**Avatud hankemenetlus"**E-ITS portaali arendustööd – *fullstack* arendaja ressursi ostmine", viitenumber 283086

# TÖÖDE KIRJELDUS

# Sisukord

[1. Hanke eesmärk 1](#_Toc172630978)

[2. Olemasoleva lahenduse tehniline kirjeldus 2](#_Toc172630979)

[3. Portaali ja halduskeskkonna hetkeseis 4](#_Toc172630981)

[4. Portaali parendussoovid 4](#_Toc172630982)

[5. API hetkeseis 4](#_Toc172630983)

[6. API parendussoovid 5](#_Toc172630984)

[7. Tellitavad tööd 5](#_Toc172630985)

[8. Nõuded valmivale tulemile 6](#_Toc172630986)

[9. Tellitavate tööde ajakava ja vahendid 6](#_Toc172630987)

[LISA 1. E-ITS portaali arhitektuuriline lahendus 7](#_Toc172630988)

[LISA 2. Etalonturbe kataloogi moodulite ja meetmete mudel 8](#_Toc172630989)

# Hanke eesmärk

* 1. Riigi Infosüsteemi Amet (edaspidi ka hankija või RIA) sõlmib hankelepingu ühe edukaks tunnistatud pakkujaga.
  2. Hankelepingu eesmärk on osta arendusressurssi *fullstack* arendaja rolli täitmiseks, et teostada olemasoleva portaali <https://eits.ria.ee> parendustööd ja edasiarendused:
     1. Standardi halduse elutsükli haldusprotsessi automatiseerimine;
     2. API võimekuse ja kasutusmugavuse parandamine;
     3. Portaali kasutusmugavuse parandamine.
  3. Eelisjärjekorras soovib hankija ellu viia äriloogika muudatused, mis parandaks kasutusmugavust. Hankija katab hankeperioodil ise vajalikud rollid, mida käesoleva hanke raames ei osteta.
  4. Tööd teostatakse 3-le lahenduse komponendile:
     1. Portaalile;
     2. Portaali halduskeskkonnale;
     3. E-ITS API-le.

# Olemasoleva lahenduse tehniline kirjeldus

# Eesti Infoturbestandardi (edaspidi: E-ITS) portaal <https://eits.ria.ee/>  on avalikkusele suunatud Riigi Infosüsteemi Ameti poolt hallatav süsteem E-ITSi dokumentatsiooni publitseerimiseks ja redigeerimiseks.

