RAHVUSRAAMATUKOGU RAAMATUKOGUDE MITTEFUNKTSIONAALSED NÕUDED 2025-1

ÜLDNÕUDED
Dokument ja selle lisad määratlevad mittefunktsionaalsed nõuded Rahvusraamatukogu (RaRa) raamatukogude uutele infosüsteemidele ja nendega seotud dokumentatsioonile.
Nõuded on kohustuslikud ka olemasolevate infosüsteemide lisaarendustele ja versiooniuuendustele mahus, mis on lisaarenduse ja versiooniuuenduste käigus võimalik.
Nõuded on kohustuslikuks täitmiseks kõikidele tulemitele.
Alternatiivsete, käesolevas mittefunktsionaalsete nõuete dokumendis puuduvate tehnoloogiate, vahendite ja metoodikate valikul rakendab hankija järgnevaid kriteeriume: sobivus olemasoleva infrastruktuuriga, platvormi tehnoloogilised omadused, kompetentsi olemasolu ja kättesaadavus tööjõuturul.
Kui mõnda konkreetselt kohalduvat nõuet ei ole pakkuja arvates võimalik või otstarbekas täita, tuleb selle mittetäitmise fakt ja põhjendus pakkumuses välja tuua. Kõik erikokkulepped fikseeritakse tellijaga kirjalikku taasesitamist võimaldaval viisil.

NÕUDE KIRJELDUS	MÄRKUS
Vastavus standarditele ja seadusandlusele	
Lahendus peab vastama „Eesti avaliku teabe masinloetava avalikustamise roheline raamat“ sõnastatud põhimõtetele ja nõuetele.	Dokument on leitav: https://www.aki.ee/sites/default/files/documents/2024-03/avaliku-teabe-masinloetava-avalikustamise-roheline-raamat-20141125.odt
Lahendus peab vastama „Aadressiandmete süsteem“ määruses kehtestatud aadressiandmete nõuetele	Määrus on leitav https://www.riigiteataja.ee/akt/103122022011?leiaKehtiv
Lahenduses tuleb tegevusalade määramiseks kasutada Eesti Majanduse Tegevusalade Klassifikaatorit (EMTAK 2025).	Klassifikaator on leitav: https://emtak.rik.ee/EMTAK/block/resource/MTU5MjQ4NzE5Nw==/EMTAK_2025.pdf
Lahendus peab vastama „Avaliku teabe seaduses“ kehtestatud teabe avalikustamise ja juurdepääsu võimaldamise nõuetele.	Seadus on leitav: https://www.riigiteataja.ee/akt/114032011019?leiaKehtiv
Lahendus peab vastama „Riigi infosüsteemi haldussüsteem“ (edaspidi RIHA) esitatud nõuetele ja reeglitele.	Määrus on leitav: https://www.riigiteataja.ee/akt/12933746?leiaKehtiv
Lahendus peab vastama “Võrgu- ja infosüsteemide küberturvalisuse nõuded“ määruses esitatud nõuete alusel määratud turbeastmele M, kui ei ole nõutud teisiti.	Määrus on leitav: https://www.riigiteataja.ee/akt/113122022030?leiaKehtiv. Täpne rakendamise ulatus lepitakse kokku lähtuvalt konkreetsest infosüsteemist. Eesti infoturbestandard https://www.riigiteataja.ee/akt/121122022034?leiaKehtiv https://eits.ria.ee/
Loodav lahendus peab vastama isikuandmete kaitse üldmäärusele ja direktiivile andmete edastamisel politseikoostöö ja õigusalase koostöö valdkonnas sätetele.	Isikuandmete kaitse üldmäärus ja direktiiv on leitavad: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&from=ET http://eur-lex.europa.eu/legal- content/ET/TXT/?uri=CELEX:32016L0680
Lahenduses peavad X-tee teenused olema realiseeritud vastavalt RIA kirjeldatud nõuetele.	Nõuded on leitavad: https://www.ria.ee/riigi-infosusteem/andmevahetuse-platvormid/andmevahetuskiht-x-tee

