitektuur – mikroteenused

- 7.1. Esimene etapp uuele arhitektuurile üleminekul saab olema lapse abivajaduse hindamise projekt (LAEH), mille arendused valmivad suvel 2022. Analüüsi üks eesmärk oli välja töötada STAR uue arhitektuuri kontseptsioon ja põhimõtted ning kaardistada esimeses etapis realiseeritavad arhitektuuritööd.
- 7.2. STAR2 ametniku rakenduse arhitektuur:



7.3. Sotsiaalkindlustusameti iseteeninduse broneeringute rakendus:



7.4. STAR tarkvarad, raamistikud ja platvormid

7.4.1. STAR₁ monoliitrakenduse komponendid:

Tarkvara	Toodang	Prelive	Test	Arendus
Apache HTTPD/2.4.6	X	X	X	

Apache Tomcat/8.5.4	x	x	x	x
JAVA/openjdk version "1.8.0_111"	x	x	x	x
Oracle Database 19c - 64bit	x	x	x	
LiquiBase	x	x	x	x
Oracle 18XE				x

7.4.2. STAR ja iseteeninduse mikroteenuste keskkond:

Tarkvara	Toodang	Prelive	Test	Arendus
Java/openjdk 17	x	x	x	x
Spring Boot	x	x	x	x
Next.js (React)	x	x	x	x
PostgreSQL 14	x	x	x	x
Kubernetes	x	x	x	x
FlyWay	x	x	x	x
Traefik Ingress	x	x	x	
Nginx Ingress				x
RabbitMq	x	x	x	x

8. Teenuse tehniline kirjeldus

8.1. Nõuded serveriruumile ja infrastruktuurile

8.1.1. Taitja majutab Tellija infosüsteemi kahes füüsiliselt eraldi asukohas ja eraldi aadressidel paiknevas serveriruumis. Serveriruumid ja nende vahelised ühendused peavad paiknema Eesti Vabariigi territooriumil ja serveriruumide minimaalne nõutud geograafiline vahemaa on vähemalt 1 km.

8.1.2. Serveriruumid peavad olema spetsiaalselt ehitatud serverite majutuseks ja vastama E-ITS turbeastmele H ning standardile ANSI/TIA-942 (Telecommunications Infrastructure Standard for Data Centers) tasemele Tier 3, mööndusega, et varugeneraator ei pea olema dubleeritud.

8.1.3. Taitja tagab STAR infosüsteemile turvatud (SSL) välise andmesideühenduse kiirusega vähemalt 100 Mbps (megabitti sekundis) ja serveriruumide vahel füüsilise, turvatud (VPN) dubleeritud ühenduse kiirusega vähemalt 1 Gbps (gigabitti sekundis).

8.1.4. Andmesideühenduse (internetiteenuse) taitja peab olema Eesti Interneti SA poolt akrediteeritud.

8.1.5. Serverite ja serveriruumide vaheline ühenduse kiirus peab olema piisav, et tagada teenustaseme nõuded. Tõrke korral peab olema tagatud teenuste üle viimine teise serveriruumi teenuse nõuetele vastava aja jooksul.