* 1. Portaal hõlmab:
     1. **avalikku vaadet** (avalik veebileht [https://eits.ria.ee](https://eits.ria.ee/)),
     2. **avalik masinliides** (siin ka: rakendusliides; teostatud Swagger OpenApi vormingus <https://eits.ria.ee/swagger-ui.html> ) ning
     3. **sisuhaldaja vaade** ehk avaliku veebilehe [https://eits.ria.ee](https://eits.ria.ee/) redigeerimiseks sisu- haldussüsteem GRAV.
     4. E-ITSi portaali olemasolevat arhitektuurilist lahendust kujutab "Joonis 1. E-ITSi portaali arhitektuuriline lahendus" LISA 1.
  2. Portaali tehniline lahendus koosneb järgmistest komponentidest ja tehnoloogiakasutustest:
     1. **sisuhoidla Bitbucket** – standardi teksti jm sisu hoitakse Git-repos (RIA Bitbucket, arhitektuurijoonisel “RIA Stash”), sisuhaldussüsteemi Grav vormingus.
     2. **sisuhaldussüsteem Grav** – Grav haldusvahendit kasutatakse portaali sisu redigeerimiseks.
     3. **eits-gravadapter** – Java-rakendus, mis teisendab sisu Grav-vormingust E-ITS portaali spetsiifilisse vormingusse. Käivitub automaatselt kui Gravis sisu muuta. Javascript teisendab Grav-i markdown vormingus failid/artiklid E-ITS portaali-spetsiifiliselt JSON ja YAML kujule, mis on kõlbulikud selleks, et portaali API saaks neid kasutada (hallatakse Jenkinsi Pipeline kaudu). Annab sisendi eits-searchile, mille kaudu uuendatakse eits-search ja rest-api alusel JSON failid.
     4. **eits-cms** – komponent, mis hoiab E-ITS portaali sisu.
     5. **eits-api** – komponent, mis pakub E-ITS API-t. API on JSON/REST-stiilis. API kaudu saab pärida andmeid E-ITS struktuuri, sõnastiku, meetmete jms standardi sisu kohta. API on dokumenteeritud OpenAPI standardi kohaselt (<https://eits.ria.ee/swagger-ui.html>).
     6. **eits-fe** – komponent, mis serveerib E-ITS portaali sisu kasutajatele. Kasutab rest-apit, et portaali sisu serveerida (<https://eits.ria.ee/>). Kirjutatud React veebiraamistikus.
     7. **eits-feedback** – kavandatud komponent portaali kasutajatelt tagasiside küsimiseks.
     8. **eits-search** – otsingu komponent. Põhineb Elasticsearch-l.
     9. **eits-update-content** - käivitub webhookiga pärast eits-gravadapteri jooksutamist; viib andmed eits-api ja eits-search komponentidesse.
     10. Portaalile on rakendatud RIA logimis- ja monitooringuvahendid (Elastic pinu, Matomo, Zabbix). Portaali arendamisel kasutatakse RIA arendusvahendeid: Jenkins, Vault.
     11. Portaal [https://eits.ria.ee](https://eits.ria.ee/) on evitatud kõrgkäideldavana – olulised komponendid on kaheõlalistes klastrites.
     12. Kasutajaliideses on kasutusel disainisüsteem Veera: <https://veera.eesti.ee/08be8a71e/p/41e598-veera-disainisusteemist>
     13. Komponentide lähtekood asub RIA koodirepodes (Bitbucket). Enamus koodi asub: eits-frontend, eits-api ja Grav komponentides.
     14. Olemasolev lahendus võimaldab avalikult publitseeritud andmete allalaadimist läbi avaliku masinliidese Swagger OpenAPI: <https://eits.ria.ee/swagger-ui.html>.
     15. Läbi Swaggeri alla laetavateks andmeteks on [https://eits.ria.ee](https://eits.ria.ee/) portaalis publitseeritud sisu. Hetkel on E-ITS portaal ise üks avaliku masinliidese põhitarbijatest ning vajab seda enda andmete näitamiseks.