Lahendus peab vastama "Infosüsteemide andmevahetuskiht" määruses kirjeldatud põhimõtetele.	Määrus on leitav: https://www.riigiteataja.ee/akt/127092016004?leiaKehtiv
Digiallkirjastamislahenduse kasutamisel kasutatakse riigi allkirjastamisteenust.	https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/digiallkirja-serverteenused
Kuupäeva ja aja (kuupäev, kellaaeg, ajaintervall) talletamisel teksti kujul tuleb aluseks võtta ISO 8601 standardis kirjeldatud põhimõtted.	Põhimõtted on leitavad: https://en.wikipedia.org/wiki/ISO_8601 või http://www.w3.org/TR/NOTE-datetime
Veebirakenduse kasutajaliides peab vastama vähemalt WCAG 2.1 tasemele AA.	Soovituste kogum on leitav: http://www.w3.org/TR/WCAG21
Veebipõhine kasutajaliides peab ühilduma HTML ja CSS standarditega.	Standardiseerimata HTML ja CSS kasutamine peab olema eelnevalt tellijaga kooskõlastatud.
Arhitektuur	
Realiseeritud lahendus peab tellija poolt kinnitatud arhitektuurile vastavalt töötama tellija poolt nõutud funktsionaalsete ja mittefunktsionaalsete nõuete ulatuses.	
Arhitektuuri kirjeldus peab sisaldama C4 või analoogseid diagramme. Diagrammid peavad kajastama süsteemi ülesehitust ja komponente, nende omavahelist suhtlust sealhulgas andmevooge.	https://c4model.com/
Kõik infosüsteemis kasutatavad komponendid peavad olema tuvastatavad, põhjendatud ja dokumenteeritud.	
Kõik lahenduses kasutatavad kolmanda osapoole komponendid (nt välised süsteemid, teegid) peavad olema tuvastatavad ja dokumenteeritud.	

Liidesed väliste süsteemidega peavad olema standardsed (allutatud sarnastele reeglitele) ja liidestamise detailid peavad olema dokumenteeritud.	
Rakenduse liidesed peavad olema tõrkekindlad.	Lõppkasutaja peab saama jätkata rakenduse kasutamist ulatuses, mis on protsessiliselt võimalik. Süsteem peab tõrke korral võimalikult lühikese aja jooksul väljastama asjakohase veateate.
Infosüsteemide platvormid (nt rakendusserver, andmebaas) ja topoloogia peavad olema tellijaga kooskõlastatud enne reaalse tarkvaraarenduse algust.	Detailne infrastruktuur on kirjeldatud KuM haldusala tehnoloogilises profiilis.
Kõik arendamisel kasutatud komponendid peavad vastuvõtmise hetkel olema viimased stabiilsed versioonid.	
Infosüsteemi ülesehituses peab kasutama kolmekihilist arhitektuuri: andmekiht, kontrollerkiht (äriloogika) ja esitluskiht.	
Infosüsteem peab olema üles ehitatud nii, et eessüsteemid (*front-end*) ja tagasüsteemid (*back-end*) on arhitektuuriliselt selgelt lahutatud.	
Liideste loomisel teiste süsteemidega ei tohi liidestuda otse eessüsteemist (front-end) vaid läbi rakenduse tagasüsteemi (back-end).	
Andmebaasid ja rakendused peavad kasutama UTF-8 kodeeringut ja UTC aega.	
Lahendused peavad olema projekteeritud laiendatavana ja edasi arendatavana.	

Komponendid peavad olema sõltumatud ja taaskasutatavad.	
Rakendust peab saama liigutada ilma ümberprogrammeerimiseta erinevate domeenide, domeenisaitide ja keskkondade vahel.	
Rakendusel peab olema haldusliides.	Haldustoimingute tegemine otse andmebaasis peab olema viidud miinimumini. Peakasutajal peab olema selge ülevaade kasutajate õigustest.
Kui rakendused saadavad e-kirju, siis peavad nad selleks kasutama välist e-posti serverit.	
Rakendus peab suutma kasutada keskkonnamuutujaid.	
Arhitektuur peab olema modulaarne, teenuste põhine.	
Ebaõnnestunud logimiste arvu peab saama piirata ajaühiku kohta.	Muudatusi (logimiste arv, ajaühik) peab saama seadistada konfiguratsioonifailis.
Klientrakendus ei tohi teostada otsepöördust andmebaasi poole.	Peab kasutama rakendusserverit või adapterit.
Rakenduse failid, mis ei tohi olla kasutajale nähtavad, peavad olema kaitstud (rakenduse kasutajale mittekättesaadavates) kaustades.	
Sorteerimisreeglistik peab vastama eesti tähestikule, tõstutundlikkus peab olema väljalülitatud.	
Lihtsamatele päringutele (nt ühe konkreetse andmeobjekti otsing) peab loodav lahendus vastama maksimaalselt 2 sekundi jooksul. Keerulisemate päringute (nt nimekirja filtreerimine) puhul on ajaline piirang 5 sekundit.	