- 8.1.6. Täitja serveriruumid peavad olema ühendatud Tellija serveriruumidega läbi VPN ühenduse kiirusega vähemalt 1Gb/s. Tellija serveriruumid asuvad serverimajutuskeskustes kahes erinevas lokatsioonis Eesti Vabariigis.
- 8.1.7. Täitja peab kasutama riistvara, millel töötab ainult Tellija infosüsteem. Pakutaval riistvaral ei tohi töötada samal ajal kolmandate osapoolte infosüsteemid. Samuti ei tohi olla kolmandatel osapooltel ligipääse pakutavale riistvarale ja operatsioonisüsteemile.
- 8.2. STAR infosüsteemi majutus- ja tugiteenuste üldised (miinimum) nõuded
- 8.2.1. Täitja kohustub tagama STAR infosüsteemi kasutamise võimaluse veebikeskkonnas ning lepingu kehtivuse perioodil kindlustama keskkondade nõuetekohase (hankedokumentis ja teenusepassis kirjeldatud) funktsioneerimise.
- 8.2.2. Täitja tagab STAR infosüsteemi järgmised majutus- ja tugiteenused:
- 8.2.2.1. Serverite, võrgu- ja salvestusseadmete ressursid.
 - 8.2.2.2. Andmebaaside administreerimine ja monitooring.
 - 8.2.2.3. Infrastruktuuri administreerimine ja monitooring.
 - 8.2.2.4. Muudatuste haldus.
 - 8.2.2.5. Konsultatsioonid ja parendusettepanekud.
 - 8.2.2.6. Muud ühekordsed tegevused ehk lisatööd.
 - 8.2.2.7. Teenuse lõpetamisega seotud tööd lepingu lõppemisel.
- 8.2.3. Infosüsteem peab olema majutatud kahes serveriruumis põhimõttel primary site ja failover site. Täitja peab kirjeldama, mis vahenditega tagatakse vajaduse korral teenuste üle viimine teise serveriruumi vastavalt käideldavusnõuetele.
- 8.2.4. STAR infosüsteemi Oracle andmebaaside vaheliseks andmete reaajas sünkroniseerimiseks peab Täitja kasutama Oracle Data Guard tarkvara. Oracle Active Data Guard tarkvara võetakse kasutusele vajadusepõhiselt, mille kasutuselevõtu tingimused lepatakse eraldi kokku teenuseosutajaga.
- 8.2.5. Tellija poolt sätestatud STAR majutuse mittefunktsionaalsed nõuded on kirjeldatud dokumendis TEHIK MFN.
- 8.2.6. Lepingu lõppedes koostatakse andmete uude majutuskeskkonda migreerimise ja seejärel hävitamise protsess Tellija ja Täitja vahel. Andmete ülekolimise ja hävitamise järgselt vormistab majutusteenuse osutaja akti, millega kinnitatakse, et andmed on hävitatud.
- 8.2.7. Teenuse osutaja vahetumisel vormistatakse andmete ülekolimise (migratsiooni) läbiviimise järgselt kolmepoolne üleandmis-vastuvõtu akt (andja, vastuvõtja, omanik).
- 8.2.8. Teenuse lõppedes, uude keskkonda andmete migratsiooni ettevalmistamine ja läbiviimisel abi osutamine (Täitja pädevuse ulatuses) on majutusteenuse osa ja ei ole eraldi tasustatav.
- 8.3. Nõuded andmete hoidmisele
- 8.3.1. Kõik infosüsteemis töödeldavad andmed (andmebaasis ja rakendusserverites) peavad paiknema keskses andmesalvestusmassiivis, mille andmemahut on lihtsasti juurde tellitav. Andmesalvestusmassiiv peab võimaldama andmete kloonimist töökeskkonnast töökeskkonna-eelsesse ja testkeskkonda. Andmesalvestusmassiivi mis tahes komponendi rike ei tohi põhjustada andmekadu.
- 8.3.2. Täitja peab maandama andmesalvestusmassiivi riknemise riski, mis võib Tellijale tähendada ulatuslikku teenusekatkestust. Täitja kirjeldab pakkumuses, kuidas ja mis vahenditega (sh SAN seadmed ja andmesalvestusmassiivid) on tagatud mainitud riskide maandamine.
- 8.4. X-tee turvaserverid ja liidetud
- 8.4.1. STAR infosüsteemis on kasutusel x-tee versioon 6 raamistik.
- 8.4.2. X-tee eraldi turvaserverid töökeskkonna, toodanguelse keskkonna ja testkeskkonna tagab Täitja.