  3. **Olemasoleva lahenduse tarbija**:
     1. **Portaali haldur** (RIA töötaja) kasutab loodud süsteemi veebilehe [eits.ria.ee](http://eits.ria.ee/) sisu publitseerimiseks ja standardi versioonide haldamiseks töövahendina;
     2. **E-ITS portaal** ise andmete näitamiseks;
     3. **E-ITS standardi rakendaja** kui avaliku vaate sirvija ja failide allalaadija. Soovib saada (nii moodulite kaupa kui ka terviklikult) meetmete täielikku nimekirja masintöödeldava andmestikuna või alla laetud failina, et kasutada seda sisendina oma asutuse E-ITSi rakendusvahendis või tekitada endale eraldiseisev töödeldav ja muudetav töötabel;
     4. **E-ITS API kasutaja** (rakendaja), kes kasutab avaliku masinliidese otspunkte eesmärgiga liidestada E-ITS portaalis kuvatav standardi andmestik  muude väljaarendatavate või loodavate lisandväärtust andvate rakendustega. Soovib kasutada saadavat ressurssi infoturbe haldamise rakenduse/töövahendi väljaarendamisel, mis võimaldab infoturbe halduse ja rakendamise tööprotsessi automatiseerida. Arendaja või teenusepakkuja (samuti rakendaja) soovib Eesti Infoturbestandardi versiooniuuenduste korral enda töövahendites Eesti Infoturbestandardi meetmete andmestikku mugavalt ja kiirelt uuendada.
     5. **Audiitor** soovib saada portaalist standardi (vähemalt) viimase kolme aasta versiooni meetmete täielikku nimekirja koos versioonide muutelugudega, alla laetud failina ja/või masintöödeldavana, et hinnata asutuse vastavust E-ITS auditeerimisjuhendi (<https://eits.ria.ee/>🡪 dokument „*Auditeerimisjuhend*“) nõuetele ning ISMS haldusprotsessi (<https://eits.ria.ee/>  🡪 dokument „*E-ITS Nõuded infoturbe halduse süsteemile*“) kontekstis. Lisaks vajab audiitor oma igapäevases töös asutuse infoturbehalduse süsteemi toimimise hindamiseks eelpoolnimetatud dokumente alla laetavatena.
  4. Eesti infoturbestandardi kasutaja kriitilised infovajadused (allalaadimised):
     1. E-ITS standardi versiooni info;
     2. moodulite loend;
     3. meetmete loend;
     4. ohtude loend ja kirjeldus;
     5. meetme sisu;
     6. meetme tunnused ja seosed;
     7. versioonide võrdluses muutelugu.
  5. Meetmetele ja moodulitele peab saama tulevikus mistahes filtreeritavaid tunnuseid ja seoseid juurde luua.
  6. Versiooni vahetusel tekivad etalonturbe kataloogi järgmised muudatused:
     1. meetme ümbertõstmine moodulis (nt muutub meetme turbeviis);
     2. meetme ümbertõstmine moodulipuus;
     3. mooduli ümbertõstmine etalonturbe kataloogis;
     4. meetmed või moodulid ühinevad;
     5. meetmed või moodulid kustutatakse;
     6. moodulisse lisandub täiesti uus meede või lisandub täiesti uus (alam)moodul;
     7. meetme tähis või nimetus võib muutuda;
     8. muutuvad meetme tunnused (nt elutsükkel, vastutaja, lisavastutaja, seos alusohuga, CIA tunnus, meetme tüüp vms);
     9. muutuvad meetme all-tingimused (meetme all-tingimus lisandub, kustub või korrigeeritakse sõnastust);
     10. tekivad mistahes uued seosed etalonturbe kataloogi elementide vahel.