Loodav lahendus peab võimaldama serveri poolt lõppkasutajale tagastatavate andmeobjektide arvu piirangut ja/või mahukate andmekomplektide lehekülgjaotust (*pagination / positioned lazy loading*).	
Kui rakenduse toimimiseks on vajalik autentimine, tuleb selleks kasutada RIA TARA, vajadusel ka RIA GovSSO-d.	https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/kesksed-autentimisteenused https://e-gov.github.io/TARA-Doku/
Turvalisus, sh infoturve	
Välistele kasutajatele mõeldud rakendustes ei ole kasutajanime ja parooliga autentimine lubatud.	E-ITS Veebirakenduste arendus CON.10.M1 Turvaline autentimine veebirakenduses Veebirakendused APP.3.1.M1 Veebirakenduste autentimine
Rakenduse autentimise jõustamine peab toimuma serveri poolel.	Veebirakenduste arendus CON.10.M1 Turvaline autentimine veebirakenduses
Ebaõnnestunud autentimine peab lõppema viisil, mis ei jäta ründajale võimalust rakendusse sisse tungida ega tohi võimaldada kasutajale ligipääsu süsteemi toimimise informatsioonile.	E-ITS Veebirakenduste arendus CON.10.M10 Tundliku taustainfo avaldamise piiramine
Rakendus (sh konteineris käitatav) ei tohi töötamiseks vajada juur*(root)*/administraatori õigusi.	E-ITS Identiteedi- ja õiguste haldus ORP.4.M2 Õiguste andmine, muutmine ja tühistamine
Autentimist võimaldav informatsioon (nt autentimissaladused, API võtmed, salasõnad) ei tohi sisalduda lähtekoodis.	E-ITS Tarkvaraarendus CON.8.M5 Turvaline süsteemi kavandamine
Rakenduse kasutajale kuvatavad URL-id ei tohi sisaldada isikuandmeid.	E-ITS Veebirakenduste arendus CON.10.M1 Turvaline autentimine veebirakenduses CON.10.M7 Konfidentsiaalsete andmete kaitse
Rakendusel peab olema konfigureeritav kasutajaseansi aegumise aeg.	E-ITS Veebirakenduste arendus CON.10.M3 Turvaline seansihaldus

Süsteemist väljumine peab toimuma kasutajale üheselt arusaadaval ja turvalisel viisil. Seansist väljumine toimub kahel viisil: kasutaja seansi lõpetab süsteem, sest seanss on olnud pikem kui süsteemile seadistatud vaikimisi ülempiir või kasutaja lõpetab seansi omal soovil.	E-ITS Veebirakenduste arendus CON.10.M3 Turvaline seansihaldus
Süsteem peab teavitama kasutajat seansi lõppemisest.	E-ITS Veebirakenduste arendus CON.10.M3 Turvaline seansihaldus
Kasutajal peab olema igal süsteemi kasutamise ajahetkel võimalik seanss omal soovil lõpetada.	E-ITS Veebirakenduste arendus CON.10.M3 Turvaline seansihaldus
Iga eduka süsteemi sisselogimise (autentimise) korral tuleb alati luua unikaalne seansi identifikaator (*session ID*)	E-ITS Veebirakenduste arendus CON.10.M3 Turvaline seansihaldus
Seansi identifikaator ei tohi kajastuda ressursilokaatoris (URL-is), veateadetes ega logides.	E-ITS Veebirakenduste arendus CON.10.M3 Turvaline seansihaldus
Seansi identifikaator peab olema piisava pikkusega, juhuslik ja unikaalne kogu aktiivse seansi jooksul.	E-ITS Veebirakenduste arendus CON.10.M3 Turvaline seansihaldus
Rakendus ja selle komponendid peavad võimaldama keskkondade lahusust (nt arendus-, test- ja toodangu keskkond).	E-ITS Tarkvaraarendus CON.8.M3 Sobiva tarkvaraarenduskeskkonna valimine CON.8.M7 Tarkvara testimine tarkvaraarenduse käigus
Andmebaasis olevate rakenduste kontod peavad omama ainult minimaalselt rakenduse tööks vajalikke õigusi.	E-ITS Identiteedi- ja õiguste haldus ORP.4.M2 Õiguste andmine, muutmine ja tühistamine
Krüptoalgoritmide ja räsifunktsioonide kasutamisel tuleb järgida RIA veebilehel avaldatud krüptograafiliste algoritmide elutsükli uuringu värskeimas versioonis toodud soovitusi ja põhimõtteid.	Uuring on leitav: https://ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/uuringud-ja-analuusid#kruptouuringud
Andmebaasi ja rakenduse vaheline suhtlus peab olema krüpteeritud kui suhtlus toimub üle avaliku võrgu.	E-ITS Tarkvaraarendus CON.8.M5 Turvaline süsteemi kavandamine Veebirakendused APP.3.1.M14 Konfidentsiaalsete andmete kaitse
Rakenduses peab olema tagatud võimekus välja vahetada aegunud ja ebaturvalisi krüptoalgoritme.	Krüptoalgoritmide väljavahetamine peab olema dokumentatsioonis kirjeldatud. E-ITS

