LAHTIÜTLEMINE: Käesolev dokument on loodud veebilehe tehnilise kirjelduse näidisena ja on koostatud minu isikliku kogemuse põhjal. Kasuta seda dokumenti ainult abimaterjalina ja määra lõplikud nõuded oma organisatsiooni vajadustest lähtuvalt.

2020 Merle Randlepp, AgileCoach.ee

TELLIJA

Hanke nimetus

TEHNILINE KIRJELDUS

## 

## 

**Sisukord**

[**Hanke eesmärk ja skoop**](#_asnqy7ocgegu) **3**

[**Ülevaade olemasolevast süsteemist**](#_g3ejva66kddq) **3**

[Tehniline platvorm](#_chyfmra4bhts) 3

[Arhitektuur](#_d2zxboz5zq5) 3

[Andmemahud](#_q13w95wj6ps3) 3

[**Nõuded uuele süsteemile**](#_p5hc71f1f00x) **4**

[Nõuded tehnilisele platvormile](#_2yiup76vrxfz) 4

[Nõuded arhitektuurile](#_skkrxh9zeay0) 4

[Majutus ja keskkonnad](#_2imya6ezjndo) 4

[Nõuded arendusprotsessile](#_s9v006rhloeh) 4

[**Visuaalne disain, vaated, prototüüp**](#_5eeb75pj0g88) **4**

[**Funktsionaalsed nõuded**](#_rhj8hc99wwb1) **4**

[Kasutajad, ligipääsuõigused, autentimine](#_5g46rqyood3e) 5

[Sisulehed](#_oa8dbodo95mr) 5

[Sisuhalduri tööriistad](#_w6u4o320qujn) 5

[Peahalduri tööriistad](#_aybvecwlayc) 5

[Uudised](#_a24wli5yi3dd) 5

[Kalender](#_5igh8j61wcer) 5

[Blogi](#_h77muprr2mp9) 5

[Uudiskiri](#_db4jje5dj2o6) 5

[Otsing](#_68xnpu2eskiy) 5

[Veebivormid](#_bdb2p7pij9qd) 5

[Liidestused](#_1uxtd9kp1ecd) 5

[JNE](#_poiasnpar2p6) 5

[**Andmete migratsioon**](#_f8pkvlkrq2t) **5**

[Veebisaidi sisu](#_gmjhe2dmi7f5) 5

[Vanade linkide ümbersuunamine](#_71egwxsk15z3) 5

[**Mittefunktsionaalsed nõuded**](#_5cd5l5unhyve) **5**

[Üldised nõuded](#_i9q5v29k5vdl) 5

[Kasutajaliides](#_qsunifaqnq59) 6

[Juurdepääsetavus](#_nksrcragvsap) 7

[SEO](#_h83lnueofbt8) 7

[Jõudlus](#_ef4wrs1oltc8) 8

[Turvalisus](#_kzoa8rqqqoon) 8

[Liidestused](#_tov9a9185313) 10

[Vastavus standarditele ja riiklikele nõuetele](#_ge8ncafc36f0) 10

[Nõuded lähtekoodile](#_m31399zd4klx) 10

[Dokumentatsioon](#_5dgpk9wpcy27) 11

[**Lisad**](#_e3cnafpoc2t0) **11**

## Hanke eesmärk ja skoop

Hanke eesmärk on luua avalik veebileht ……………...………………………………..  
Töö tulemusena valmib ……………………. veebileht koos administreerimisliidesega, mille vajalikud funktsionaalsused on tagatud tarkvara laiendamise ja/või seadistamisega ning mille puhul on tagatud käesolevas dokumendis loetletud nõuete täitmine, samuti funktsionaalsuse testimine enamlevinud brauseritega, sh nutiseadmete brauseritega.

Eelnevalt on teostatud järgmised eeltööd, mis on käesoleva hanke sisendmaterjalideks:

* kasutusmugavuse ja kasutajaliidese analüüs
* visuaalse disaini ja CVI loomine
* klikitava prototüübi loomine (*mobile*, *desktop* vaated)

Käesolevas hanke tellitavad tööd:

* uue veebilehe loomine
* veebilehe arendus- ja hooldusteenused pärast lansseerimist

Tööde tegemise aeg on ……….. kuud alates hankelepingu sõlmimisest (sh testperiood).