# Portaali ja halduskeskkonna hetkeseis

* 1. Jõudlusprobleemid. Uuenduste avalikustamine võtab ebamõistlikult kaua aega;
  2. Kasutusmugavus jätab soovida, probleemid info leitavuse ja esitusviiside paindlikkusega;
  3. Pisiparanduste sisseviimine on portaali haldajale väga aeganõudev;
  4. Frontend koodivead.
  5. Portaalis kasutajal pole tagasiside andmine mugav ja sisuliselt ei toimi.

# Portaali parendussoovid

* 1. Portaali kasutajaliidese lahendus peab olema kasutajatele mugav, arusaadav ning loogiline. Otsitav peab olema intuitiivselt leitav.
  2. Väljapakutud kasutajaliidese tehniline lahendus peab tagama jätkusuutliku arenduse ning olema tellijale tulevikus mõistlikult hallatav.
  3. WCGA nõuded on uuendatud kehtivale versioonile.
  4. Portaali stiililehtede disainimuudatuste tegemine on muudetud paindlikumaks.
  5. Kuna Eesti Infoturbestandardi vastu on tuntud ka rahvusvahelist huvi, siis on oluline, et masinliides toetab ka E-ITS andmestiku väljaandmist ingliskeelse tõlkena. Mitme-keelsus (automaattõlge, käsitsi redigeeritav valideeritud tõlge) on planeeritud lisada nii E-ITS portaali kui masinliidesesse.