	Krüptokontseptsioon CON.1.M1 Krüptomehhanismide kasutuselevõtu kavandamine
Kõik paroolid ja salasõnad peab rakendus salvestama kas räsituna ja soolatuna või krüpteeritud kujul.	E-ITS Identiteedi- ja õiguste haldus ORP.4.M23 Nõuded paroole töötlevatele IT-süsteemidele Tarkvaraarendus CON.8.M5 Turvaline süsteemi kavandamine Veebirakenduste arendus CON.10.M7 Konfidentsiaalsete andmete kaitse
Kõik võtmed ja salasõnad peavad olema asendatavad ning need tuleb toodangu keskkonna installatsiooni ajal luua või asendada.	E-ITS Identiteedi- ja õiguste haldus ORP.4.M23 Nõuded paroole töötlevatele IT-süsteemidele
Võrguliikluse krüpteerimiseks peab olema HTTPS valmidus.	Veebirakenduste arendus CON.10.M7 Konfidentsiaalsete andmete kaitse
Tarkvara iga versioon peab läbima koodikvaliteedikontrolli süsteemi SonarQube või samaväärse lähtekoodi analüüsi vahendiga nii, et pole Security, Blocker ja Critical tüüpi vigu.	
Tarkvara iga versioon peab olema kontrollitud Common Vulnerabilities and Exposures (CVE®) järgi ja ei tohi sisaldada teadaolevaid turvanõrkuseid.	https://cve.mitre.org/
Rakendusse ja andmetele tohib olla ligipääs ainult dokumenteeritud ning kirjeldatud teid mööda ja dokumenteeritud autentimisprotseduure kasutades.	E-ITS Veebirakenduste arendus CON.10.M2 Veebirakenduse juurdepääsu reguleerimine CON.10.M7 Konfidentsiaalsete andmete kaitse
Kui rakendus kasutab brauseri küpsiseid (*session cookie*) või muid tehnoloogiaid (nt local storage jm), mis salvestavad kasutaja arvutisse informatsiooni, siis tuleb kasutajat sellest eelnevalt teavitada.	E-ITS Isikuandmete kaitse CON.2.M1 Isikuandmete kaitse kavandamine CON.2.M24 Privaatsusseadistused veebilehtedel
Rakendus ei tohi teostada X-tee päringut otse kasutaja arvutist.	

Rakendusserver ja andmebaas peavad olema võimelised töötama eraldi serveritel.	
Veebirakenduse kõik viited failidele ja kataloogidele peavad olema ilma absoluutse failiteeta.	E-ITS Veebirakenduste arendus CON.10.M10 Tundliku taustainfo avaldamise piiramine
Kui rakenduse poolt töödeldavate andmete konfidentsiaalsuse klass on 2 või kõrgem, peab rakenduse andmemudel võimaldama lihtsate vahenditega andmete anonümiseerimist.	
Välistele kasutajatele mõeldud veebilehega rakendused peavad olema kaitstud keelatud päringute eest.	E-ITS Veebirakenduste arendus CON.10.M2 Veebirakenduse juurdepääsu reguleerimine CON.10.M6 Kaitse veebirakenduste volitamata automaatse kasutamise eest CON.10.M7 Konfidentsiaalsete andmete kaitse
Kui rakendus võimaldab mitteautenditud kasutajal edastada andmeid, tuleb need andmed puhastada XSS filtriga.	E-ITS Veebirakenduste arendus CON.10.M15 Päringuvõltsingu takistamine
Kui on nõutud andmete jälgimise rakendamine tuleb selleks kasutada RIA poolt pakutavat andmejälgijat.	https://github.com/e-gov/AJ/
Loodava lahenduse realiseerimisel tuleb arvestada, et rakendus paigaldatakse Kubernetese klastrisse.	
Rakenduste paigaldused tehakse Helm skriptidega.	
Juhul, kui rakendus loob faile või võimaldab failide üles laadimist tuleb failide salvestamiseks kasutada S3 tehnoloogiat.	E-ITS Veebirakendused APP.3.1.M4 Andmete ja sisu kasutamise piiramine
Lähtekood	

