Soovituslik mudel
2014

# Avalik kohtvõrk ja WiFi
# Valdkonnakäsitlus, mõisted, nõuded ja soovitused

# Sisukord

# 1. Käsitlusala

## 1.1. Avalikud internetiteenused

Infoühiskonna üheks tunnuseks on ühiskonna liikmete vaba ligipääs teabele.
Internet muudab elu kiiremaks, mugavamaks ja arendab ühiskonda tervikuna.
WiFi on mugavaim ligipääs Internetile ja see on kergesti kasutatav kõigi nutikate seadmetega.
Oluline on avada ligipääs Internetile viisil, et see oleks turvaline, kergesti leitav ja tööshoitav.

Andmesides kasutatakse tänapäeval internetiühenduse pakkumiseks väga mitmeid tehnoloogiaid (näiteks arvuti-kohtvõrgud, DSL, fiiberoptika, mobiilside, WiFi. )
IT rakenduste realiseerimisel on tarkvara poolt erinevaid platvorme ja võimalusi samuti rohkesti. Kõnealuste süsteemide puhul tuleb arvestada ühilduvuse (millega teenuseid kasutada) küsimusi, väga tõsiselt tuleb tegeleda turvalisuse probleemidega ning kuna IT valdkonnas on tehnoloogia arenenud kiiresti, tuleks vaadata ka, et süsteem oleks arenguvõimeline.
Käesolev dokument selgitab, kuidas luua ligipääs Internetile avalikus kohas.

## 1.2. WiFi roll avalikus kohas

WiFi traadita võrkude kasutamise eeliseks on eelkõige selle tehnoloogia lihtsus ja mugavus. (praktiliselt kõik tänapäeva sülearvutid ja nutikad seadmed kasutavad WiFi ning tootjaid ühendav organisatsioon Wi-Fi Alliance tagab seadmete ühtesobivuse .)

WiFi võrgu saab ettevõte, organisatsioon või KOV luua oma vajaduste järgi.

> WiFi muudab töökeskkonna kiireks ja mugavaks.
> Külastajate arv suureneb ja teabelevi paraneb.
> WiFi on interaktiivne suhtluskanal, mille kasutajaid saab küsitleda ja tegevusse kaasata.

Avalik WiFi peab olema eraldiseisev võrk.
Võrku sisenejad võtavad vastutuse oma tegevuse eest ja vajadusel peab olema võimalik käivitada kasutajate autentimine.
.
Avalikes internetiteenustes on enamasti kasutusel avatud WiFi võrgud, selle põhjuseks on eelkõige kasutusmugavus ning vajadus kasutajaid WiFi uksel tuvastada, sõltumata WiFi võrgu parameetritest.
Kahjuks on avalikel WiFi võrkudel omad probleemid, nendest täpsemalt peatükis 5 “Ühenduse turvalisus”.

# 2. Mõisted

## 2.1 Sissejuhatus.

Käesolevas jaotises "Mõisted" selgitame ja piiritleme kasutatavad mõisted ning esitame mõistete väljendamiseks valitud terminite määratlused ja sisuseletused dokumendi teksti paremaks mõistmiseks. Esitatakse ka asjakohased vähemtuntud lühendid ja tingtähised.

## 2.2 Dokumendis käsitletavad mõisted ja terminid.

Autentimine - kinnituse andmine olemi väidetavale identiteedile. Kasutaja autentimise korral identifitseerib kasutajat talle teadaolev (nt parool), tema valduses olev (nt pääsmik) või ta isiku tunnusomadus (biomeetrik). Tugev autentimine põhineb tugevatel mehhanismidel (nt biomeetrial) või kasutab nimetatud vahenditest vähemalt kaht (nn mitmefaktoriline autentimine)

**Autoriseerimine** - volituste või õiguste andmine

**Avalik WiFi leviala** – WiFi leviala, mis on loodud traadita Interneti kasutamiseks. See on mõeldud külalistele ja peab paiknema väljaspool ettevõtte sisevõrku.

**DHCP** - Interneti protokoll, mis annab hosti käivitamisel talle dünaamiliselt IP-aadressi (RFC 2131)

**EAP (Extensible Authentication Protocol)** - autentimismeetod vastavalt standardile IEEE 802.1X. EAP on detailselt kirjeldatud RFC 3748

**Hotspot** - avaliku WiFi pöördumispunkt, mille kaudu kasutajad sisenevad võrku.

**Identifitseerimine** - olemi ühese identsuse üheselt määramise protsess. Meetod, mis seisneb ühe või mitme sellise atribuudi kasutamises, mille väärtused identifitseerivad etteantud olemi iga eksemplari üheselt.

**Infoturve** - teabe konfidentsiaalsuse, tervikluse ja käideldavuse säilitamine, võib peale selle hõlmata ka muid omadusi, näiteks autentsust, jälitatavust, salgamise vääramist ja usaldatavust.

**Interneti-teenuseandja (ISP)** - ettevõte, mis pakub juurdepääsu Internetile, tavaliselt tasu eest. Kõige tavalisemateks viisideks ISP-ga ühendus luua on kasutada lairiba ühendust (kaabel või DSL). Lisaks on kasutusel raadiolingid ja mobiilivõrgud.

**Port 80 ehk Web** – tegemist on TCP 80 teenusega, millel üldiselt töötab veebiserver.

**Kasutajaliides** - tarkvara- ja riistvarakogum, mis võimaldab kasutaja interaktsiooni Arvutisüsteemiga.

**Kasutus- ja vastutusleping** - kahe huvipoole vaheline juriidiliselt siduv, või samasugune täielikult organisatsioonisisene lepe tarkvarateenuse või infosüsteemi teenuse osutamise kohta teenuse kasutamise tingimuste ja teenuste kirjelduste esitamisega.

**MAC-aadress e. meediumipöörduse juhtimise aadress** - identifitseerib arvuti võrguliidese. Igal võrguliidesekaardil on ühene MAC-aadress. Traadita kohtvõrgu turbe tugevdamiseks peaks pääsupunkt võimaluse korral MAC-aadressidega identifitseerima lubatavad klientarvutid.
**Marsruuter, ruuter** - võrguseade erinevate, erinevatel võrguprotokollidel põhineda võivate võrkude vahelise andmevoo loomiseks ja reguleerimiseks teede või marsruutide valimisega marsruutimisprotokolli mehhanismide ja algoritmide alusel, kusjuures marsruutimisteavet hoitakse marsruutimistabelis.

**Tugijaam (Pääsupunkt, Access Point)** - riistvaraseade või arvutitarkvara, mis töötab sidejaoturina ning võimaldab traadita terminali kasutajatele juurdepääsu statsionaarsele kohtvõrgule.

**Standard IEEE 802.11** - IEEE traadita kohtvõrgu tehnoloogia standardite perekond. Kasutaja saab kohtvõrguga ühendust pidada raadiokanali (traadita ühenduse) kaudu

**WiFi teenuste identifikaator, SSID (Service Set Identifier)** - traadita pääsupunktide identifikaator, harilikult nime kujul. SSID eristab ühte traadita kohtvõrku teisest, ning kõik konkreetsesse võrku ühendatud seadmed peavad omama ühte ja sama SSID-d. SSID kujutab endast32-baidist tõstutundlikku tekstistringi, mis lisatakse kõigile antud võrgus liikuvatele andmepakettidele.

**Traadita kohtvõrk, WLAN** - raadiosagedusi kasutav traadita kohtvõrk. Levinuimad kasutatavad standardid on IEEE 802.11b, 802.11g, 802.11n, 802.11a, 802.11ac edastuskiirustega vastavalt 11 Mbit/s kuni 800 Mbit/s, sagedusel 2,4 GHz ja 5 GHz.

**Tuvastamine** - olemi identiteedi tõestamine autentimise positiivse tulemuse korral.

**WEP (Wired Equivalent Privacy), "traatsidele vastav privaatsus"** - krüptograafiaprotokoll, mis on määratletud traadita kohtvõrgu standardites IEEE 802.11.

WEP pakub side krüpteerimist 40- või 104-bitise jaosvõtmega. See võti ühendatakse 24-bitise algväärtustusvektoriga, nii et tulemuseks on 64- või 128-bitine võti. Protokollide teadaolevate nõrkuste tõttu tuleks turbe tugevdamiseks WEP võtmeid tihti vahetada. WEP järglane WPA2 ületab õige konfigureerimise puhul need nõrkused, pakkudes ajutisi jaosvõtmeid.

**WiFi leviala** – traadita arvutivõrgu leviala, mis on teostatud ühtesobivate seadmetega.

**WiFi, Wireless Fidelity** - traadita kohtvõrgu seadmete tootjate ühenduse WiFi Alliance'i kaubamärk. WIFI sertifitseeritud logo seadmel tähendab, et seade vastab nõuetele ning on koostoimiv teiste WiFi logo kandvate seadmetega.

**Virtuaalne kohtvõrk, VLAN** - virtuaalseid kohtvõrke kasutatakse võrkude loogiliseks struktureerimiseks. Seejuures moodustatakse füüsilise võrgu sisse loogiline võrgustruktuur, et ühendada funktsionaalselt kokkukuuluvad töökohad ja serverid ühte virtuaalsesse võrku.

**Virtuaalne privaatvõrk, VPN** - ühisvõrke kasutav privaatvõrk. Näiteks krüptograafilisel tunneldusel põhinev võrk, mis töötab teise võrgu infrastruktuuril. Virtuaalne privaatvõrk on võrk, mida füüsiliselt rakendatakse teise võrgu (tihti Internet) sees, kuid mis on loogiliselt
sellest võrgust lahutatud. VPNides saab krüpteerimismeetmete abil kaitsta andmete terviklust ja konfidentsiaalsust, samuti saab kindlalt autentida kommunikatsioonipartnerit, seda ka juhul, kui mitmed võrgud või arvutid on rendiliinide või avalike võrkude kaudu üksteisega ühendatud. Mõistet „VPN“ kasutatakse tihti tähistamaks krüpteeritud ühendusi, transpordikanali kindlustamiseks võib siiski kasutada ka teisi meetodeid, näiteks kasutatud
ülekandeprotokolli spetsiaalseid funktsioone.