# API hetkeseis

* 1. API genereerib eri päringuid, millest osa on loodud EITS esimese portaaliga ja mida pole muudetud. Reaalselt vajab portaali kasutaja kuvatavatest päringutest vaid mõnda. Portaali haldaja kasutab oma tööks failide ja viitade tegemiseks paari päringut, mis ka on avalikud.
  2. API päringute tulemid on vigased ja ei vasta kasutajate soovidele.
  3. API (päringute metaandmed) ei sisalda standardi litsentsitingimusi.
  4. **Portaali muutelugu. Portaali muutelugu on osa APIst, mis kuvab portaalis kahe standardi versioonide erinevusi** masinloetavalt.(<https://eits.ria.ee/et/versioon/2023/eits-poohidokumendid/muutelugu>):
  5. Muuteloo esitusviis pole rakendajale arusaadav (muudatused esitatakse kui lisamised ja kustutamised). Muudatused pealkirjade tekstides kajastuvad nagu moodul või meede oleks kustutatud ja uuesti lisatud.
  6. Muuteloos kuvatakse välja ainult meetme teksti muudatusi. Samas tehakse ka muid muudatusi, mida muutelugu fikseerib, aga muudatused ise pole kasutajale võrdlused nähtavad.

# API parendussoovid

* 1. Valitud E-ITS standardi versiooni etalonturbe kataloogi tervikpäring 10 moodulgrupi kõikide moodulite, moodulite kirjelduse ja alammoodulitega ning nende meetmetega (andmestiku kõige väiksem ühik on meede koos oma all-tingimustega). Portaalis hoitakse standardist kolme (3) versiooni. Eesti Infoturbestandard on kohustuslik (vt „*Küberturvalisuse seadus*“ <https://www.riigiteataja.ee/akt/106082022018?leiaKehtiv>) ja rakendatakse vastavalt kehtiva standardi versiooni numbri alusel, siis peab API poolt väljaantav standardi info olema alati seotud E-ITSi standardi versiooniga. See tähendab, andmed peab saama kätte iga E-ITSi versiooni kohta eraldi ning kasutaja peab saama valida, millise E-ITS standardi versiooni kohta andmestik/andmefail luuakse.
  2. Kohustuslike dokumentide allalaadimine (kehtestatakse iga aastaselt vabariigi valitsuse määrusega) ja nende dokumentide muutelugu.
  3. RIA poolt toodetud ja kooskõlastatud juhendmaterjalid.
  4. Mooduleid ja meetmeid kirjeldavat andmemudelit vt LISA 2.
  5. **Muuteloo arendussoovid:**
     1. Muutelugu peab võimaldama nii rakendajatel, audiitoritel kui ka standardi omanikul tuvastada standardi erinevate versioonide vahelisi erinevusi.
     2. Muutelugu portaalis on inimloetav tekst, kus peab olema võimalik jälgida tehtud muudatusi moodulites tervikuna ja eraldi meetmetes. Muudatuste halduse kuvamine võiks dubleerida standardi esitusviisi portaalis (lõõts moodulipuuna)
     3. API võimaldab allalaadimisel ise konstrueerida standardi sisust kasutajale sobivate väljadega andmetabeleid .json ja .csv vormingus.
     4. API kuvab välja ainult rakendajale vajalikke päringuid. Portaali halduri vajalikud päringud on ligipääsuõigustega piiratud.

# Tellitavad tööd

| * 1. **Arendaja tööaeg järgmiste tegevuste teostamiseks** |
| --- |
| * + 1. Portaali ja sellega seotud komponentide eits.ria.ee analüüsi- ja arendustööd, sh dokumenteerimine ja testimine;     2. Mittefunktsionaalsete nõuete realiseerimine:        1. EITS etalonturbe meetmed tarkvara arendusele (täpne nimekiri lepitakse kokku peale lepingu sõlmimist)        2. OWASP ASVS L2        3. RIA MFN (<https://e-gov.github.io/MFN/>)        4. Veebiraamistiku (Veera) nõuded        5. WCAG, kehtiva versiooni tase AA (<https://www.w3.org/TR/WCAG22/>)        6. RIA kontrollnimekirjad (täpne nimekiri lepitakse kokku peale lepingu sõlmimist) |