Lähtekood tarnitakse koodivaramu koodihoidla KuM sektsiooni. Koodihoidlasse üleslaaditud lähtekood peab olema täielik ehk sellest saab koostada ja paigaldada täisfunktsionaalse rakenduse.	https://koodivaramu.eesti.ee/kultuuriministeerium
Üleantavad versioonid peavad olema ilmutatud kujul harudena (*releases)* või minimaalselt viitedetega (*tags)*, milliste nimetused kajastavad üleantavaid versioone.	
Koodihoidla failide vaikimisi kodeering on UTF-8 ilma BOM signatuurita.	Välja arvatud juhtudel, kui tehnilises kirjelduses on tehnoloogiliste eripärade või muude piirangute tõttu sätestatud teisiti.
Koodihoidla failide realõpud LF tüüpi.	
Koodihoidlasse üleslaaditud lähtekood peab olema kompileeritav ilma muudatusteta.	
Koodihoidlasse tuleb korraga laadida kõik iga muudatusega seotud materjalid.	Enne materjalide üleslaadimist tuleb koodihoidlast võtta viimane uuendatud koodi seis.
Materjalide üleslaadimisega peab kaasnema sisuline üleslaetavat materjali kirjeldav kommentaar.	
Rakenduse lähtekood peab olema kommenteeritud detailsusega, mis võimaldab erialast ettevalmistust omaval tarkvaraarendajal teostada süsteemi edasiarendust.	
Rakenduse lähtekood, kommentaarid, muutujate, tüüpide ja funktsioonide nimed peavad olema inglise keeles, sisulised ja andma aimu nende otstarbest.	
Koodis kasutatavad konstandid ja lühendid tuleb kirjutada suurtähtedega.	

Rakenduse lähtekood ei tohi sisaldada pöördumispunktide aadresse, paroole ega võtmeid (ka siis kui need on koodist väljakommenteeritud).	
Rakenduse lähtekoodis peab olema võimalik tuvastada muudatuse teinud konkreetne füüsiline isik.	
Lähtekood peab olema kompileeritav tellija poolt määratletud arenduskomplekti ja versioonidega.	Tellija poolt aktsepteeritud Java kompilaatorid on Gradle ja MAVEN. Alternatiivsete vahendite kasutamine on lubatud kui nende rakendamine on põhjendatud ja kooskõlastatud tellijaga.
Kasutuses mitteolev kood tuleb rakendusest eemaldada või selgelt eraldada.	
Andmebaas	
Andmebaasi tabelid ja väljad peavad olema kommenteeritud. Kommentaarid peavad olema inglise keeles ja sisulised.	
Andmebaasi väljapikkused peavad olema väljendatud sümbolites (tähemärkide arv).	
Andmebaasi objektide nimetused peavad olema inglise keeles ning andma selget aimu otstarbest (va ajutised rakenduse poolt genereeritavad tabelid nn temp).	
Andmebaasi tabelite nimetused tohivad sisaldada ladina tähestiku väiketähti „a-z“, numbreid „0-9“, alakriipsu "_". Andmebaasi objekti nimetus ei tohi alata numbriga.	