Hankes kirjeldatud tööde tulemi üleandmise tähtaeg on ………………

## Ülevaade olemasolevast süsteemist

### Tehniline platvorm

### Arhitektuur

### Andmemahud

Olemasolevas veebilehes on ca ………… sisulehte. Andmebaasi suurus on ……………. Failisüsteemis on ca ………………. faili, kogumahuga ………..

Veebitoimetajate suurusjärk on ca ………….. inimest.

Veebisaidi külastuste maht on ………..

## Nõuded uuele süsteemile

### Nõuded tehnilisele platvormile

### Nõuded arhitektuurile

### Majutus ja keskkonnad

### Nõuded arendusprotsessile

## Visuaalne disain, vaated, prototüüp

*Viited lisamaterjalidele*

## Funktsionaalsed nõuded

Uus veebisait peab sisaldama allpool kirjeldatud funktsionaalsust. Tehnilise analüüsi etapis võib selguda vajadus neid väheses mahus muuta või täiendada (aga mitte suuremas ulatuses kui ca 10-20% kogumahust).

### Kasutajad, ligipääsuõigused, autentimine

### Sisulehed

### Sisuhalduri tööriistad

### Peahalduri tööriistad

### Uudised

### Kalender

### Blogi

### Uudiskiri

### Otsing

### Veebivormid

### Liidestused

### JNE

## Andmete **migratsioon**

### Veebisaidi sisu

### Vanade linkide ümbersuunamine

Uues veebisaidis muutub sisu struktuur ja navigatsioon, seega tuleb arvestada, et osad veebiaadressid peavad kindlasti jääma funktsioneerima. Täpsemad kokkulepped tehakse tehnilise analüüsi käigus.

## Mittefunktsionaalsed nõuded

### Üldised nõuded

* + 1. Realiseeritud lahendus peab Tellija poolt kinnitatud arhitektuurile vastavalt töötama Tellija poolt nõutud funktsionaalsete ja mittefunktsionaalsete nõuete ulatuses.
    2. Rakendus peab olema edasi arendatav ja laiendatav.
    3. Rakendus peab olema arendatud selliselt, et oleks võimalik selle all olevaid tarkvarasid (CMS, andmebaas, veebiserver jms) vajadusel uuendada ja paigata ilma täiendava arenduseta.
    4. Rakendus ja selle komponendid peavad võimaldama keskkondade lahusust (nt arendus-, test- ja toodangu keskkond).
    5. Veebilahenduse disain peab olema rakendusfunktsionaalsusest eraldatud, et oleks võimalik sõltumatult muuta nii rakenduse koodi kui disaini.
    6. Rakenduse, andmebaasi ja kolmanda osapoole komponentide platvorm(id)/versioon(id) peavad olema sellised, mille eluea lõpp (EOL) pole teadaolevalt vähem kui 2 aasta pärast.
    7. Rakenduse arenduses ei ole kasutatud programmeerimiskeeli, mis pole Top 25 TIOBE index'is.
    8. Mitteleitud lehte ja serveri veateateid (nt error 404 ja 403) peab olema võimalik seadistada.
    9. Uniform resource identifier (URI) pikkus ei tohi ületada ühegi rakenduse poolt toetatava brauseri maksimaalset lubatud väärtust.
    10. Veebilehele peab olema võimalik lisada ilma täiendava arenduseta uusi keeli, kõik sõned peavad olema peahaldurile tõlgitavad.
    11. Veebisisu kodeeritakse UTF-8 formaadis.