**WPA ja WPA2 (WiFi protected Access), "kaitstud WIFI"** - turbe tugevdamise spetsifikatsioon traadita sidele konfidentsiaalsuse ja tervikluse pakkumiseks on andmeturbe protokoll IEEE 802.11 standardile. WPA arendus oli tingitud eelmise süsteemi WEP puudustest. WPA kasutab ajutise võtme teostuse protokolli TKIP (Temporal Key Integrity Protocol) ning AES algoritmi (WEP kasutas RC4 algoritmi).

**Arvuti võrgu aadressi teisendus, NAT / Network Address Translation** – Kasutusel oleva IP aadressi teisendamine üldkasutatavaks ja vastupidi. NATi kasutatakse kuna saadaval olevad avalikud IP aadressid on piiratud ressurss. Tavaliselt jääb NATist kasutaja poole sisevõrgu IP aadressid ning teisele poole NATi avalik internet.

**Avalik IP aadress** – Avalik IP aadress on kätte saadav üle interneti, eeldusel, et sellele pole kehtestatud tarkvaralisi piiranguid nagu tulemüür.

**Privaatne IP aadress** – sisevõrgu kasutatav IP aadress, millele internetist otse ühendust võtta ei saa.

**Roaming** - võimalus liikuda ühe AP levist teise säilitades olemasolevad ühendused. Spetsiaalne roamingu standard on kirjeldatud IEEE 802.11r kuid roaming võib toimuda ka ilma seda rakendamata.

**Klientide isoleerimine** - turvameede, mis keelab ühel levialas oleval seadmel võtta ühendust teise seadmega. Vähendab viiruste levikuks ja rünnete võimalusi, samas piirab ka kasutajate omavahelise suhtlemise kohtvõrgus, suhtlus toimub läbi veebititeenuste: Skype, Viber jne.

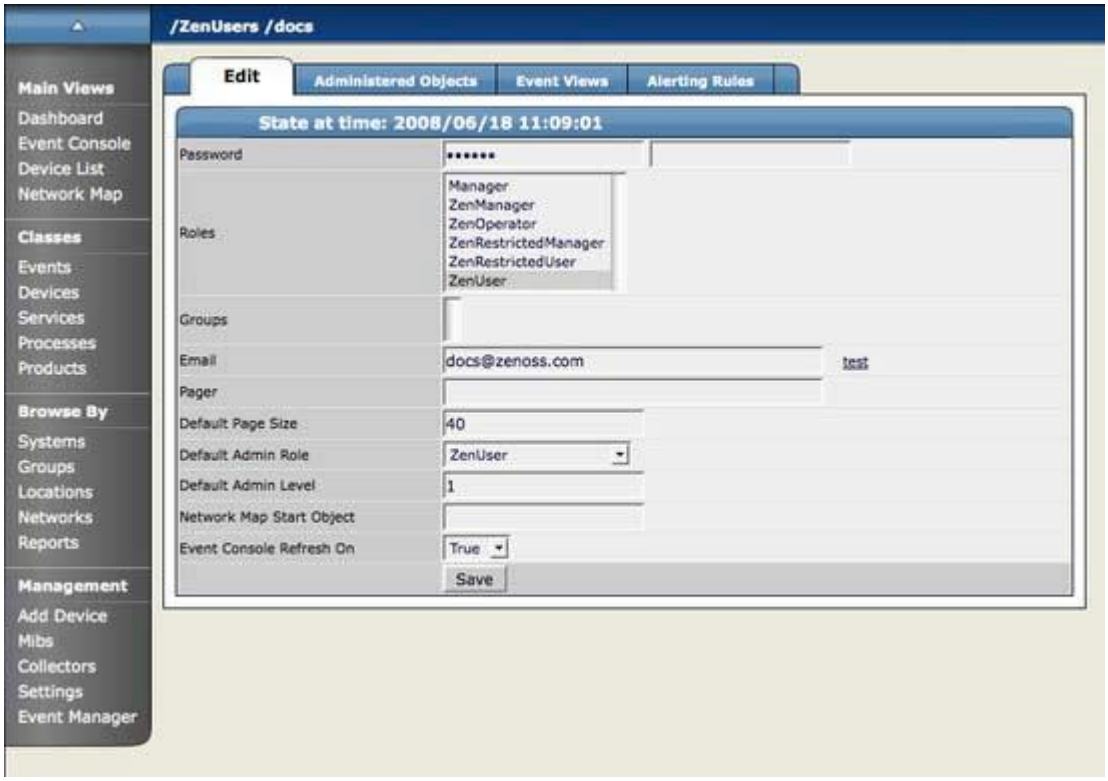
# 3 Kasutusliidese funktsionaalsuse kirjeldus.

### 3.1 Sissejuhatus kasutusliidese kirjeldusse.

Kirjeldame kasutusliidese funktsionaalsust. Kasutusliidese all mõeldakse lahenduse seda osa, mida kasutab inimene või läbi mille on süsteem ühendatud teise süsteemiga. Kirjelduse lihtsamalt arusaadavaks tegemiseks on toodud näidislahenduste joonised. Heas süsteemis on vähemalt kaks kasutusliidest, milleks on - kasutaja ligipääsu liides ehk võrgu uks ja süsteemi haldamine.

### 3.2 Kasutusliidesed:

Iga kasutajaliidese kohalt toome eraldi välja, kelle jaoks see on:




- WIFI kasutaja või WIFI leviala looja/haldaja.
- mida saab teha - mis selle eesmärk on.

#### 3.2.2. administreerimine.

Administreerimise lehekülge kasutatakse süsteemi määrangute ja teiste süsteemidega liitmise seadistamiseks. Sellel leheküljel määratakse leviala nimi, kus asub esilehekülg, kellel millised õigused on administreerimiseks, jne.

Administreerimise lehekülge kasutab leviala haldaja, kes kasutab seda muudatuste tegemiseks süsteemis.

### 3.2.3. Avalehe ehk ukse lokaliseerimine

Avaleht on uks, mille kaudu kasutaja siseneb võrku, nõustudes kasutuslepingu tingimustega.

Soovitatav on koheselt uksele lisada võimalus siseneda läbi autentimise internetiteenuse piiramatuks kasutamiseks ja juhul, kui kasutaja keeldub autentimisest, siis vastavalt pakkuja soovile kas teavitada teda kasutamise mittelubamisest või siis luua piiratud kasutamise võimalus ( internetti kasutada vaid pakkuja koduleheküljе piires või piiratud kiirusega).
Vt ka pt. 4 "Kasutajate tuvastamise nõuded".

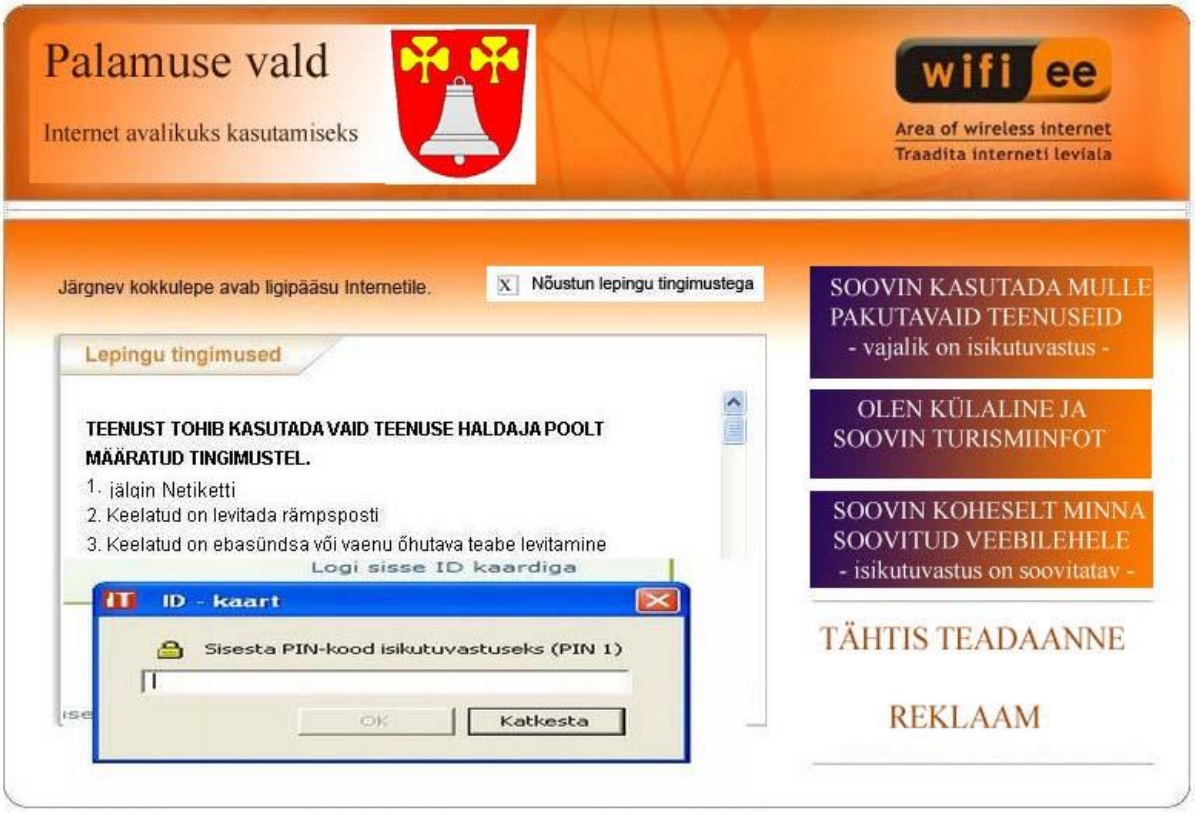
Uks on WiFi leviala kasutajale.