# Tööde korraldus ja nõuded valmivale tulemile

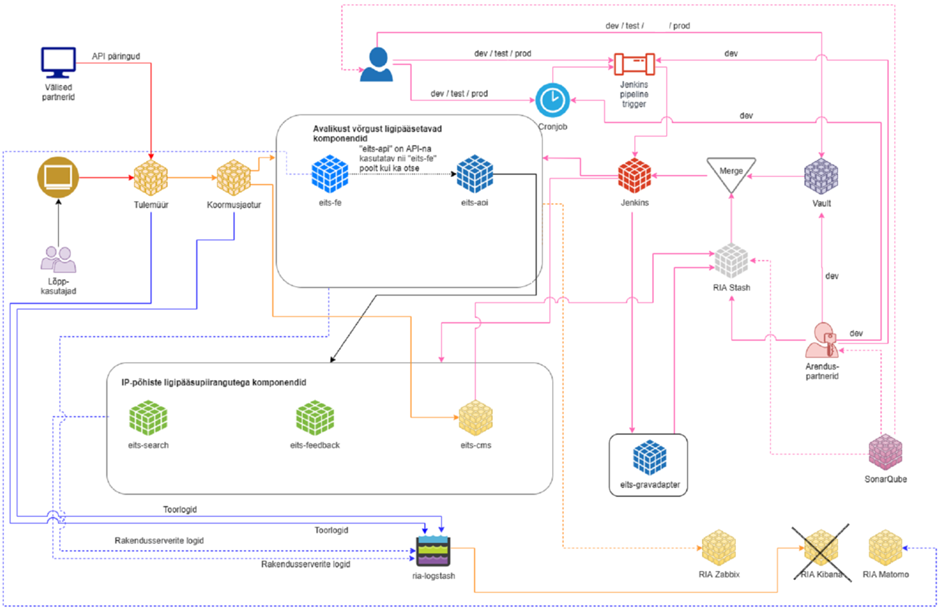
* 1. Töid teostatakse vastavalt hankijaga kokkulepitud arendusmudelile.
  2. Tööde teostamiseks ja tööde tulemina valmiva koodi ja dokumentatsiooni tarnimiseks kasutab pakkuja hankija keskkondi.
  3. Töid teostatakse pakkuja poolt eelnevalt kooskõlastatud arenduspileti alusel, kui ei ole kasutusloo tasemel kirjalikult teisiti kokku lepitud.
  4. Hankija koostab tellitavate parenduse ja arendustööde esmased prioriteedid
  5. Tööde prioritiseerimine lepitakse lõplikult kokku hankija esindajaga regulaarsetel kohtumistel ning tööülesannete täpsustamine, mahuhindamine ja jooksev prioriseerimine toimub RIA *JIRA* keskkonna vahendusel.
  6. Projekti dokumentatsioon kirjeldatakse RIA *Confluence*’is, lähtekoodiga seonduv dokumenteeritakse hankija poolt valitud keskkonnas.
  7. Vahetulemused ja jooksvad arendused hoitakse hankija *GitHubi* või *Bitbucket* keskkonnas.
  8. Tööks vajalikud testandmed koostab pakkuja hankijaga eelnevalt kooskõlastatud mahus, arvestades, et vaikimisi lähtub pakkuja *test-driven development* põhimõtetest, mille kohaselt on testidega kaetud kõik arendused.
  9. Pakkuja peab arendustööde läbiviimisel juhinduma *jätkusuutliku arenduse* põhimõtetest. Tehtavad arendustööd peavad edaspidi võimaldama arendatavate komponentide edasiarendusi järgmistes iteratsioonides.
  10. Hankija viib läbi koostöös kolmanda osapoolega teostatud töödele turvatestimisi. Turvatesti tulemusena võimalikud tekkinud puudused tuleb kõrvaldada täitja poolt jooksvalt nende selgumisel, kuid mitte hiljem kui kahe (2) nädala jooksul.
  11. Pakkuja annab hankijale kohe teada tööde teostamisel vajaliku info puudumisest, tööülesannete lõppemisest, tekkinud tõrgetest jms. Viivituse ajal, mil hankija täpsustab infot, lahendab tõrget vms, teostab pakkuja neid tööülesandeid, milles on vajalik info olemas ja pole tõrkeid.
  12. Pakkuja peab arendustööde teostamisel lähtuma *OpenAPI spetsifikatsioonist*.
  13. Komponendi tehniline dokumentatsioon peab sisaldama täielikku paigaldusjuhist koos tarne automaatskriptidega ja kogu funktsionaalsust katvaid näidispäringuid.
  14. Pakkuja peab teenuse-spetsiifiliste ärifunktsionaalsuste kirjeldamise ja esilekutsumise tagama eraldi konfiguratsioonifailide tasemel, mitte tarnitava lahenduse lähtekoodis.
  15. Arendatavad rakendused peavad töötama kõikide tänapäevaste veebilehitsejatega (Chrome, Safari, Firefox, Edge viimased versioonid) ning olema kasutatavad nii Android, iOS, Mac OS X, Linux ja Windows seadmetes.
  16. Arendatavad rakendused peavad olema skaleeruvad.
  17. Arendatavad komponendid peavad olema projekti raames taaskasutatavad.
  18. Tööde tulemid peavad olema evitatud kõrgkäideldavana.
  19. Paigaldusjuhise samm-sammult järgimine peab lõppema rakenduse eduka täieliku paigaldumisega ettenähtud keskkonnas.
  20. Pakkuja vastutab süsteemi tööde kvaliteedi ning terviklikkuse eest ja, et selle alusel tehtav infosüsteem on realiseeritav ja rakendatav koostoimelise ja riigi IT põhimõtetele vastava infosüsteemina.
  21. Pakutavad lahendused peavad olema otstarbekad ning arvestama Eestis kehtivaid õigusakte.
  22. Pakkuja ei tohi töö teostamiseks kasutada lahendusi, millega kaasnevad hankijale kasutamist piiravad litsentsitingimused ja/või täiendavad (püsi)kulud, välja arvatud juhul kui hankijaga on kirjalikku taasesitamist võimaldavas vormis kokku lepitud teisiti.
  23. Töid peavad teostama pakkumuses nimetatud isikud. Meeskonnaliikme väljavahetamine on võimalik hankelepingus nimetatud tingimustel.
  24. Üleandmise-vastuvõtmise akt esitatakse kord kuus. Aktis peab olema nimetatud teostatud tööd ja töötatud töötundide arv mis on kooskõlas Jiras fikseeritud tööde sisu ja mahuga. Hankija ei kinnita aktis pooleliolevate tööde kohta esitatud töötunde.