### Kasutajaliides

* + 1. Rakendus peab ühilduma täielikult HTML 5 ja CSS 3 standarditega. HTML Validator <http://validator.w3.org> ja CSS validator <https://jigsaw.w3.org/css-validator/> ei tohi anda ühtegi veateadet, kuid võib anda hoiatusi (warning).
    2. Toetatud peavad olemas Google Chrome, Mozilla Firefox, Edge ja Safari väljaandja tootelehel avaldatud tööde üleandmise hetkel viimase ametliku versiooni ja sellele eelneva versiooniga. Edge’i eelneva versioonina on käsitletud Internet Explorer 11.
    3. Veebirakendus peab olema kasutatav Android, iOS, Mac OS X, Linux ja Windows seadmetes.
    4. Veebileht peab kohanduma lõppkasutaja tööseadme võimalustele (Responsive Design põhimõtted) ja olema mobile-first lähenemisega.
    5. Rakendus peab olema kohanduv erinevate arvutiekraani laiustega (1024, 1280, 1366, 1920, 256, UHD 4K px) ning enamlevinud nutitelefoni ja tahvelarvuti ekraanidega.
    6. Kasutajaliides peab alati küsima kinnitust andmete kustutamise ja massmuutmise kohta.
    7. Kasutajal peab süsteemis liikudes igal lehel (va esileht) olema võimalik näha navigatsiooniriba ehk leivarida (breadcrumb trail) ning iga navigatsiooniribal sisalduv pealkiri peab viima vastavale lehele.
    8. Javascripti ja CSS failid peavad olema minifitseeritud, laaditud lokaalselt ning ei tohi olla viidatud kolmanda osapoole serveritest.
    9. Google Pagespeed skoor peaks olema minimaalselt 70.

### Juurdepääsetavus

* + 1. Kasutajaliides peab peab vastama WCAG 2.1 nõuete (<https://www.w3.org/TR/WCAG21/>) tasemele minimaalselt AA (<https://www.aki.ee/et/teabe-avalikkus/veebilehtedele-juurdepaasetavusest>).
    2. Lahendus peab arvestama enim-kasutatavate ekraanilugeritega: <https://webaim.org/projects/screenreadersurvey8/#browsercombos> .
    3. Kõigile audio-visuaalsetele elementidele peab olema lisatud või olema võimalus lisada tekstiline selgitus (alt-tekst).
    4. Lehel peab olema võimalik navigeerida ning kasutada kõiki andmesisestusväljasid erinevate sisestusseadmetega (hiir/ klaviatuur/ hääljuhtimine).
    5. Lehel sisu peab olema ühilduv vaegnägijate poolt kasutatavate suurendustarkvaradega (zoom in/ zoom out).
    6. Tekstide ja tausta värvide kontrastsus peab olema piisav, et eristada teksti ja tausta ka must-valgel ekraanil.
    7. Kõiki sisulehti peab olema võimalik vaadata tekstiversioonis ja need peavad olema printerisõbralikud.
    8. Kogu info, mida antakse edasi värvidega, peab olema edasi antud ka tekstilisel kujul.

### SEO

* + 1. Veebileht peab olema optimeeritud, et tagada globaalsete otsingumootorite tugi (SEO).
    2. Sisulehtede URLid peavad olema koostatud vastavalt sisuhalduses sisestatud sisulehe pealkirjale (clean url).
    3. Veebilehel kasutatakse inimloetavaid veebiaadresse (leheküljele antakse tekstiline veebiaadress vastavalt pealkirjale, see ei ole suvaline numbrite, tähtede ja kirjavahemärkide segu).
    4. Veebilehtede paremaks leidmiseks kasutatakse automaatset XML sisukaardi protokolli (sitemap.xml).
    5. Veebileht peab toetama külastusstatistika lisamist (Google Analytics, Facebook Pixel vm).
    6. Rakenduses tuleb tagada eelmise veebi oluliste linkide toimimine, st toimub ümbersuunamine uue lehe lingile.

### Jõudlus

* + 1. Süsteemi peab saama kasutada samaaegselt ………. kasutajat. Tuleb arvestada, et toodud arvulised näitajad võivad ajas suureneda. Lehe laadimise aeg ei tohi ületada 2s.
    2. Jõudluse tõstmiseks kasutada puhverdamist. Puhverdamine peab olema seadistatud viisil, mis tagab külastajale igal ajahetkel ajakohase info kuvamise (ei ole lubatud aegunud info kuvamine).
    3. Täitja esitab arenduse lõpus koormustestide raportid.