Uksele lisatakse vajalikud teabelingid, reklaam ning muu asukohapõhine teave.
Kuna süsteemi on võimalik luua liigendatult ehk kasutada ühte süsteemi mitmete asukohtade jaoks, siis on mõistlik luua pilve valmis avalehe vorm, mida pakkuja saab täita ning läbi selle hästi lihtsalt luua oma graafilise disaini ja sisuga WiFi-ukse.

### 3.2.4. kasutaja tuvastamine

Kasutaja tuvastamiseks sisestab kasutaja oma ID-kaardi PIN1-koodi või nime ja parooli, mille abil ta tuvastatakse ning lubatakse internetti kasutama.

Tuvastamise lehekülg on WiFi leviala kasutaja jaoks, et ta saaks ennast tuvastada




interneti teenusepakkujale. Autentimisega luuakse olukord, kus teenuse kuritarvitamise korral on võimalik kasutajat tuvastada, samas kohustub teenusepakkuja autentimisega seotud informatsiooni mitte avaldama kolmandatele osapooltele (vt ka p 9 WiFi kasutuslepingu näidist). Läbi kasutaja tuvastamise saab teenuse kasutajale tagada teiste autentimist eeldavate teenuste kohese kasutamise võimaluse.

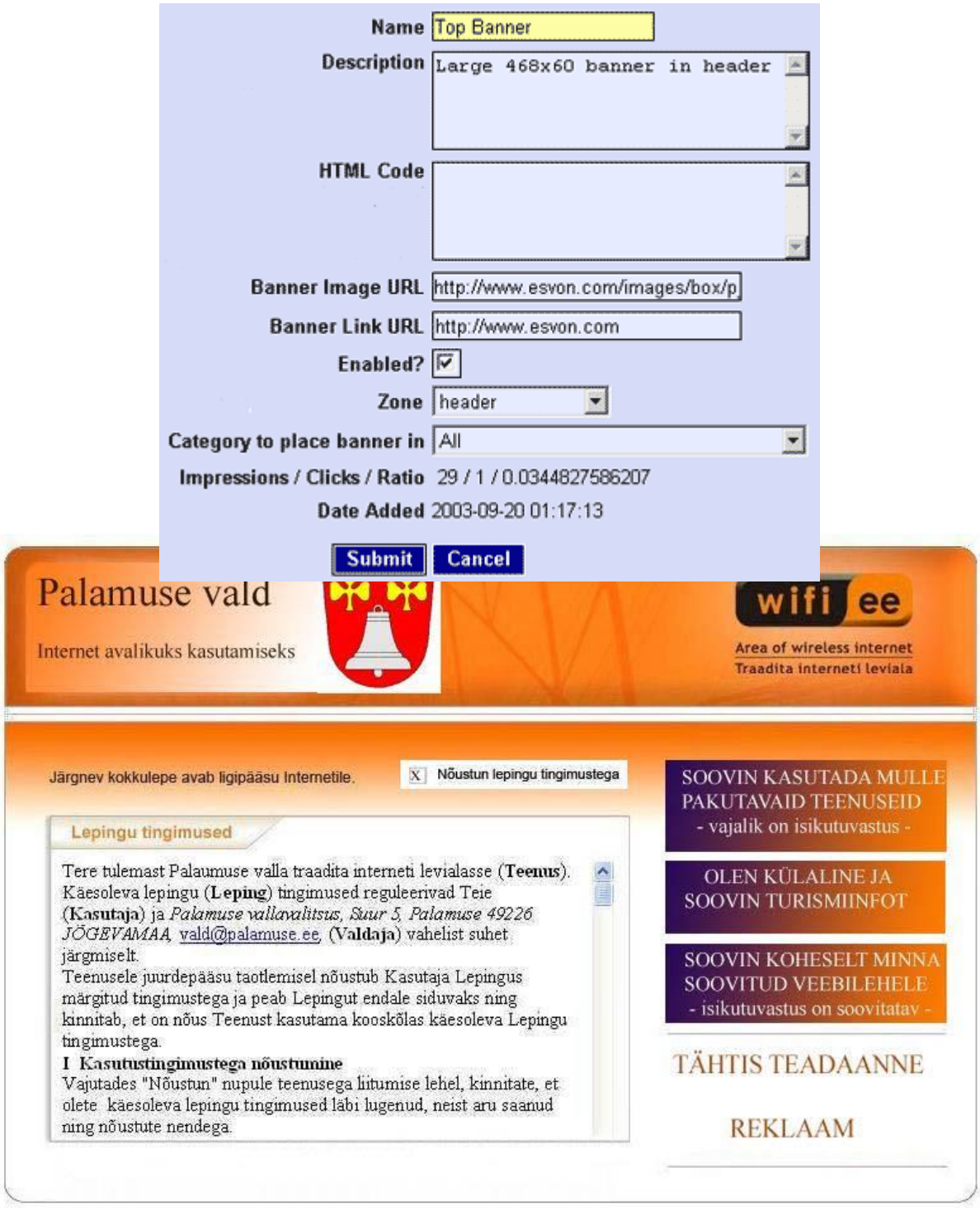
Kasutaja tuvastamise kiirendamiseks on võimalik pruukida GMail, FB, Linkedin jne. kontot, mille kasutaja on sidunud oma identiteediga.

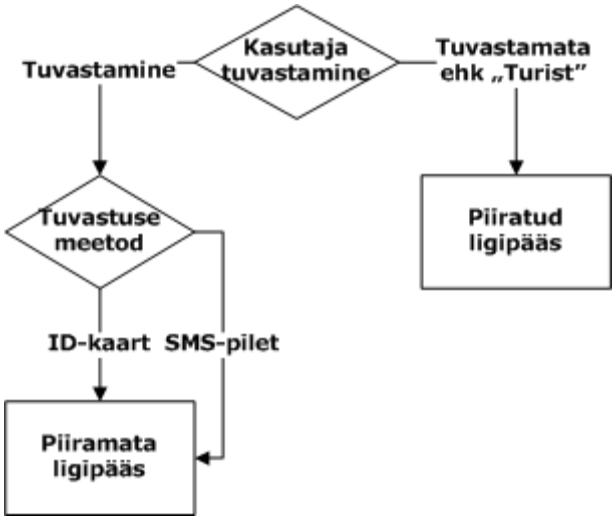
### 3.2.5. kasutusleping

Kasutusleping on ekraani üks osa (tavaliselt esilehel), millel on nuppud „Nõustun“ ja „Ei nõustu“. Vajutades „Nõustun“ nupule saadetakse kasutaja poolt sisestatud nimi ja parool serverile kasutaja autoriseerimiseks

### 3.2.6. Reklaam

Reklaam-kasutajaliides on mõeldud kogu süsteemis avaldatavate reklaamide või avalikkusele edastatavate teadete seadistamiseks. Selle lehekülje abil saab laadida uusi reklaam pilte ja kustutada vanu. Lisaks avaldab see lehekülg ka reklaamidele klikkimise statistika.






# 4. Kasutajate tuvastamise nõuded

## 2.1. Sissejuhatus kasutajate tuvastamise nõuetesse.

Selles peatükis käsitleme kasutajate tuvastamise nõudeid. Kasutaja tuvastamine on vajalik, et turvalisuse seisukohalt oleks hiljem võimalik määratleda probleemide tekitaja ning võimaldada kasutajale isikukohased interneti võimalused (sotsiaalinternet, kiirus, jne.)

Kui kasutaja jääb tuvastamata, siis võimaldatakse talle piiratud kogus teenuseid, milleks üldiselt on veebipõhised teenused - pakkuja koduleheküIg, jne.

**Tuvastamise klassid**

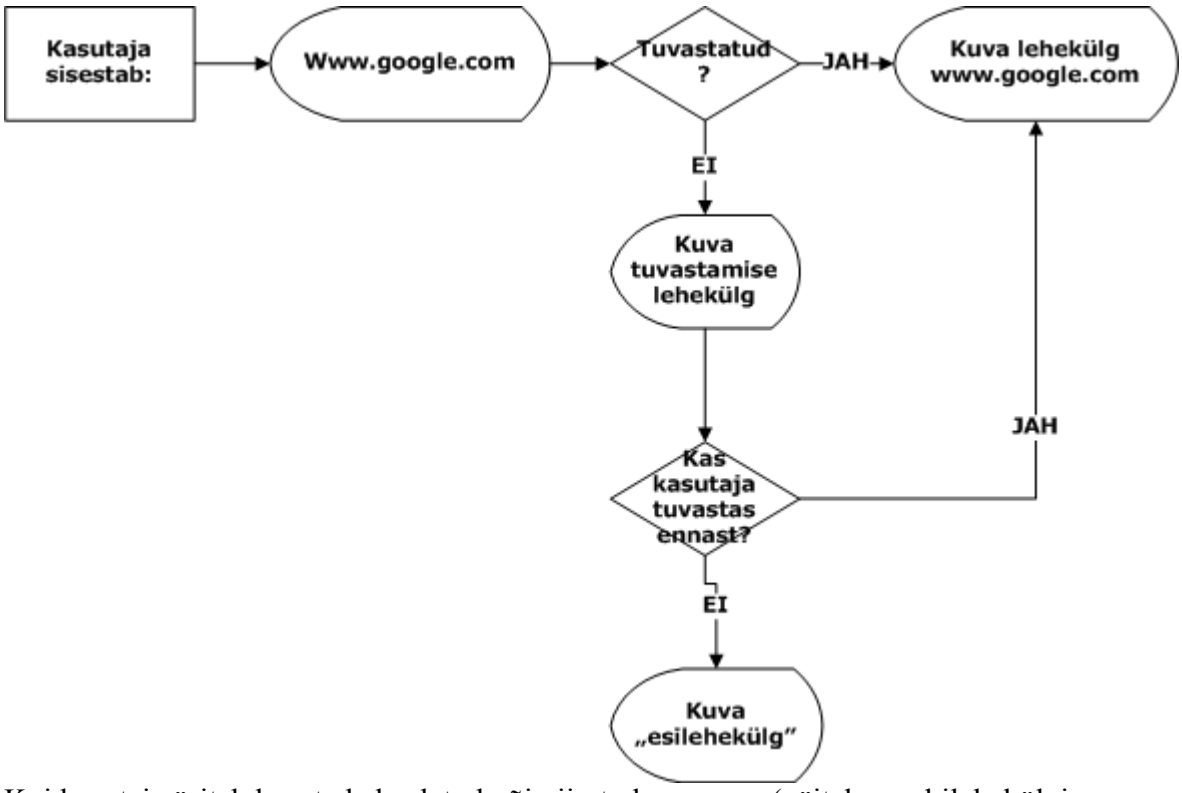
Mõeldavate tuvastusvõimaluste ja põhjalikkuse järgi jaotame klassid nelja kategooriasse, milleks on:

- tuvastamata kasutaja
- ID-kaart ja mobiil-ID
- Open-ID

### 2.1.1. Tuvastamata kasutaja

Tuvastamata kasutaja klassifitseerub oma olemuselt anonüümseks kasutajaks, kes pääseb interneti kasutama anonüümselt. Antud kasutaja vajaduse võib põhjustada vajadus kiirelt ühenduse saamiseks või tuvastamismeetodeid kasutada mitte võimaldava seadme kasutamine.
Sellisteks seadmeteks võivad täna näiteks olla valveseadmed (turvavideokaamera) või WIFI telefon.

Tuvastama kasutajal on interneti kasutamisel piirangud, mis langevad ära enda nõuetekohasel tuvastamisel.




Kui kasutaja üritab kasutada keelatud või piiratud ressursse (näiteks veebilehekülgi, mis pole lubatud), siis suunatakse ta teenuse avalehele ning antakse võimalus ennast tuvastada.

#### 2.1.1.1. Sihtgrupp

Lihtsad seadmed, turistid.

#### 2.1.1.2. Piirangud

Piirangud on mõistlik rakendada ühest variandist:

Lubatud on ainult kindlate veebiteenuste kasutamine, näiteks internetipank, pakkuja koduleht.

Tüüpiline kasutuskoht on klientidele suunatud infokiosk või -leviala.
Lubatud on kõik veebiteenused (pordid TCP:80 j TCP:443). Muud pordid/teenused on suletud. See on paljudes levialades kasutusel olev praktika ning hoiab ära mõningat tüüpi viiruste leviku WiFi kliendilt internetti. Probleemiks on kasutaja võimalus kasutada muid vajalikke protokolle nagu IMAP-SSL TCP pordis 993 e-posti lugemiseks. Lubatud on kõik teenused, välja arvatud TCP port 25. TCP port 25 suletakse reeglina spämmi saatmise ära hoidmiseks. Kindlasti ei tohi seda lubada tuvastamata kasutajale. Tuvastamata kasutaja saab e-posti saata ainult läbi veebiliidese. See on soovitatav variant. Tasub ka tähele panna riske, mis tulenevad "IP over ICMP" ning "IP over DNS" võimalikust kasutamisest ning neid vajadusel maandada.

### 2.1.2. ID kaart ja mobiil ID

Kasutajad logivad ennast süsteemi kasutades ID kaarti või mobiil id. Sellise lahenduse korral on selge, kes on kasutaja.
Lahenduse miinimum teostus põhineb aegunud ja kehtetute sertifikaatide andmebaasile, mida täiendatakse kord ööpäevas. Kasutaja tuvastamisel kontrollitakse, kas sertifikaat on aegunud või mitte. Aegunud või kehtetu sertifikaadi korral tuvastamine ebaõnnestub. ID kaardi kasutajal on vaja teada PIN1 koodi. Kodulehe liidestamist ID-kaardi kasutajate sertifikaatide andmebaasiga korraldab AS Sertifitseerimiskeskus (SK).

#### 4.2.3.1. Sihtrühm

Kasutajate grupp, kelle jaoks on interneti kasutamine tasuta või eelneva registreerimisega. ID-kaardi või analoogse autentimise abiga on võimalik ilma täiendava autentimiseta alustada kohalike e-teenuste tarbimist pakkuja kodulehel.

#### 4.2.3.2. Piirangud

Piirangud puuduvad või siis olemasoleva „kõigile“ kätte saadava ühenduse korral on piiranguks üldlevinud teenused ja kiiruse piirang. Spämmi saatmise vältimiseks tuleks e-posti (porti 25) minevad ühendused lubada ainult ISP enda postiserverisse (näiteks Elionil mail.estpak.ee). Võimalikud piirangute näited juhul, kui pakutava teenuse kiirus ei ole piisav vabaks kasutamiseks:

1. massiivne andmevahetus (>100 MB failide liigutamine) on lubatud kell 00.00 - 06.00
2. Kasutajale lubatud andmesidemaht on X GB kuus.

### 2.1.3. Open ID

On teatud juhtudel alternatiiv ID kaardile (EstOpenID kasutuselevõtmisel). Võimaldab „volitada“ teatud autentimise õigusi.

#### 4.2.4.1. Sihtrühm

Allkirjaõigust mitte omavad ehk alaealised, kes soovivad kasutada vastavalt vanema antud ID kaardi volituse alusel.

#### 4.2.4.2. Piirangud

Sarnased ID-kaardile.

# 5. Ühenduse turvalisus

## 5.1. Ühenduse turvalisus.

Kasutaja poolt vaadates tähendab sidevõrgu turvalisus põhiliselt kahte asja –võrgu kaudu edastatav info ei tohi olla kättesaadav võõrastele (asjasse mittepuutuvatele) isikutele ja et edastatav info ei tohi olla teekonnal lähtepunktist sihtkohani võõraste poolt muudetav ning lihtsasti võltsitav. WiFi võrgu kontekstis on kahjuks mõlemad kirjeldatud punktid tavalise, avatud võrgu puhul, täitmata – kui kasutaja ise midagi ette ei võta, on tema poolt saadetav informatsioon WiFi võrgus teistele nähtav ning halvemal juhul ka muudetav või võltsitav.

Lahenduseks on VPN ühenduse või raadiovõrgu salastuse (krüpteeringu) kasutamine.

Lisaks ülaltoodule jäävad kasutajat võrgu turvalisuse valdkonnast vaadates ohustama erinevad internetist lähtuvad arvutivõrgu rünnakud, ussid, viirused jms ohud, mille vastu võib siiski osalist abi saada kogu võrku korralike(seadistustega) tulemüüride, ründetuvastuse/tõkestuse- seadmete (IDS/IPS Intrusion Detection System ja Intrusion Prevention System) kaitsmisega.

Teenusepakkuja poolt vaadates tähendab turvalisus lisaks kasutaja poolsetele tingimustele ka vastutust võrgu kui terviku toimimise eest (näiteks kas üks klient või rikkes sõlmpunkt suudab kogu võrgu töö seisma panna?), võrgu juurdepääsuõiguste toimimise (kes ja kuskohast võivad mingitele võrgu osadele juurdepääsu omada) ning võimaliku kuritarvituste (klientide tahtlik või tahtmatu, sh viiruste ja „troojalaste“ toime tõttu toime pandu) tõkestamine või siis tagajärgedega tegelemine. Tavalise avatud WiFi võrgu puhul sõltub teenusepakkuja poolse turvalisuse osa paljuski kasutatavast riistvarast ja selle seadistustest, näiteks on turvalisust tõstvateks tegevusteks WiFi klientide tugijaama piires üksteisest isoleerimine (inglise k. AP Isolation), võrguliikluse filtreerimine, võrguseadmetele (või erinevatele kasutajagruppidele) eraldi haldusvõrgu(VLAN) kasutamine.

## 5.2. VPN ja andmete salastamine.

Lisaks tavalistele, avatud WiFi võrkudele on olemas ka väga turvalisi WiFi võrke. Kahjuks tuleb nende puhul enamasti siiski teha väga suur kompromiss turvalisuse ja kasutusmugavuse vahel – praktiliselt kõik turvalised süsteemid nõuavad teatavaid eelseadistamisi (ja halvemal juhul ka teadmisi), mis teevad nende kasutamise avaliku, kõigile kättesaadava teenuse pakkumiseks keeruliseks, kuigi mitte võimatuks.

Seega tuleb avaliku WiFi puhul hetkel kasutada siiski kaks võimalust:
teenuse kasutamisel tulebki arvestadagi ebaturvalise sidekanaliga ning motiveerida WiFi kliente kasutama turvatud veebilehti (HTTPS) ning rakendusi (näiteks SSL toetusega e-posti tarkvara) ja VPN (Virtual Private Network) tehnoloogiat.

Väga lühidalt öeldes tähendab VPN internetiühenduse sisse veel ühe teise, võõraste eest kaitstud ühenduse tegemist. Loomulikult nõuab VPN teist “otsa” kuhumaani kliendi seadmest selline kaitstud ühendus toimib, see VPN teenuse teine ots võib

minimaalselt asuda ka näiteks sama WiFi tugijaama juures või siis WiFi võrgu keskseadmes. Ühe VPN lahenduse suurimaks miinuseks on selle seadistamise keerukus. On olemas küll igasugu lihtsaid pakette/viisardeid/juhendeid, kuid reeglina on toimiva VPN ühenduse käivitamine väga kasutatava operatsioonisüsteemi (ning paljudel mobiilsetel seadmetel ka riistvara) spetsiifiline tegevus ning igalt teenuse kasutajalt seda oskust eeldada pole võimalik.