- 8.4.3. Majutuskeskkonnas peab olema STAR jaoks seadistatud eraldi adapterserverid tootmis-, toodangueelse ja testkeskkonnale (arenduse x-tee päringud suunatakse testkeskkonda) STAR andmekogu päringute vahendamiseks telistele süsteemidele läbi x-tee.
- 8.4.4. Turvaserverid peavad olema valmis võimalikeks lisanduvateks liidesteks.
- 8.4.5. Teenuse täitja peab tagama vajalike muudatuste rakendamise x-tee turva – ja adapterserverites vastavalt lisanduvate või muutuvate liideste vajadusele.
- 8.4.6. Tootmis- ja testkeskkonnas peab olema paigaldatud x-tee andmevahetuse jälgimiseks RIA andmejälgija (<https://github.com/e-gov/AJ>)
- 8.5. Muudatuste haldus
- 8.5.1. Arendusmuudatuste paigalduse õigustoodangu- ja toodangueelsesesse keskkonda on ainult täitjal, kui ei lepita kokku teisiti. Test- ja Koolituskeskkonda võib paigaldusi teostada Teenuse täitja, arendaja ja Tellija.
- 8.5.2. Arendusmuudatused valmistab ette Arendaja ja edastab paketeeritult koos paigaldusjuhendiga paigaldamiseks toodangu- ja toodangueelsesesse keskkonda. Paigalduspakettide, juhendite jm vajaliku informatsiooni edastamiseks ja paigaldustega seotud tegevuste dokumenteerimiseks, kasutatakse tellija tööde/projektide juhtimise keskkonda Jira.
- 8.5.3. Teenusetäitja paigaldab arendusmuudatuse lepingu raames vastavalt teenuse passile.
- 8.5.4. Toodangukeskkonda tehakse üldjuhul kuni 8 arendusmuudatuse tarnet kuus. Toodangueelsesesse keskkonda kuni 16 arendusmuudatuse tarnet kuus. Test- ja koolituskeskkonda tehakse üldjuhul kuni 20 arendusmuudatuse tarnet kuus. Arendusmuudatuse töökeskkonda viiakse sisse väljaspool aktiivset tööaega.
- 8.5.5. Teenusetäitja peab vastavalt tellimusele käivitama parandusskripte vigade tuvastamiseks ja parandamiseks.
- 8.5.6. Arendusmuudatuste paigalduse aja kooskõlastab Täitja Tellijaga.
- 8.5.7. Täitja poolt arendusmuudatuse paigalduse ebaõnnestumisel vastutab Täitja süsteemi taastamise (rollback) eest.
- 8.5.8. Täitja uuendab toodangueelse ja testkeskkonna andmeid toodangukeskkonna andmetega Tellija tellimusel kui tarnejuhend seda ette näeb, kuid mitte rohkem kui punktis 8.5.4 kirjeldatud tarnete arv.
- 8.5.9. Täitja peab värskendama STAR statistikabaasi iga öö. Andmed laetakse STAR toodangukeskkonna andmebaasist.
- 8.5.10. Teenusetäitja tagab Tellija tellimisel arenduspartneritele ligipääsu test- ja toodangueelsele keskkonnale (andmebaasile, rakendusserverile) 2 tööpäeva jooksul.
- 8.5.11. Teenusetäitja tagab tellija tellimisel arenduspartneritele ligipääsu sulgemise test- ja toodangueelsele keskkonnale esimesel võimalusel, kuid mitte hiljem kui 2 tööpäeva jooksul.
- 8.5.12. Täitja peab kindlustama Tellija tellimisel (andme)halduritele / rakenduse administraatoritele lugemisõigustes (read only) ligipääsud kõikide STAR keskkondade serverite operatsioonisüsteemi konfiguratsioonifailidele ja andmebaasidele.
- 8.6. Varundamine ja teenuse taastamine
- 8.6.1. Täitja teeb majutuskeskkonnas olevatest süsteemidest regulaarselt varukoopiaid selliselt, et oleks tagatud teenuse passis sätestatud tingimuste täitmine. Täitja peab pakkumises kirjeldama, et milliste vahendite ja meetoditega tehakse varukoopiaid.
- 8.6.2. Varukoopiaid tehakse rakendusi seiskamata st, et tellija infosüsteemide käideldavus ei ole varukoopiate tegemise ajal mõjutatud. Varundust teostatakse väljaspool infosüsteemi tööaega.
- 8.6.3. Varukoopiad tuleb salvestada töökeskkonnast eraldi asuvatele andmekandjatele, mis asuvad erinevas füüsilises lokatsioonis. Varukoopiad ja nende allika vaheline andmevahetus peab olema krüpteeritud.
- 8.6.4. Täitja on kohustatud hoidma töökeskkonna varundatud andmeid järgnevalt:

- 8.6.4.1. Vähemalt kahe viimase kuukoopia.
- 8.6.4.2. Vähemalt neli viimast nädalakooptiat.
- 8.6.4.3. Vähemalt viis viimast tööpäevakooptiat.
- 8.6.5. Kuukoopiad on planeeritud kopeerida täiendavalt andmesaatkonda. Ajakava ning täpne tehniline lahendus töötatakse välja ja realiseeritakse koos eduka Täitjaga töö käigus lepinguperioodi alguses.
- 8.6.6. Andmekadu põhjustavat intsidenti käsitletakse kui erakorralist intsidenti. Erakorralise intsidendi korral on lubatud teenuse järjestikune seisak kuni 4 tundi ja summaarne seisak kuni 4 tundi nädalas ja kuni 6 tundi kalendrikuus. Pärast intsidendi lahendamist ja/või andmete taastamist esitab Täitja Tellijale detailse raporti, kus toob välja intsidendi põhjuse, mis põhjustas andmekadu ning meetmed selliste juhtumite vältimiseks või esinemise tõenäosuse vähendamiseks tulevikus.
- 8.6.7. Täitja töötab pärast iga keskkonna käivitamist ühe kuu jooksul välja vastava keskkonna taasteplaani ja esitab selle tellijale ülevaatamiseks ja kinnitamiseks. Taasteplaani peab sisaldama tegevuskava ja süsteemi üldist arhitektuuri kirjeldust visuaalsel kujul. Olulised infrastruktuuri komponendid (serverid, võrguseadmed jne) peavad olema kirjalikult lahti seletatud.
- 8.6.8. Täitja testib taasteplaani ajakohasust, kui toimub muudatus tellija infosüsteemiga seotud infrastruktuuris, kuid mitte harvemini kui üks kord aastas. Täitja kooskõlastab tellijaga testi läbiviimise aja ning esitab Tellijale pärast testi läbiviimist raporti, kus märgib ära taasteplaani vastavuse tegelikule olukorrale ja plaanist leitud puudused. Puudused tuleb kõrvaldada Tellijaga kokkuleppel mõistliku aja jooksul ning seejärel korraldada uus taasteplaani test.
- 8.7. Monitooring
 - 8.7.1. Täitja tagab tsentraliseeritud tehnilise toe teenuse, mis on avatud 24 tundi ööpäevas ja seitse päeva nädalas, mille kaudu sooritatakse mitmesuguseid süsteemiga seotud järelevalve, muudatuste ja veahalduse menetlustoiminguid.
 - 8.7.2. Tehnilise toe teenuseid osutatakse osana majutusteenustest, kus kõik süsteemihoiatused saadetakse tsentraliseeritud 24 tundi toimivale tehnilisele toele (sh võrgu, serveri ja rakenduse hoiatused).
 - 8.7.3. Kõik keskkonnad peavad olema Täitja poolt monitooritud kogu lepinguperioodi vältel.
 - 8.7.4. Täitja võimaldab Tellijale ja Tellija poolt nimetatud arendajale juurdepääsu monitooringuinfole või edastab monitooringuteated Tellija poolt etteantud meiliaadressile.
 - 8.7.5. STAR logidele peab Tellijal olema ligipääs üle veebiliidese. Logide haldus peab töötama täitja majutuse keskkonnas (on premise).
 - 8.7.6. Täitja installeerib vajadusel või Tellija palvel serveritesse täiendavad monitooringuagendid, mis koguvad infot serverite ja rakenduste seisundi kohta. Tellijal on kasutusel monitooringu süsteem Prometheus ja Grafana.
 - 8.7.7. Täitja monitoorib serverites asuvate infosüsteemide tööd vähemalt järgmiste komponentide osas:
 - 8.7.7.1. Andmesideühenduse olemasolu tellija serverite ja infosüsteemide vahel.
 - 8.7.7.2. Serverite riistvaraliste komponentide töökorras olek.
 - 8.7.7.3. Serverite protsessorite ja mälu kasutus.
 - 8.7.7.4. Kõvaketaste täituvus.
 - 8.7.7.5. Süsteemi load (UNIX süsteemide puhul).
 - 8.7.7.6. Andmebaasisüsteemi töökorras olek.
 - 8.7.7.7. Andmebaasile eraldatud ressursside olemasolu.
 - 8.7.7.8. Varukoopiate tegemise õnnestumine.
 - 8.7.7.9. Monitooringusüsteemi töökorras olek.
 - 8.7.8. STAR infosüsteemi rakenduste monitooring