### Turvalisus

* + 1. Lahendus peab olema turvaline, arvestades parimaid tänapäevaseid praktikaid XSS, SQL injection ja muude sarnaste rünnete vastu.
    2. Kogu leht peab läbivalt kasutama ainult HTTPS protokolli, HTTP pealt on lubatud vaid automaatne ümbersuunamine HTTPS protokollile.
    3. Arendatud veebilehele, veebilehe funktsionaalsust pakkuvale tarkvarale (sisuhaldus, moodulid) peavad olema paigaldatud viimased stabiilsed versioonid ja kõik turvauuendused. Veebilehe majutamisega seotud turvauuenduste paigaldamise eest vastutab veebilehe majutusteenuse pakkuja.
    4. ISKE turvaklass on K1T1S1 ja arvestada tuleb minimaalselt moodulite B5.4, B5.7 ja B5.21 nende meetmetega, mis on realiseeritavad arendaja poolt vt <https://www.ria.ee/iske>.
    5. Süsteem ei tohi võimaldada kasutajale ligipääsu süsteemi toimimise informatsioonile. Täpsem kirjeldus on leitav ISKE meede M4.400 "Turbe seisukohalt oluliste andmete väljastamine veebirakendustes": <https://iske.ria.ee/8_03/ISKE_kataloogid/7_Kataloog_M/M4/M_4.400> .
    6. Rakenduse turvalisuse tagamiseks (näiteks XSS, SQLInjection jne) tuleb järgida OWASP-i parimaid praktikaid. Enne lõpliku töö vastuvõtmist teostab tellija arendatud veebilehele OWASP ASVS verisoon 4 (märts 2019, <https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf> ) põhjal tasemel 1 oportunistliku turvatesti, mille skoopi kaasatakse vastavalt vajadusele taseme 2 testi elemente. Veebilehe arendaja on kohustatud turvatestil tuvastatud puudused enne töö üleandmist kõrvaldama.
    7. Lahendus peab võimaldama kasutajate tegevuse logimist ja logide monitooringut. Süsteem peab säilitama administraatorite ja automaatsete tegevuste logid vähemalt 12 kuud.
    8. Autentimist võimaldav informatsioon (nt autentimissaladused, API võtmed, salasõnad) ei tohi sisalduda lähtekoodis ega võrgus olevates lähtekoodi repositooriumites.
    9. Rakendus tohib kasutada vaid sessiooni küpsiseid. Muude küpsiste kasutamine on keelatud.
    10. Kui rakendus kasutab sessiooni küpsiseid (*session cookie*) või muid tehnoloogiaid (nt *local storage* jm), mis salvestavad kasutaja arvutisse informatsiooni, siis tuleb kasutajat sellest teavitada.
    11. Autenditud sessiooni tunnust ei tohi ainult lihtsa küpsisega lahendada, et vältida sessiooni ülevõtmist.
    12. Rakendusel peab olema konfigureeritav kasutajaseansi aegumise aeg. 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 limiit või kasutaja lõpetab seansi omal soovil.
    13. URL ei tohi sisaldada isikuandmeid või sessioonivõtit.
    14. Rakendusse ja andmetele tohib olla ligipääs vaid dokumenteeritud ja tellimuses kirjeldatud teid mööda ning dokumenteeritud autentimisprotseduure kasutades.
    15. Andmebaasis olevate rakenduste kontod peavad omama ainult minimaalselt rakenduse tööks vajalikke õigusi.
    16. Kõik paroolid ja salasõnad peab rakendus alati salvestama vaid krüpteeritud või räsitud+soolatud kujul.
    17. Konfiguratsioonifailid peavad olema vastavalt rakendusserveri tüübile vaikimisi kaitstud failid. Rakenduse failid, mida kasutaja näha ei tohi, peavad olema vaikimisi kaitstud kaustades.
    18. Kui rakendus võimaldab mitteautenditud kasutajal edastada andmeid (nt veebivormis), tuleb need andmed puhastada XSS filtriga või eemaldada HTML-tag’id.
    19. Veebipõhiste rakenduste poolt saadetavad vormidel peab paiknema peidetud unikaalne räsi, mida kontrollitakse vormi vastuvõtmisel, et vältida CSRF rünnakuid.
    20. Kommentaaride või blogi funktsionaalsuse kasutamisel tuleb rakendada Captcha laadset vm tehnoloogiat, et ära hoida küberkurjategijate või masinrünnet blogimise või kommenteerimise teenuse vastu.
    21. Tuleb kasutada vajalikke HTTP turvapäiseid (näiteks HTTP Security Headers - Content Security Policy, X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Cross-Origin Resource Sharing ning kui leht täielikult HTTPS siis ka Strict-Transport-Security).
    22. Arvestada tuleb turvalisuse nõuetega süsteemi arhitektuuri loomisel kogu lahenduse elutsükli vältel.
    23. Peale töö vastuvõtmist tellija poolt, rakendub tehtud tööle 2 aastane garantii periood, mille jooksul kõrvaldab arendaja oma kuludega veebilehes tuvastatud vead.