Siinkohal võib tuua väikese muutuse viimasel ajal jõudsalt levima hakanud SSL-VPN (Secure Socket Layer Virtual Private Network) tehnoloogia, mida saab kasutada ka tavalise brauseriga. SSL-VPN lahendus võimaldab läbi HTTPS (HTTP üle SSL) teenuse turvalist ühendust nii veebiliiklusele, mitmesugustele terminalilahendustele kui ka teistele võrguressurssidele (sh IP tunnel). Analoogiliselt tavalise VPN ühendusega on muidugi ka SSL VPN puhul vajalik keskne server, mis VPN ühendusi vastu võtaks Kui vähegi on võimalik, tuleks kaaluda lisaks avalikule ning ilma salastuseta WiFi võrgule ka teise, tugeva turvatasemega (näiteks WPA2) WiFi võrgu tekitamisele ning selle kasutamise reklaamimisele. Sellist „multiple SSID“ mitme võrgu korraga tekitamist võimaldavad kaasaegsed baasjaamad. Ligipääsu koode turvalise võrgu kasutamiseks võib jagada klientidele konkreetsel objektil või välja töötada lahendus Eesti ID rakendamisel turvalise võrgu ligipääsu autoriseerimisel. ID põhise lahenduse väljatöötamine nõuab alguses küll tööd, kuid korra välja töötatud lahendust on ilmselt lihtsasti võimalik rakendada lihtsamalt juba paljudel WiFi baasjaamadel.

### 5.3. Klientide kontroll.

Kirjeldatavas süsteemis peaks kindlasti olema võimalus klientide kontrolliks. Olulised parameetrid, mida kontrollida ja vajadusel logidesse salvestada saaks, on näiteks tugijaamade kohta klientide MAC ja IP aadressid ning võrku sisenemise ja lahkumise kellaajad. Kuna sellest infost on reaalne kasu ainult serveri põhise logide kasutamise korral, tuleks vastav lahendus ka seadistada. Võimalike probleemide paremaks lahendamiseks on soovitav kasutada teekonnal kliendi seadmest avaliku internetini ainult ühte võrguaadresside transleerimise (NAT) toimingut, niimoodi on võimalik kontrollida võrgu toimimist kliendist kuni keskseadmeni ja ka teistpidi.

### 5.4. Vastutuse piirid.

Turvalisusega on praktiliselt alati seotud ka vastutus.
Avaliku teenuse puhul tuleb paika panna, kes ja kuipalju turvalisuse ja võrgus toimuva eest vastutab. Võimalikud probleemid on seotud anonüümsete või peaaegu anonüümsete klientide võimaliku lubamatu tegevusega võrgus.

Võrgus ilmselgelt keelatud tegevused on mainitud liitumise tingimuste juures ning võrgu kasutuskorraga tuleb kliendil nõustuda enne talle võrku ligipääsu võimaldamist. Võrgu haldaja saab osaliselt oma vahenditega piirata mittesoovitavat käitumist võrgus, kui logimine toimib korralikult saab klienti rikkumistest ka teavitada või ka tema teenus peatada.

Loomulikult vastutab kaudselt avalikus võrgus toimuva eest ka võrgule internetiteenust

pakkuv ISP (Internet Service Provider ehk WiFi-võrgule internetiteenuse pakkuja), kes mingil võib samuti seada piiranguid osa/kogu võrgu tööle, täpsed tingimused toodud välja ISP teenuse lepingus.

### 5.5. Terviklahendus.

Teenuse avaleht, klientide autentimine ja VPN teenuse võimalus on kokku terviklahendus, mis aitab nii kliente kui teenuse pakkujat, sisaldades kõike vajalikku turvalise (WiFi) teenuse kasutamiseks. Dokumendid turvalisuse probleemide tutvustamisega ning lahenduste kohta (sh näiteks VPN kasutamise juhend ja turvalise paralleelvõrgu kasutamise juhend) peaksid olema viidatud teenuse avalehelt.

# 6. Haldusmudeli kirjeldus.

Sõltumata sellest, kas WiFi-leviala luuakse avalikuks kasutamiseks klientidele, turistidele või elanikkonnale, kellel pole võimalust kvaliteetset püsiühendust hankida, tuleb luua peale nõuetele vastava leviala rajamist ka jätkusuutlik haldusmudel, kuidas WiFi-leviala ülalpidamisega seonduvaid teemasid lahendada.

Põhiküsimused on:

### 6.1. Kes hoiab teenuse töös?

Tuleb leida partner, kes tegeleb võrgu hoolduse ja klientide probleemidega.
Partneri kohus on lahendada jooksvad probleemid ja garanteerida objektide WiFi ja kohtvõrkude töö.

A. Omavalitsus sõlmib teenusepakkujaga leppe doteeritud teenuse osutamiseks oma elanikele. Elanikele tuleb tagada ligipääs Internetile kiirusel vähemalt 128 kbit/s (Kasutajate tuvastamine ja arvestus toimub ID kaardi, mobiil ID abil või mõne muu autentimismeetodi kasutamisel, mis tagab registreeringu logi pidavasse andmebaasi. Teenus peab olema kaughaldusega- võimaldama kokkulepitud piiranguid ja kontrollida teenuse töövõimet kohapeale minemata.
Vajadusel siiski tagab ettevõte ka kasutajatoe ning abistamise teenusetarbija asukohas.

B. Omavalitsus ja ettevõtja sõlmivad koostööleppe, mille alusel ettevõtja pakub avalikku WiFi teenust oma asukohas. WiFi paigaldamine toimub sel juhul omavalitsuse kulul, kuid teenuse püsikulud tasub ettevõtja.
Samal viisil on sobiv toetada AIP loomist.

Eeskujuks sobivad Tartu linn ja Taheva vald, kelle võrgud on töös püsinud > 10 aasta.

### 6.2. Kuidas on korraldatud kontroll ja järelevalve teenuse osutamise üle.

See, kui avaliku WiFi-teenuse osutamine on üle antud teenusepakkuja ettevõttele, ei vabasta vastutusest kontrollida teenuse osutamise nõuetele vastavust ja vajadusel sekkumist lepingu nõuetekohaseks täitmisks. Seetõttu peab olema määratud teenuslepingu täitmise eest järelevalvet teostav isik, kelle kontaktandmed lisatakse

WiFi-esilehele kliendikaebustega või leviala kuritarvitamisega seotud probleemide lahendamiseks. See määratav isik omab vastavalt oma ametiülesannetes sätestatud juhtudele õigusi ligipääsuks autentimise ja internetiteenuse kasutuslogide andmebaasidele.
Võrkude korrasolekut ja kasutusmahtu peab olema võimalik eemalt jälgida.

### 6.3.Reklaami või asukohapõhise teabe kasutamine WiFi-uksel.

Reklaam ja teave postitatakse kindlale veebiaadressile, mis on seotud WiFi uksega.
Sel viisil saab teabe vahetamisega hakkama müügijuht või sekretär.

### 6.4. Kuidas on tagatud teenuse töökorras hoidmine ja amortiseerunud tehnoloogia väljavahetamine, et oleks tagatud teenuse osutamise töökindlus ja jätkusuutikkus.

Tehnikat on WiFi-lahenduse korral nii väljas, ilmastikumõjude käes (POE WiFi AP) kui toas (võrgu kestseade + server jne.).
Paigaldatud ja teenusepakkumiseks kasutatav riistvara vajab pidevat järelvalvet + hooldust, mille teostab lepingupartner.

# 7. Riistvara funktsionaalsus

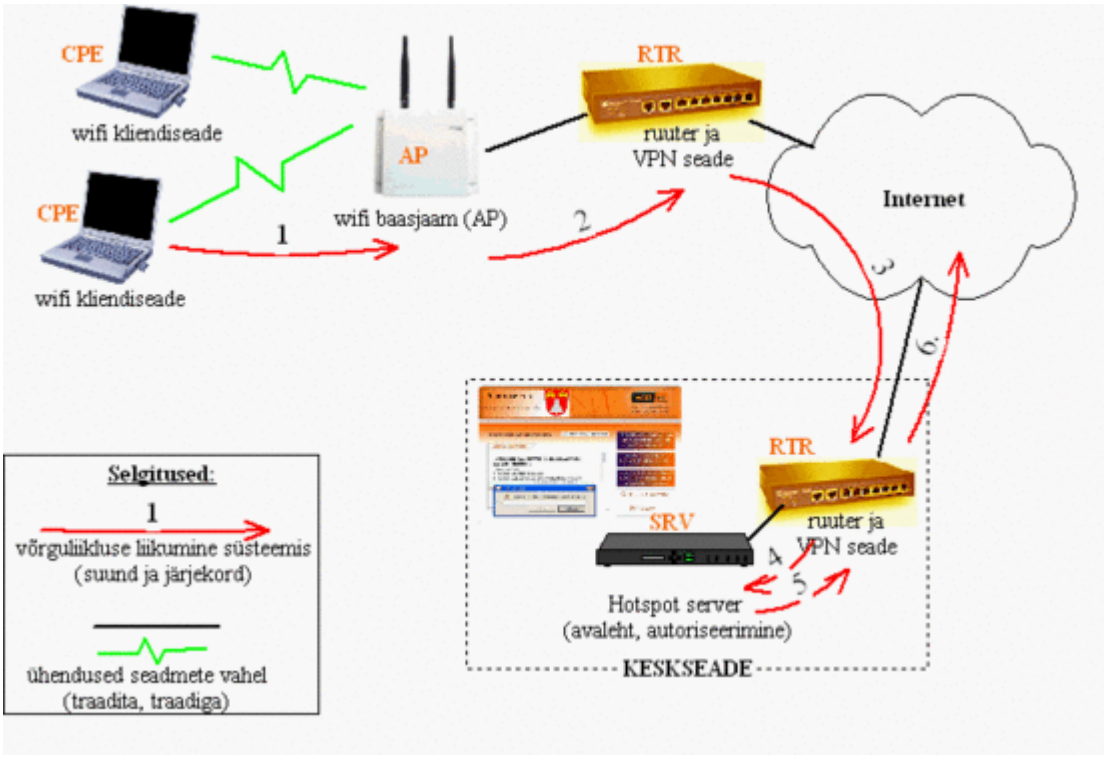
### 7.1. Eessõna

Korraliku WiFi lahenduse teostamisel tuleb seadmete valikul lähtuda nii lahenduse suurusest, st planeeritavast tugijaamade ning klientide arvust kui ka planeeritavast koormusest, st palju üheaegseid kasutajaid arvatakse tulevat.