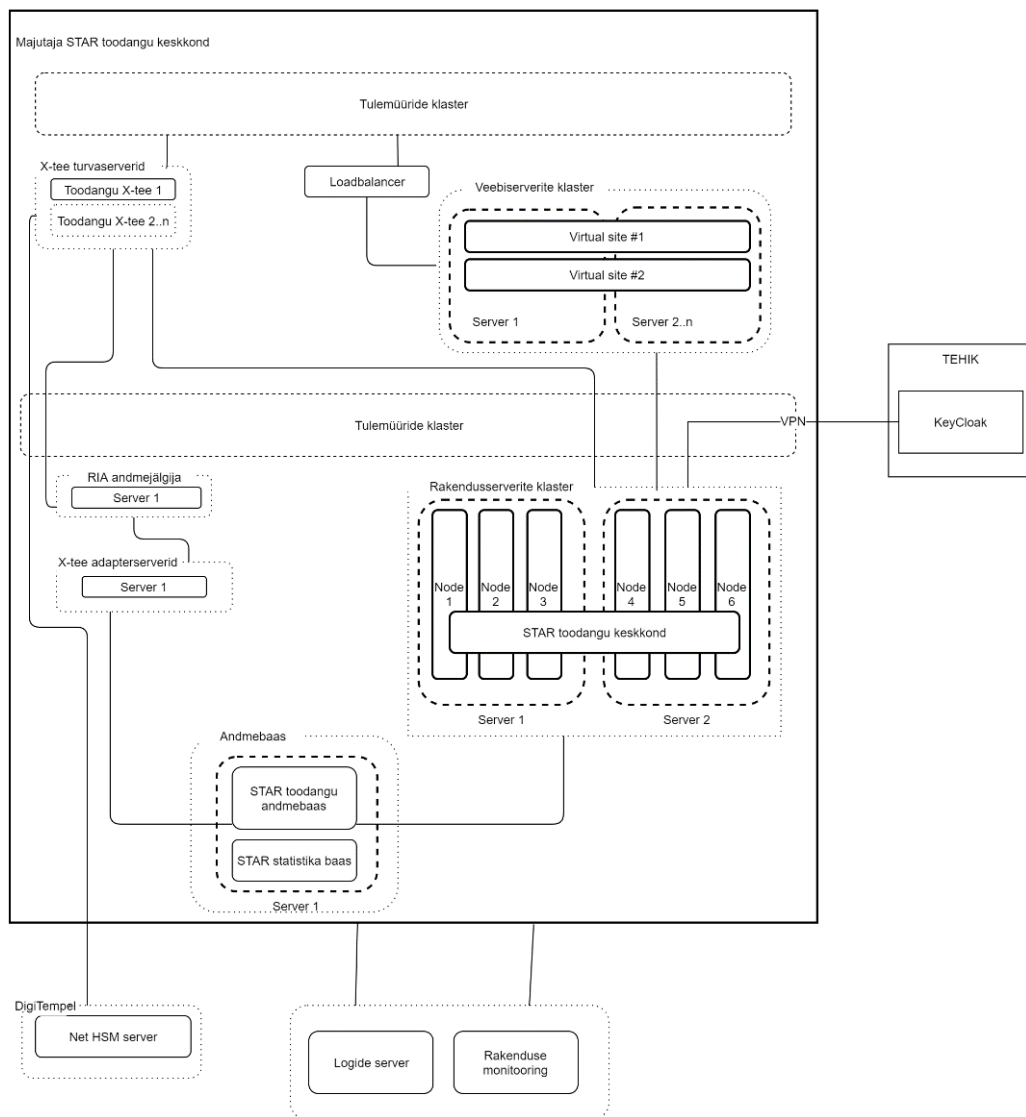
- 8.7.8.1. Taitja poolset STAR rakenduse monitooringut ei nõuta. Taitjal peab olema valmisolek integreerida oma keskkonda Tellija poolt kasutatavad rakenduse monitooringu vahendid (agendid vms).
- 8.7.9. Teenuse tehniline tugi
 - 8.7.9.1. Taitja peab tagama kasutajatoe (ühtne kontaktpunkt, telefoni number, e-mail ja/või avalik portaal) vastavalt Teenuse passis toodud nõuetele.
 - 8.7.9.2. Taitja peab teavitama Tellijat kriitilistest ja keskmise taseme vigadest koheselt ja asuma teenuse nõutud tingimustele vastavust taastama.
 - 8.7.9.3. Kui tõrget ei ole võimalik teenuse passis nõutud aja jooksul lahendada, peab Taitja esitama põhjendused ja lahendusettepanekud.
 - 8.7.9.4. Kriitilise taseme tõrkeks loetakse olukorda, kus STAR toodangukeskkonna tervikuna või oluliste komponentide, s.h andmevahetused teiste infosüsteemidega, kasutamine ei ole võimalik.
 - 8.7.9.5. Keskmise taseme tõrkeks loetakse olukorda, kus STAR toodangukeskkonna kasutamine on oluliselt häiritud.
 - 8.7.9.6. Madala taseme tõrkeks loetakse olukorda, kus STAR toodangukeskkonna kasutamine on võimalik, kuid on häiritud.
- 8.7.10. Aruandlus ja infovahetus
 - 8.7.10.1. Taitja esitab majutusteenuse osutamise kohta igakuiselt ülevaate eelmise kuu kohta, mis sisaldab vähemalt järgmist informatsiooni:
 - 8.7.10.1.1. Süsteemi komponentide käideldavus vastavalt teenuste passi nõuetele.
 - 8.7.10.1.2. Perioodi vältel toimunud intsidendid koos algus- ja lõpuajaga, juurpõhjusega (kui on selgunud) ning kirjeldusega, kuidas neid edaspidi vältida.
 - 8.7.10.1.3. Perioodi vältel tehtud plaanilised tööd.
 - 8.7.10.1.4. Muudatuste logi.
 - 8.7.10.1.5. Tellija poolt perioodi jooksul esitatud pöördumiste staatus, mis sisaldab ka lahendamata pöördumisi eelmistest perioodidest.
 - 8.7.10.1.6. Taitja poolsed ettepanekud infosüsteemi ja majutuse parendamiseks ning teostamiskava.
 - 8.7.10.2. Aruandlus peab olema Tellija kontaktisikutele kättesaadavaks tehtud veebi kaudu või e-kirja teel.
 - 8.7.10.3. Taitja peab võimaldama Tellijal tellida tellimustööna täiendava tasu eest ühekordseid raporteid nt andmebaasi detaileid koormusraporteid.
 - 8.7.10.4. Taitja ja Tellija vaheline töökeel on eesti keel.
- 8.8. Vajalikud ligipääsud Tellijale
 - 8.8.1. Teenuse taitja ja Tellija võrkude vahele tuleb rajada VPN tunnel. Kogu osapoolte vaheline andmete liikumine peab toimuma läbi VPN tunneli.
 - 8.8.2. Teenuse taitja peab kindlustama ühenduse Tellija SSO teenusele.
 - 8.8.3. Teenuse taitja peab kindlustama Tellija andmeaida andmete laadimise süsteemile (Tellija teenus) ligipääsu STAR toodangukeskkonna andmebaasile.
 - 8.8.4. Teenuse taitja peab kindlustama Tellija andmehalduritele otseligitipääsud STAR kõigi keskkondade andmebaasidele.
 - 8.8.5. Teenuse taitja peab pakkuma FTP (või samaväärne) serveri teenust, mille kaudu edastab Tellija installeerimiseks vajalikud paketid.
- 8.9. Nõuded monoliit arhitektuuri tehnilisele ülesehitusele
 - 8.9.1. STAR Toodangukeskkond:
 - 8.9.2. Kasutatavad rakendusserverid peavad olema eraldatud andmebaasiserverist;
 - 8.9.3. Rakendusserverid peavad võimaldama koormuse jaotamist vähemalt kahe serveri vahel;