Igas andmebaasi tabelis peab olema defineeritud primaarvõti *(primary key).*	
Ühest andmetabelist teise viitamisel tuleb kasutada võõrvõtit (foreign key). Võõrvõtme nimi peab seostuma tabeli ja väljaga, millele see viitab.	
Kõik võõrvõtmed peavad olema indekseeritud.	
Indeksite rakendamine peab toimuma vajaduspõhiselt, lähtudes süsteemi jõudlusanalüüsist. Eesmärk on tasakaalustada päringute kiirust ja andmebaasi optimeeritust, vältides üle optimeerimist.	
Kõik tabelid peavad sisaldama välju "date_created", "date_updated", "date_deleted".	
Andmebaasi objektide loomiseks tuleb kasutada andmebaasi migratsioonivahendeid.	KUM poolt heaks kiidetud migratsioonivahenditeks on Liquibase ja Flyway
Kui rakenduse versioon nõuab andmebaasi muudatusi, peavad üleantava koodiga kaasas olema andmebaasi paigalduse migratsiooniskriptid.	
Logimine ja monitooring	
Süsteemi muudatused ja rakenduse ning kasutajate tegevused logitakse seostatuna muudatuse/tegevuse teostanud konkreetse füüsilise isiku ja tema rolliga.	
Logiteadete sisu peab olema kirjutatud inglise keeles.	
Logimine peab olema konfigureeritav ning kasutada tuleb standardseid logiformaate, et võimaldada hilisem logianalüsaatorite kasutamine.	

Failisüsteemi logimisel peavad logid olema katalogiseeritud, üldlevinud faililaiendiga (nt .log, .txt, .xml) ja roteeruvad.	
Rakendus ei tohi väljastada kasutajale veateateid või aktiivsusjälgi, mis sisaldavad seansi identifikaatorit või isikuandmeid.	
Sisselogimise mehhanismid peavad olema võimelised logima nii õnnestunud, kui ka ebaõnnestunud sisselogimise katseid.	
Rakendus peab omama sisemist meetrikat ja infot sündmuste kohta.	Nt. Prometheus
Rakenduse ärilogi(*auditlog*) andmebaas peab olema sõltumatu rakenduse tööbaasist.	
Auditlogide dokumentatsioon peab sisaldama selget määratlust logitavate sündmuste ja tegevuste kohta, tagades läbipaistvuse ning vastavuse turva- ja regulatiivsetele nõuetele.	
Logide säilitamise põhimõtted peavad olema selgelt määratletud, sealhulgas logitavate sündmuste tüübid ning nende säilitamise periood vastavalt turvanõuetele ja regulatiivsetele nõuetele.	E-ITS OPS.1.1.5 Logimine https://eits.ria.ee/et/versioon/2024/eits-poohidokumendid/etalonturbe-kataloog/ops-kaeidutoeoed/ops1-oma-kaeidutoeoed/ops11-itpoohitoeoed/ops115-logimine
Kõik logid peavad olema kaitstud rakenduse kasutaja poolse lubamatu ligipääsu ja muutmise eest.	
Kui rakenduse konfidentsiaalsuse turvaosaklass on 2 või kõrgem (S2, S3) ja/või tervikluse turvaosaklass on 2 või kõrgem (T2, T3), peab rakendus logima andmete loomist, muutmist (sh kustutamist) ja vaatamist.	Turvaosaklasside S3 ja T3 korral peab rakendus logima ka administraatorite ja haldurite poolt tehtavaid andmete muudatusi (sh otse andmebaasis) ja vaatamisi.
Logimise tasandid on: • DEBUG – arendamise etapis süsteemi olekut kirjeldav informatsioon (kasutatakse ainult arenduskeskkonnas) • INFO – kasutaja päringute informatsioon, kasutaja infoteated (nt „Andmed salvestatud“, „Andmed muudetud“) • WARNING – kasutajale kuvatav valest sisendist tekkiv oodatud viga (nt „Vigaselt sisestatud andmed“)	

• ERROR – süsteemi vead, mis tekivad kasutaja sisendist (nt vigase andmebaasipäringu tekkimine) • FATAL – rakenduse toimimise kriitilised vead, mis takistavad rakenduse tavapärast toimimist (nt vigane konfiguratsioon)	
Konfiguratsioon	
Kõik komponendid peavad olema ajakohase turvakonfiguratsiooniga ja versiooniga.	
Komponentide vaheline (nt rakendusserveri ja andmebaasi serveri) suhtlus peab olema krüpteeritud.	
Komponentide vahelise ühenduse jaoks tuleb kasutada minimaalselt vajalike õigustega kontot.	
Rakenduste omavahelisel suhtlemisel tuvastatakse üksteist oAuth2 abil.	
Rakendus peab olema aedikkäideldud, konteinerdatud või muul viisil isoleeritud, et takistada ründajal rakenduse kasutamist teise rakenduse ründamiseks.	
Rakenduse konfiguratsiooniparameetrid ei tohi muutmisel vajada uuesti kokku kompileerimist.	Eraldi konfiguratsioonifail võib olla kasutusel logimise ning arendaja ja administraatori vastutusala parameetrite jaoks.
Konfiguratsiooniparameetrite nimed peavad olema inglise keelsed ja sisulised.	Kui sisulist nime ei ole võimalik kasutada, siis peab kasutatava nime kõrval olema seletus.
Konfiguratsioonifailid peavad olema rakendusserveri tüübile vastavalt vaikimisi kaitstud.	