Kui lahenduse loomine eeldab ka ühenduste loomist tugijaamade vahel, tuleb arvestada, et võrguliikluse koormus tugijaamade vahel on oluliselt suurem, kui tugijaamast kasutaja arvutini. Seetõttu tuleb kõnealuste ühenduste rajamisel arvesse võtta, et need ühendused (nii traadita- kui ka kaablivõrgu korral) tuleb teha ka korralike ja selleks mõeldud seadmete abil.

Repiiterite (vahevõimendite) kasutamine ühe baasjaama signaali edastamiseks teise seadmeni ei ole mõistlik, kuna wifi raadiokanal on jagatud ressurss ning repiiteri kasutamine vähendab KOGU võrgu kiirust vähemalt 2 korda, lisaks süvenevad oluliselt nö peidetud kliendi probleemid, kus kahe üksteist raadio mõttes mitte nägeva kliendiseadme poolt korraga baasjaama poole saadetud info muutub müraks ning mõlemal seadmel tuleb oma saatmist korrata. Baasjaamade omavaheliseks ühendamiseks on kõige parem siiski kas tavaline võrgukaabeldus (CAT5), optiline kaabel, DSL modemid või ka selleks ette nähtud raadiolingi seadmed, näiteks 5GHz sagedusvahemikus ning kohe välitingimustes toimimiseks mõeldud seadmed.

**7.2. Ruuter, võrgu keskseade, saatja. Viited seadmete kehtivatele standarditele.**

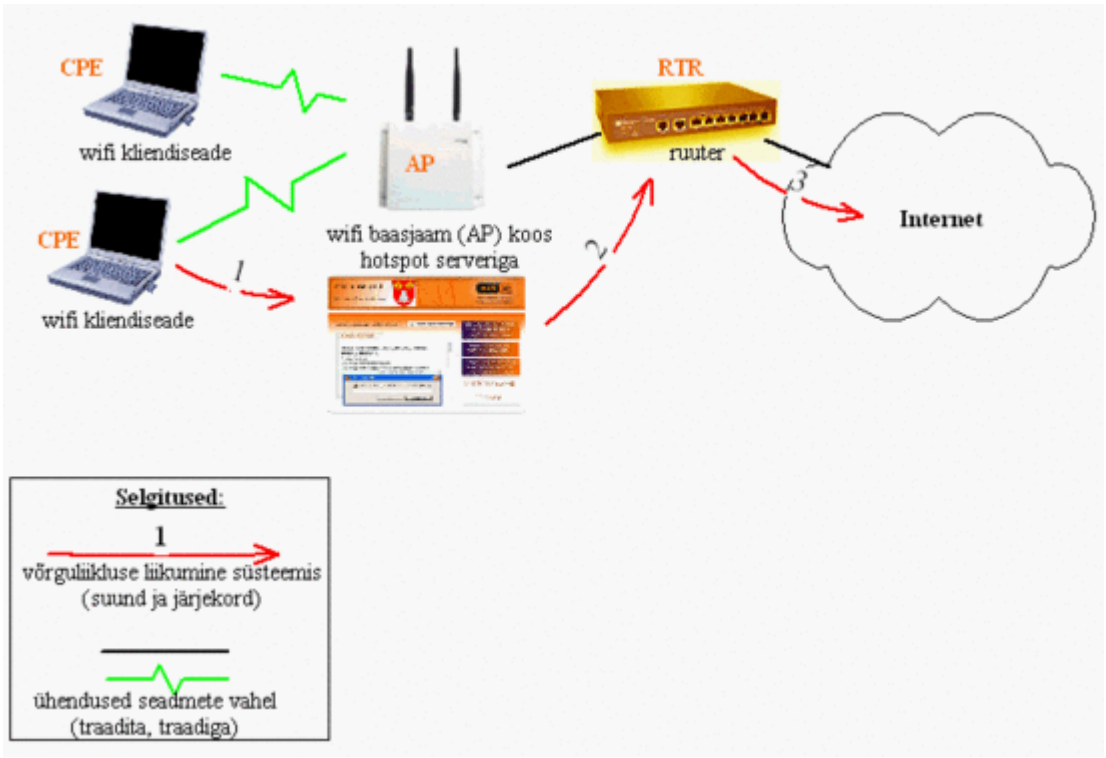



Lahenduse kirjeldus.

*Joonis 1*

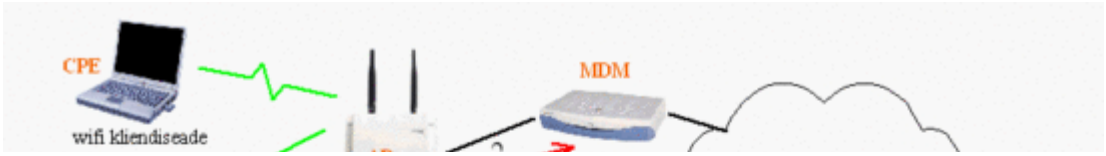
Tõsisemate WiFi võrkude rajamisel tuleb soovitada kolmekihilist lahendust (vt joonised 1 ja 2): On olemas WiFi baasjaam (AP ehk Access Point), ruuter (joonisel RTR) ja keskseade (joonisel SRV). Sellisel juhul liigub kõik WiFi klientidelt (joonisel CPE) tulev liiklus (vt punase noolega tähistatud teekond 1 ja 2) läbi VPN tunneli (joonisel teekonnad 3 ja 4) keskseadmesse, mis kuvab kasutajale WiFi avalehe ning peale seal edukat autoriseerimist võimaldab ligipääsu internetile (teekonnad 5 ja 6). WiFi juurdepääsupunkti ülesandeks on kasutajatele ühenduse võimaldamine ning minimaalse turvalisuse tagamine (kasutajate vahelise liikluse blokeerimine, soovi korral WPA2 või VPN tehnoloogial turvalise ühenduse võimaldamine).

Kui WiFi võrgu jaoks on baasjaama ja keskseadme vahel kasutada oma etherneti taseme sisevõrk (näiteks VDSL ühendused, fiiberoptika, raadiolingid või juba olemasolev VPN süsteem), pole iga baasjaama juures vaja ruutereid kasutada, piisab kas modemitest või switchidest (sõltuvalt ühendustest). Sellise võrgu lahenduse eeliseks on kokkuhoid juba olemasoleva sidevõrgu ärakasutamisel (või sidekulude pealt, kui pole tarvis täiendavaid ühendusi osta) ning piisavalt suure läbilaskega võrgu

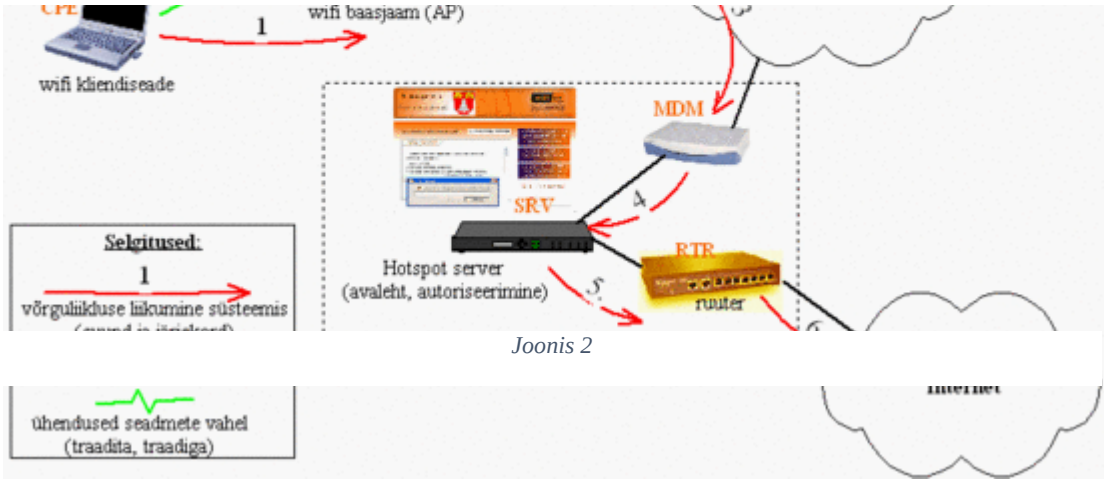



korral pole vaja muret tunda ühenduskiiruste piiramise pärast juba baasjaama juures. Lahenduse skeem on toodud joonisel 2, modem on tähistatud MDM-ga ning liiklus kliendiseadmest kuni internetini punaste nooltega.

Väikese võrgu (vt Joonis 3 ) korral saab loomulikult neid kihte kombineerida ning teha osa või kogu funktsionaalsuse ära ühe seadmega, siis asuks WiFi baasjaama (AP)




*Joonis 3*




*Joonis 2*

sees ka autoriseerimise ning avalehe server ning liiklus kulgeks WiFi klientidelt (CPE) läbi juurdepääsupunkti (teekond 1 ja 3) ja ruuteri (RTR) otse internetti (teekond 3).