- 8.9.4. Igas rakendusserveris peab olema töösse rakendatud vähemalt kolm Java virtuaalserverit (JAVA Virtual Machine).
- 8.9.5. Keskkonnas peavad olema automaatse ümberlülitusega dubleerivad koormusjaoturid.
- 8.9.6. Koormusjaoturid peavad toetama lisaks koormuse jaotamisele ka SSL ühenduste termineerimist (SSL Offloading).
- 8.9.7. STAR toodangueelne- ja testkeskkond:
- 8.9.8. Toodangueelne keskkond (prelive) peab olema Toodangukeskkonnaga sarnase konfiguratsiooniga, kuid võib olla ilma dubleeriva rakendusserverita.
- 8.9.9. Rakendusserveris peab olema töösse rakendatud vähemalt kolm Java virtuaalserverit (JAVA Virtual Machine).
- 8.9.10. Test- ja koolituskeskkond võib olla ilma dubleeriva rakendusserverita ja vähendatud Java virtuaalserverite arvuga.
- 8.9.11. Majutuskeskkond peab olema kaitstud automaatse ümberlülitusega dubleeritud tulemüüriga;
- 8.10. Tellija tarkvara profiil STAR keskkondadele
 - 8.10.1. Oracle Database 19g Standard Edition
 - 8.10.2. Tellijal on olemas kahe (2) protsessori Oracle Standard Edition litsents koos toega.
 - 8.10.3. Varukoopiate tarkvara valib Taitja teenuse nõuetest tulenevalt;
 - 8.10.4. Toodangukeskkonna nädisarhitektuur on toodud punktis 11.
- 8.11. Litsentsid ja sertifikaadid
 - 8.11.1. Serverite operatsioonisüsteemi tarkvarad peavad olema kaetud tootjapoolse tarkvaratoega lepingu perioodi vältel. Vajalikud litsentsid tagab Taitja.
 - 8.11.2. Infosüsteemi tööks vajalikud litsentsid ja tootja toe tagab Tellija;
 - 8.11.3. Süsteemi arengust tingitud vajaduse korral tagab infosüsteemi tööks vajalikud lisalitsentsid Tellija;
 - 8.11.4. Turvalise ühenduse loomiseks vajalikud SSL sertifikaadid tagab Tellija;
 - 8.11.5. Kõik keskkondade tööks vajalikud sertifikaadid ja nende kogused tuleb loetleda Taitja poolt ja esitada Tellijale tööks vajalike sertifikaatide soetamiseks.