### Liidestused

* + 1. Andmevahetus peab toimuma eranditult autenditud tunnusega šifreeritud andmeedastuskanalis (nt SSL andmevahetusprotokollil).
    2. Liidesed väliste süsteemidega peavad olema standardsed (allutatud sarnastele reeglitele) ja liidestamise detailid peavad olema dokumenteeritud.
    3. Platvormile peab saama järgnevatesse etappides lisada uusi liidestusi.
    4. Kõik välised komponendid (nt välised süsteemid, teegid), millele toetudes loodav lahendus töötab, peavad olema tuvastatavad ja dokumenteeritud.
    5. Rakenduse liidestused 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 ja saatma automaatsed teavitused administraatorile.

### Vastavus standarditele ja riiklikele nõuetele

* + 1. Lahendus peab vastama dokumendis „Riigi infosüsteemi koosvõime raamistik“ kirjeldatud põhimõtetele <https://www.mkm.ee/sites/default/files/riigi_it_koosvoime_raamistik.pdf>.
    2. Lahendus peab vastama dokumendis "Infoturbe koosvõime raamistik" kirjeldatud põhimõtetele https://www.mkm.ee/sites/default/files/infoturbe\_raamistik.pdf .
    3. Lahendus peab vastama dokumendis „Veebide koosvõime raamistik“ kirjeldatud põhimõtetele. https://www.mkm.ee/sites/default/files/veebide\_raamistik.pdf.
    4. Lahendus peab vastama „Avaliku teabe seaduses“ kehtestatud teabe avalikustamise ja juurdepääsu võimaldamise nõuetele. https://www.riigiteataja.ee/akt/114032011019?leiaKehtiv
    5. Loodav lahendus peab vastama isikuandmete kaitse üldmäärusele ja direktiivile andmete edastamisel politseikoostöö ja õigusalase koostöö valdkonnas sätetele. Isikuandmete kaitse üldmäärus ja direktiiv on leitavad : <https://www.aki.ee/et/teavitus-uudised/andmekaitse-reform>
    6. Veebileht peab toetama kehtivate andmekaitse nõuete täitmist (küpsistega valikuline nõustumine, privaatsuspoliitika jms).

### Nõuded lähtekoodile

* + 1. Rakenduse lähtekood on kirjutatud selgusega, mis võimaldab erialast ettevalmistust omaval tarkvaraarendajal teostada süsteemi edasiarendust.
    2. Lähtekoodi kommentaarid peavad olema selged, arusaadavad ja sisuliselt kirjeldama vastavat koodi, mille juures nad on ning moodustama vähemalt 20% koodi mahust.
    3. Üleantav kood ei tohi sisaldada paroole (ka siis kui need on koodist väljakommenteeritud), mida kasutati arenduse käigus. Kõik arenduse käigus kasutatud paroolid tuleb asendada fraasiga „<password>“.
    4. Rakendus peab olema kirjutatud objektorienteeritult.
    5. Keskkonnapõhiseid muutujad peavad olema konfiguratsioonifailist seadistatavad.
    6. Rakenduse kood on versioneeritud kasutades Git'i.

### Dokumentatsioon

* + 1. Arendaja peab koostama:
* tehnilise spetsifikatsiooni,
* rakenduse paigaldusjuhendi,
* sisuhalduri kasutusjuhendi,
* peahalduri kasutusjuhendi
  + 1. Paigaldusjuhend peab muuhulgas sisaldama vajalike lisatarkvarade installeerimis-, konfigureerimis- ja kasutamisjuhiseid.
    2. Dokumentatsioon ja juhendid on korrektselt vormistatud nii õigekeele, terminoloogia, viitamise kui tehnilise vormistuse mõttes.

## Lisad