### 7.3. Sidekanalid.

Mõningal määral sõltub kasutatav riistvara funktsionaalsus (st kuidas seadmed häälestatakse) ka sellest, millised sidekanalid on võrguseadmete vahel kasutusel, milliste parameetritega on kogu võrgu väline internetiühendus. Näiteks seab see piirid, kuskohas tuleb piirata klientide sidekiiruseid, kas juba WiFi tugijaamas või keskserveris – kui WiFi baasjaama ja keskserveri vahel on kiire internetiühendus, puudub vajadus tegeleda kiiruste piiramisega WiFi baasjaamas. Kui oluline on teenuse katkematu kättesaadavus, tuleks kasutada sidekanalite dubleerimist. Näiteks lisaks põhilisele DSL ühendusele võib tagavara ühendus olla üle mõne raadiosidet kasutava võrgu. Selline lahendus nõuab WiFi baasjaamale ühendust andvalt ruuterilt vastava funktsionaalsuse olemasolu.

### 7.4. VPN ühendused.

Et tagada kasutajatele suurem turvalisus, võib teenuse juurde ühe lisavõimalusena pakkuda VPN ühendust. Selleks tuleb kasutaja seadmest (CPE) vastava tarkvara abil luua turvaline sidekanal kliendiseadme ja VPN serveri vahele. VPN server võib asuda näiteks keskserveri juures (Joonis 1 ja 3, keskseadme ruuter RTR), olla wifi baasjaama (AP) sees (joonis 3 puhul) või olla ka hoopis väljaspool kirjeldatavat võrku, näiteks interneti teenusepakkuja juures. Kui kasutada VPN serverit koos keskseadmega, on tehniliselt võimalik ühendada VPN sisselogimine ja wifi võrgu avalehe sisselogimine. Selleks peab VPN server olema ühendatud keskseadme kasutajate andmebaasiga, võimaldades VPN ühenduse loomisel kasutada WiFi võrgu sisselogimise kasutajatunnust ja parooli või siis ID-kaardi põhist autoriseerimist.

### 7.5. Nõuded seadmetele

Käesolevad seadmed peavad vastama järgmistele standarditele või omadustele:

#### 7.5.1. Wifi tugijaam (AP)

Eesti Vabariigi õigusaktid. (RTL, 20.06.2003, 72, 1056, http://www.riigiteataja.ee/ert/act.jsp?id=598354)

- EN300.328 (üldised nõuded raadioseadmetele)
- IEEE 802.11b (WiFi võrgud sagedusel 2.4GHz, modulatsioonikiirus kuni 11Mbit/s)
- IEEE 802.11g (WiFi võrgud sagedusel 2.4GHz, modulatsioonikiirus kuni 54Mbit/s)
- IEEE 802.11a* (Wifi võrgud sagedusel 5GHz, modulatsioonikiirus kuni 54Mbit/s)
- IEEE 802.11n** (MIMO tehnoloogiaga wifi võrgud, modulatsioonikiirus kuni 300Mbit/s)
-IEEE 802.11ac ( WiFi võrgud sagedusel 5 GHz, kiirusel kuni 800 Mbits )

Turvalisus:

- IEEE 802.11i ehk WPA2*
- Klientide isoleerimine baasjaama piires
- IEEE 802.1q ehk VLAN*

Kaughaldus:

- SSHv2
- SNMP
- ülevaade kõigist raadio klientidest (signaalitugevused, vead, info hulk),
- Syslog
- NTP (interneti aja protokoll)*,
- mõistlik konfiguratsiooni haldus (salvestamine, taastamine).

- Suurema süsteemi puhul (üle 5 WiFi baasjaama erinevates asukohtades) peab olema võimalik kasutada süsteemi ühtseks haldamiseks keskset haldussüsteemi või tarkvara.

Lisavõimalused:

- IEEE 802.1p ehk QoS*
- IEEE 802.11r** (kiirem roaming baasjaamade vahel)
- kaugtoide (PoE, IEEE 802.3af või passiivne)*

### 7.5.2. Ruuter

Ühenduvus:

- seadmel peab olema vähemalt kaks võrguliidest
- VPN toetus (IPSec)
- L2 taseme VPN*
- VLAN võimalus (suuremate süsteemide korral)*

Kaughaldus:

- SSHv2
- SNMP
- Syslog
- NTP
- mõistlik konfiguratsiooni haldus (salvestamine, taastamine)

Jõudlus:

- peaks võimaldada töödelda vähemalt wifi tugijaama liiklust (11b puhul ~4.5Mbit/s, 11a/g umbes 20Mbit/s, 11n kuni 130Mbit/s).
- Kui ruuter annab ühenduse mitmele wifi baasjaamale, peaks ruuter võimaldama töödelda vähemalt 50% kõigi wifi baasjaamade ühenduskiiruste summast.

### 7.5.3. Keskseade

Ühenduvus:

suuremaks turvalisuseks vajalik etherneti taseme ühenduvus (L2) WiFi tugijaamadega, selleks on vajalik VPN seade või moodul,

- DHCP server

Jõudlus:

- vähemalt 30% kõigi wifi AP-de läbilaskvusest

Haldus:

- SSH
- SNMP
- Syslog
- NTP
- mõistlik konfiguratsiooni haldus (salvestamine, taastamine).
- Keskseadmes peab sisalduma Syslog server,
- võrgu monitooringu server ning koormuse statistika server (näiteks SNMP abil)

Üldised nõuded:

- WiFi avalehe server (Captive portal tüüpi lahendus, HTTP, HTTPS), võimalus delegeerida avalehe autoriseerimine välisele serverile (üle HTTP/HTTPS vahendite)
- RADIUS serveri kasutamise võimalus, ID kaardi kasutamise võimalus autoriseerimisvahendina.
- Teenuse kvaliteedi tagamise (sh kiiruse piiramine) võimalus
- reeglite määramine kasutajate ja kasutajagruppide kohta
- ülevaade kasutajatest (st hetkeinfo) ja koormusest.

Märkused:
* - Täiendavad funktsioonid, mille omamine pole hädavajalik saavutamaks minimaalset kuid hästi ühilduvat süsteemi.
** - Funktsioonid, mille tuge võib oodata lähitulevikus ning mille omamine on lisaväärtuseks teenusele.

# 8. Leviala leitavus ja visuaalne tähistamine

WiFi uks peab märkima kes pakub teenust kellele ja mis tingimustel.
Ettevõtte või KOV  logo peab viitama tema portaali ja kasutaja peab nõustuma teenuslepinguga.

Mööduja tarvis tuleb tõmbekeskusesse lisada eesti/ inglise keelne WiFi teenuse tähis, pildil. Olemasolevad tähised on kasutusel Kadriorus, Toompeal ja muudel objektidel.

# 9. WiFi kasutuslepingu eelnõu

Palun lugege käesolev leping hoolikalt läbi enne meie traadita interneti teenuse kasutamist!

Tere tulemast _____ (firma, omavalitsus) traadita interneti levialasse (Teenus).

Käesoleva lepingu (Leping) tingimused reguleerivad Teie (Kasutaja) ja _____ nimi, reg kood, registri nimi, teenuse osutaja aadress, kontaktandmed (sh elektronposti aadress) (Valdaja) vahelist suhet järgmiselt.

Teenusele juurdepääsu taotlemisel nõustub Kasutaja Lepingus märgitud tingimustega ja peab Lepingut endale siduvaks ning kinnitab, et on nõus Teenust kasutama kooskõlas käesoleva Lepingu tingimustega.

I Kasutustingimustega nõustumine

Vajutades "Nõustun" nupule teenusega liitumise lehel, kinnitate, et olete käesoleva lepingu tingimused läbi lugenud, neist aru saanud ning nõustute nendega.
Kui Te ei nõustu käesoleva Lepingu tingimustega, siis ei ole Teil Teenuse kasutamise õigust. Teenusega liitumise lehel „Nõustun“ nupule vajutamine on samaväärne lepingu allkirjastamisega. Käesoleva leping jõustub „Nõustun“ nupule vajutamise kuupäeval.

II Teenuse tasu

Teenust osutatakse tasuta infoühiskonna teenusena, teenuse Kasutaja otsesel taotlusel.

III Jälgimiskohustuse puudumine

Teenuse Valdajal ei ole kohustust jälgida teavet, mida ta vaid edastab või millele juurdepääsu pakub, mida ta edastamise eesmärgil ajutiselt vahemällu salvestab või teenuse Kasutaja jaoks talletab, samuti ei ole tal kohustust otsida ebaseaduslikku tegevust näitavaid fakte ja asjaolusid. Samas on Valdaja kohustatud tulenevalt „Infoühiskonna teenuse seadusest“ teavitama pädevaid ametiisikuid ebaseaduslikust tegevusest või pakutavast teabest.

IV Turvalisus

Traadita süsteemid, nagu Teenus, kasutavad raadiokanaleid hääl- ja andmeside edastamiseks kompleksvõrgus. Privaatsuse tagab VPN käivitamine kasutaja poolt. Valdaja ei vastuta Kasutaja ega muu isiku ees privaatsuse puudumise ega riivamise eest, mis võib esineda või mida võib kogeda Teenuse kasutamisel. Kasutaja tunnistab, et Teenus ei ole olemuselt turvaline ning traadita sidet on võimalik kinni püüda selleks ettenähtud seadmete ja tarkvaraga.

Lisaks tunnistab Kasutaja, et ta vastutab selliste ettevaatusabinõude tarvitusele võtmise ja selliste turvameetmete kasutamise eest, nagu on Kasutaja olukorras ja Teenuse otstarbel kõige sobivamad. Kasutaja nõustub ja võtab käesolevaga enda kanda kõik riskid (sealhulgas, kuid mitte ainult häkkerite, usside, troojalaste või viiruste poolt põhjustatud kahju riskid), mis tulenevad Teenuse kasutamisest Kasutaja poolt või on sellega seotud.