9. Nõuded mikroteenuste arhitektuuri tehnilisele ülesehitusele

- 9.1. Kubernetese klastrid eraldi toodangu-, toodangueelse ja testkeskkondade jaoks.
- 9.2. Testikeskkonna klastrit võib vajadusel kasutada ka arenduskeskkonnana. Samaaegselt on testkeskkonna klastris STAR test ja arenduse rakendused.
- 9.3. Kubernetese klastreid peab saama laiendada lisaserveritega majutuse perioodi ajal;
- 9.4. Kubernetese klatri füüsilised serverid ei tohi olla jagatud teiste Teenuse taitja klientidega;
- 9.5. Soovituslik on kasutada Rancher Kubernetes Engine (RKE) Kubernetes distributsiooni;
- 9.6. Rancher kasutajaliides Kuberneteses rakenduste haldamiseks;
- 9.7. STAR rakendused Java ja JavaSkript keeltes;
- 9.8. PostgreSQL andmebaasid;
- 9.9. Redis andmebaasid;
- 9.10. RabbitMQ sõnumivahetus;
- 9.11. Minio S3 failisalvestus;
- 9.12. Matomo kasutajate käitumise monotooring;
- 9.13. Taristuteenused:
- 9.14. Kõrgkäideldav salvestusteenus klatri piires;
- 9.15. Sertifikaatide väljastus ja haldus (cert-manager);
- 9.16. Teenuseid kirjeldavad YAML failid paiknevad Tellija Gitlab lähtekoodi repositooriumis;
- 9.17. Docker konteinerite registrid paikneb Tellija juures.

10. Toodangukeskkonna näitlik arhitektuur



IV. Lisad

1. *Tehnilise kirjelduse lisad on:*

- 1.1. Teenuse pass SKAIS₁;
- 1.2. Teenuse pass SKAIS₂;
- 1.3. Teenuse pass STAR;
- 1.4. TEHIK MFN 2024.