Samasisulisi konfiguratsiooni parameetreid ei tohi korduvalt kasutada, lubatud on kirjeldada ainult üks kord.	
Kasutajaliides	
Kasutajaliidese kõik disainiotsused peavad olema tellijaga kooskõlastatud.	
Kasutajaliideste realiseerimiseks kasutatavad UI raamistikud ja komponendid tuleb tellijaga eelnevalt kooskõlastada.	Tuleb hakata kasutama Veera disainisüsteemi https://veera.eesti.ee/08be8a71e/p/48af80-veera-disainisusteem-100
Ühe veebirakenduse realiseerimiseks kasutatavate erinevate UI raamistikute ja komponentide arv peab olema minimaalne.	
Kasutajaliidese kõik osad ja teated peavad olema eestikeelsed.	
Peale kasutaja sisselogimist rakendusse kuvatakse sisse loginud kasutaja nimi ja rolliinfo. Kui ühele kasutajatunnusele on määratud mitu rolli, kuvatakse kasutajale rollivalik.	
Kasutajaliides peab alati küsima kinnitust andmete kustutamise ja massmuutmise kohta.	
Kasutajal peab olema võimalik rakenduses tegevus pooleli jätta ja hiljem jätkata samast kohast ilma kohustuseta algusesse liikuda.	
Kasutajaliides peab veatult toimima brauseritega, mida toetab eID baastarkvara, kui hanke tehnilises kirjelduses ei ole nõutud teisiti.	eID poolt toetatav brauserite nimekiri on leitav: http://www.id.ee/?id=33993 Lahendus peab toetama brauserite versioone, mille kasutus on vähemalt 5% Eestis ning mille kasutustrend on kasvav.
Kõikide eelnevast nõudest välja jäävate brauserite kasutamise puhul peab kasutaja saama tõrke korral vastavasisulise teavituse.	Kasutajat tuleb teavitada mittetoetatud brauseri kasutamisest.
Veebilehitseja navigatsiooninupud peavad käituma rakenduses analoogiliselt klassikalise veebilehitsemisega (nt veebilehitseja	

„Tagasi“ nupp navigeerib kasutaja eelmisele kuvatud lehele).	
Kasutajaliideses navigeerimine peab lähtuma äriloogikast ja võimaldama andmete sisestamist ning kasutamist ainult klaviatuuri kasutades.	
Kasutajaliidese toiminguni navigeerimiseks peab kehtima kolme klõpsu printsiip, väljalogimiseks ühe klõpsu printsiip.	
Interaktiivse vormi puhul ei tohi lehe värskendamisega tegevust korrata (nt faili teistkordselt laadida, saadetud andmeid uuesti saata).	
Kui vorm koosneb mahukatest andmeväljadest, peab kasutajaliides eeldefineeritud ajavahemike järel salvestama välja sisu, et vältida sisestatud andmete kadumist.	Mahukad andmeväljad täpsustatakse/lepitakse kokku detailanalüüsi käigus arenduse teostamisel. Salvestamine puudutab vaid sisestamise vormi kohta.
Vormide puhul peab tellija poolt nimetatud väljal olles kuvama kasutajale juhised, mis kujul informatsiooni väljale sisestada tuleb.	
Andmete sisestamisel peab rakendus kontrollima nii esitluskihis kui tagasüsteemis (backend), et sisestatud andmed vastavad välja tüübile.	
Rakendus peab võimalikult palju informatsiooni automaatselt eeltäitma (nt kirje sisestamise kuupäev).	
Kasutajaliides peab olema tõlgitav teise keelde ilma rakenduse lähtekoodi muutmata.	
Vältida tuleb kuvasid, mis eeldavad info lugemiseks kerimist paremale-vasakule.	
Kui rakenduses teostatav päring on pikem kui kolm sekundit, peab kasutajat sellest visuaalselt teavitama (nt ekraanil on liivakella kujutis; kuvatakse teade, et päringut teostatakse).	