V Teenuse kasutamine

Teenus ei ole ette nähtud rentimiseks, müümiseks ega ärikasutuseks ja seda ei tohiks kasutada äriprotsessideks. Valdaja ei vastuta Teenuse kasutamisest tulenevalt mõju eest äritegevusele ega äritegevuse katkemise eest.

Kasutaja nõustub mitte kasutama ega üritama kasutada Teenust pettuslikul, ebaseaduslikul, ahistaval ega kuritarvitaval eesmärgil ja nii, et see kahjustab või toob kaasa riski Valdajale, tema äritegevusele, mainele, töötajatele, teistele Kasutajatele, seadmetele või kolmandatele isikutele.

Sobimatu kasutus hõlmab konkreetselt (kuid mitte ainult) järgmist:

1. Kohaliku omavalitsuse, riigi või EL õigusakti rikkumine;
2. sisu postitamine või edastamine, milleks Kasutajal ei ole postitamise või edastamise õigust;

3. sisu postitamine või edastamine, mis rikub kolmanda isiku huve, avalikkuse huve, füüsilise isiku privaatsust või muud õigust;
4. sisu postitamine või edastamine, mis on ebaseaduslik, ebaõige, jälituslik, ahistav, teotav, laimav, solvav, ülekohtune, ähvardav, ropp, vihale õhutav, kuritarvitav, kahjutekitav või muul viisil ebasoovitav, nagu Valdaja omal äranägemisel otsustab;
5. andmete püüdmine, kogumine või salvestamine kolmandate isikute kohta ilma nende teadmise või nõusolekuta;
6. Teenuse mitteavalikele aladele sisenemine, nendega manipuleerimine või nende kasutamine;
7. mis tahes süsteemi või võrgu haavatavuse uurimise, skannimise või testimise või turva- või autentimismeetmete rikkumise katse;
8. soovimata teadete, sealhulgas, kuid mitte ainult toodete või teenuste reklaamide, püramiidskeemide, spämmi, kettkirjade või rämpskirjade, saatmine või saatmise katse;
9. füüsilise või juriidilise isiku matkimine, valeavalduse tegemine või muul viisil

valetamine oma seoste koha füüsilise või juriidilise isikuga;

10. päiste võltsimine või muul viisil tuvastuselementidega manipuleerimine, et varjata Teenuse kaudu edastatava materjali päritolu;
11. materjali saatmine, mis sisaldab tarkvaraviirusi või muud nuhktarkvara, mille eesmärgiks on katkestada, hävitada või piirata arvuti tarkvara või riistvara või sideseadmete toimimist;
12. Teenuse või Teenusega ühendatud serverite või võrkude segamine või katkestamine

või Teenusega ühendatud võrkudega seotud nõuete, protseduuride, poliitikate või eeskirjade mittetäitmine;

13. Teenuse kasutamine suurte andmemahtude edastamiseks, eriti pidevalt suurte andmemahtude edastamiseks, veebiserveri, IRC-serveri või muu serveri hosting;
14. Teenuse kasutamine häälsisuga seotud teenusteks, sealhulgas, kuid mitte ainult jutuliinideks;
15. Automaatse meetodi kasutamine ühenduse katkemise vältimiseks mitteaktiivsuse tõttu või muul moel ühenduse säilitamiseks, kui seda aktiivselt ei kasutata;
16. Teenuse edasimüük.

Juhul kui Kasutaja rikub käesolevat aktsepteeritava kasutuse poliitikat, võib Valdaja astuda üht või mitut järgmist sammu või muid loetlemata samme Valdaja äranägemisel:

(1) anda välja hoiatusi;
(2) katkestada ajutiselt Kasutaja juurdepääs võrgule;
(3) lõpetada alaliselt Kasutaja juurdepääs võrgule; ja/või
(4) alustada kohtumenetlust rikkumiste keelamiseks ja/või rikkumistega tekitatud kahjudesissenõudmiseks, kui on.

## VI Juurdepääsu piirangud

Valdaja eesmärgiks ei ole lubada piiramatut juurdepääsu kogu internetile. Samuti ei ole
Valdaja kavatsuseks luua traditsiooniline või piiratud avalik foorum (st vaba kõnetool).
Seetõttu võib Valdaja selle tasuta Teenuse osutamisel piirata juurdepääsu teatud saitidele ja sideprotokollidele, mis leitakse olevat õelad ja ebasobivad, või lõpetada Kasutaja juurdepääsu sellele Teenusele, kui Kasutaja kasutab seda juurdepääsuks pornograafilistele, täiskasvanutele suunatud, viha õhutavatele või nuhkvara sisaldavatele materjalidele või veebisaitidele.

Kasutaja nõustub ja tunnistab, et antud Teenus pakub ainult piiratud juurdepääsu internetile.

Kasutaja nõustub loobuma igasugustest nõuetest, mis võivad tuleneda Valdaja otsusest
blokeerida juurdepääs pornograafilistele, täiskasvanutele suunatud, viha õhutavatele või nuhkvara sisaldavatele materjalidele või veebisaitidele selle Teenuse kaudu. Kasutaja nõustub samuti mitte kasutama seda Teenust mis tahes lubamatul viisil autoriõigustega kaitstud materjali allalaadimiseks, olenemata sellest, kas see on audio, video, foto, teksti või muul kujul, või pornograafilise, täiskasvanutele suunatud, viha õhutava või nuhkvara sisaldava materjali allalaadimiseks, olenemata sellest, kas see on audio, video, foto, teksti või muul kujul.

## VII Probleemidest teatamine ja kaebused

Kui Kasutaja kogeb Teenusele juurdepääsul või kasutamisel probleemi, tuleb probleemist teatada, helistades WiFi uksel märgitud telefoninumbril või saates e-kirja

probleemi kirjeldusega aadressil info@wifi.ee 2 ööpäeva jooksul, alates probleemi märkamisest.

.

VIII Vastutuse piirang

Valdaja ei kontrolli Internetis olevaid materjale, infot ega teenuseid. Internet sisaldab redigeerimata materjale, millest mõned võivad olla Kasutajale solvavad või seksuaalse sisuga, mille eest Valdaja ei vastuta. Kasutaja võtab endale täieliku vastutuse Teenuse ja Interneti kasutamise eest ja sellega seotud riskid ning vastutab teenuste, toodete ja informatsiooni täpsuse, terviklikkuse ja kasulikkuse eest.

IX Garantiidest loobumine

Teenuse osutamine toimub põhimõttel „Nagu on“ ja „Nagu on kättesaadav“. Valdaja ei garanteeri, et Teenused on katkestuseta, vigadeta või vabad viirustest või muudest kahju tekitavatest teguritest. Kasutaja loobub eeldatavatest garantiidest, sealhulgas ka omandi mitterikkumise, kasulikkuse või konkreetseks eesmärgiks sobivuse osas, mis puudutab Valdaja või Interneti kaudu pakutavaid kaupu, informatsiooni või teenust. Kasutaja tunnistab eespool nimetatud riskide esinemist ning võtab traadita sidele omased turva-, privaatsus- ja konfidentsiaalsuse riskid enda kanda. Valdaja ja tema töötajad ei vastuta kahjude ega kulude eest, mis tulenevad otseselt või kaudselt Kasutaja poolt Teenuse või Interneti kasutamisest, sealhulgas kaudsete, juhuslike, näidis-, mitmekordsete, erakorraliste, trahvi- ega tulenevate kahjude eest. Valdaja ega tema esindaja poolt antud nõuanded ega informatsioon ei moodusta garantiid.Valdaja ei anna ühtki selgesõnalist garantiid.

X Lõpetamine

Valdaja võib ilma etteteatamata lõpetada käesoleva Lepingu või Kasutaja juurdepääsu Teenusele mis tahes põhjusel, sealhulgas, kuid mitte ainult juhul, kui Valdaja usub omal
äranägemisel, et Kasutaja on Lepingut rikkunud.

XI Kahjude hüvitamise tagatis

Kasutaja nõustub kaitsma Valdajat, hüvitama talle ja hoidma ta puutumatuna kõigist nõuetest, nõudmistest, kohtuasjadest, kohustustest, kuludest või kahjudest, mis tulenevad Kasutaja poolt Teenuse kasutamisest või Kasutaja poolt käesoleva Lepingu rikkumisest.

XII Muudatused

Valdaja võib omal äranägemisel muuta käesoleva Lepingu tingimusi. Need muudatused on siduvad ja kehtivad alates postitamise kuupäevast. Kasutaja nõustub vaatama tingimused üle enne igat Teenuse kasutamist, et hoida end muudatustega kursis. Teenuse kasutamise jätkamisega pärast selliseid postitusi nõustub Kasutaja aktsepteerima kõik sellised muudatused ja nendega nõustuma.

XIII Vaidlused

Küsimused, mis tekitavad erimeelsusi, püüavad Kasutaja ja Valdaja selgitada läbirääkimiste teel. Juhul kui lahendusteni ei jõuta, lahendatakse vaidlusalused küsimused Tartu maakohtu Jõgeva kohtumajas. Lisaks nõustub Kasutaja, kui seadusega ei ole keelatud, et käesoleva Lepingu või Teenusega seotud vaidluse, nõude või erimeelsuse peab Kasutaja esitama kuue (6) kuu jooksul alates kuupäevast, mil Kasutajal tekib õigus sellist nõuet esitada.

XIV Lepingu jagatavus

Lepingu ühe või mõne osa tühisus ei too kaasa teiste osade tühisust, kui leping on osadeks jagatav ja võib eeldada, et Kasutaja või Valdaja oleks lepinguga nõustunud ka tühise osata.