# Tellitavate tööde ajakava

* 1. Hankija ostab *fullstack* arendaja rolli ressurssi hankelepingu jõustumisest 24 kuud. Pakkuja peab alustama hankelepingu täitmist esimesel võimalusel, kuid mitte hiljem kui 5 tööpäeva jooksul alates hankelepingu allkirjastamist poolte poolt.
  2. Rolli töömaht on hankelepingu täitmiselt hinnanguliselt 0,5 koormusega, mis võib kuude lõikes varieeruda.
  3. Hankelepingu täitmise ajal valminud ja üleantud töödele teostab tellija valminud lahendustele turvatestimise käesolevast hankest eraldi RIA poolt valitud partneri poolt kasutades manuaalset läbistustestimist.

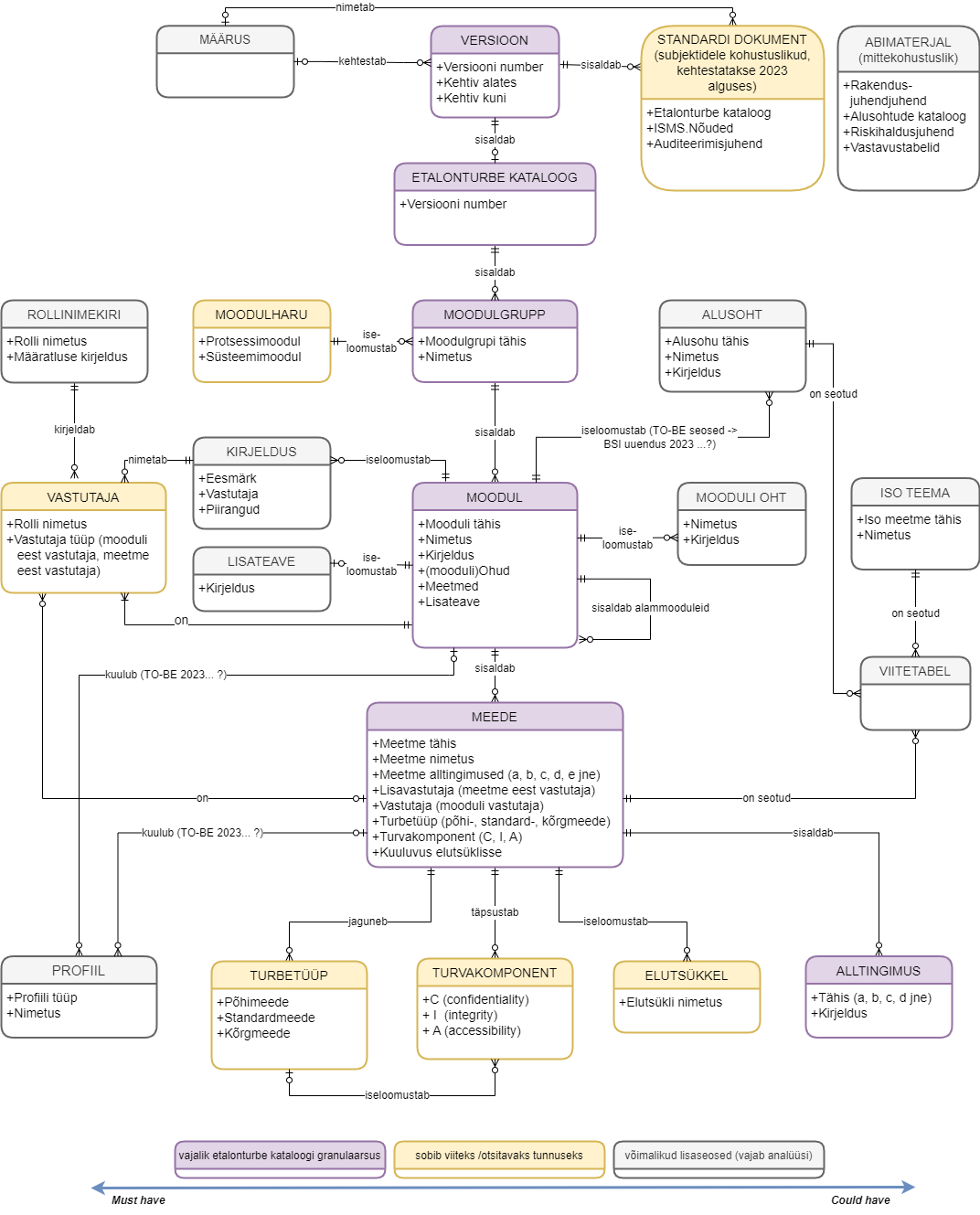
# LISA 1. E-ITS portaali arhitektuuriline lahendus

Joonis 1. E-ITS portaali arhitektuuriline lahendus



# LISA 2. Etalonturbe kataloogi moodulite ja meetmete mudel

Joonis 2. Etalonturbe kataloogi moodulite ja meetmete mudel

****