Rakenduse esilehel peab olema võimalus halduri poolt lisada kasutajale mõeldud teavitusi ja informatsiooni.	
Kasutajaliides peab teavitama kasutajat ette seansi aegumisest.	
Veateade peab olema kirjutatud lühidalt, selges ja lõppkasutajale arusaadavas keeles. Süsteemi rikete tehnilisi üksikasju ei tohi välja näidata.	
Veateade peab sisaldama probleemi kirjeldust, vea koodi ja lahendust või infot, mis juhendab kasutajat edaspidiseks vea vältimiseks.	
Süsteem peab asendama vaikimisi veateate lehekülje, kuid säilitama algse HTTP vastuskoodi.	
Testimine	
Rakenduse kõik üleantavad versioonid peavad olema enne tellijale üleandmist täies mahus testitud: testitakse kõiki funktsionaalseid ja mittefunktsionaalseid nõudeid. Tellija nõudmisel tuleb arendajal koos rakenduse üleandmisega esitada testitulemuste raport.	
Tarkvara peab sisaldama ühik-, integratsiooni- ja E2E teste. Testide ulatus ja detailid peavad olema määratletud projektidokumentatsioonis ning kajastuma testiraportis.	
Rakenduse igakordsel versiooni üleandmisel tellijale, peab kaasas olema skript analüüsi käigus kokkulepitud jõudlustestide teostamiseks.	
Jõudlustestid peavad olema läbiviidud vähemalt kahekordse eeldatava koormuse varuga.	
Rakenduse koormuse testimiseks tuleb luua testandmete kogum.	

Loodav rakendus peab olema enne tellijale tarnimist testitud viimase kehtiva OWASP Top 10 väljatoodud turvanõrkuste vastu.	Testimistulemuste raport tuleb esitada tellijale rakenduse üleandmisel.
Dokumentatsioon	
Kogu rakenduse dokumentatsioon peab olema kirjeldatud korrektses eesti keeles.	Erandiks võib olla kolmanda osapoole komponentide dokumentatsioon (dokumentatsioon, mis pole kirjutatud tellija jaoks). Erandina käsitletakse ka väliste partneritega seotud projektdokumentatsiooni. Kõik erandid tuleb kirjalikku taasesitamist võimaldaval viisil kooskõlastada tellijaga enne dokumentatsiooni koostamist.
Dokumentatsioon peab olema eesti keeles ja sisaldama versiooni numbrit, muutmise kuupäeva, autori nime ja olema koostatud selge struktuuriga ja peab olema piisavalt selge, et Tellija iseseisvalt suudab selle järgi toimida.	Iga dokumendi versiooni kõik uuendused (võrrelduna eelmise kehtinud versiooniga), peavad olema visuaalselt eristatavad.
Lahenduse dokumentatsioon peab sisaldama RIHA määrusest tulenevat kohustuslikku informatsiooni.	RIHA määrus on leitav: https://www.riigiteataja.ee/akt/13147268?leiaKehtiv
Lahenduse dokumentatsioon peab sisaldama E-ITS'is nõutud dokumente.	Nõuded on leitavad (CON.8.M12 Detailne tarkvara dokumentatsioon): https://eits.ria.ee/et/versioon/2024/eits-poohidokumendid/etalonturbe-kataloog/con-kontseptsioonid-ja-metoodikad/con8-tarkvaraarendus
Kõik dokumendis viidatud ja seotud teised dokumendid peavad olema tellijale edastatud enne dokumendi heakskiitmist tellija poolt.	
Kõik tellijale esitatud dokumendid peavad olema redigeeritavad enamlevinud redaktoritega (nt Microsoft Office, LibreOffice).	

Loetelu üleantavatest dokumentidest lepitakse kokku konkreetse lahenduse vajadustest lähtuvalt. Reeglina peab üleantav dokumentatsioon sisaldama järgmiseid dokumente: • Spetsifikatsioon ehk süsteemianalüüs; • Prototüüp ja kasutajaliidese vaated, seejuures prototüüpimise keskkond peab olema tellija poolt kontrollitav; • Rakenduse lähtekood; • Paigaldusjuhendid ja skriptid; • Kasutusjuhendid; • Testimise kokkuvõte.	
Üleantav spetsifikatsioon ehk süsteemianalüüs peab võimaldama süsteemis realiseeritud lahenduste verifitseerimist andmebaasi tasemel.	Eelistatud keskkond on KuM Atlassian Confluence.