Tallinna Ülikool

Informaatika Instituut

Pjotr Savitski

OpenID põhine autentimine veebirakendustes Meenutusteportaali näitel

Magistritöö

Juhendaja: Mart Laanpere

Autor:…….…… “……“ …..…….2008

Juhendaja:…….…… “…… “ …..…….2008

Instituudi direktor: ……..……... “…… “ …..…….2008

Tallinn 2008

Sisukord

Sissejuhatus

Seoses juba pikka aega käiva Interneti ülikiire arenguga ja uute ning kasulikke ideede juurutamisega erinevatesse veebirakendustesse on selle kasutusvaldkond pidevalt laienemas. Viimastel aastatel on tekkinud palju sotsiaalse tarkvara põhimõtetel ülesehitatud veebirakendusi, mis on muutumas aina populaarsemaks Interneti kasutajate seas. Erinevate kasulikke veebiteenuste hulk on pidevalt kasvamas, samas kasvavad ka olemasolevate rakenduste poolt pakutavad võimalused. Kuid tuleb tõdeda, et hetkel ei saa üks Interneti aktiivne kasutaja piirduda ainult ühe hästi suure ja paljude võimalustega veebiteenuse kasutamisega. Peaaegu igal kasutajal on olemas kasutajakonto vähemalt mitmes erinevas veebirakenduses, mida ta kasutab kas isiklikel otstarvetel või töö juures.

See aga võib tekitada probleemi – kasutajal tekib palju kasutajakontosid erinevates veebikeskkondades. Igas keskkonnas on oma kasutajanimi ja salasõna. Neid kõiki meeles pidada on kindlasti raske ja tülikas. On olemas ka veel üks võimalus, mida mõned inimesed kindlasti kasutavad – proovida kasutada kõikjal ühte ja sama kasutajanime ja salasõna. Sellise lähenemise puhul on aga tegemist suure turvariskiga, kuna mõni rakendus ei pruugi piisavalt turvaline olla.

Mõnede rakenduste puhul kasutatakse ühekordse sisselogimise süsteemi (Single Sign-On või SSO), mis annab võimaluse sisestada oma kasutajatunnust ning salasõna ainult ühe korra. Pärast seda saab kasutada mitut erinevat rakendust konkreetse seanssi jooksul ilma selleta, et kasutajal oleks vaja veel kord kuskile sisse logida. Üheks näiteks võib olla Google, kes rakendas oma süsteemi juba mõnda aega tagasi. Kõik selle firma poolt pakutavad veebiteenused võivad kasutada ühist kasutaja autentimissüsteemi, mis on väga mugav ja kasulik. Aga kas sellised süsteemid saavad aidata siis, kui on vaja minna teise teenusepakkuja veebirakenduse juurde?

Üks võimalik lahendus sellele probleemile on juba olemas. Selleks on OpenID avatud, tasuta, detsentraliseeritud, vaba kasutaja-keskne digitaalse identiteedi raamistik.

Käesoleva magistritöö uurimisprobleemiks on: millised on OpenID põhise autentimise eelised ja puudused ja kuidas seda rakendada konkreetse veebilahenduse kontekstis?

Uurimuse eesmärgiks on: kaardistada OpenID põhise autentimise eelised ja puudused võrreldes alternatiividega ja töötada välja toimiv rakendus Meenutusteportaali jaoks.

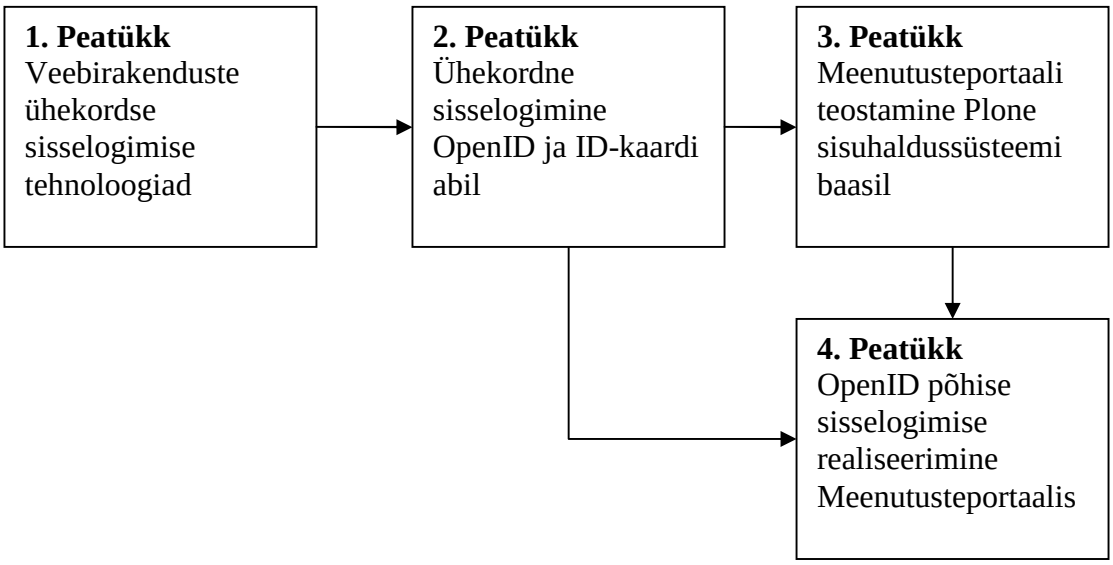
Töö kirjutamisel lähtub autor järgmistest uurimisküsimustest:

- Mille poolest erineb OpenID alternatiividest?
- Mis on OpenID eelised ja puudused?
- Kas olemasolev OpenID lahendus Plone sisuhaldussüsteemi jaoks vastab spetsifikatsioonidele?
- Kuidas realiseerida ID-kaardi põhist autentimist üle OpenID?

Eesmärgi saavutamiseks püstitab autor järgmised ülesanded:

- Erialakirjanduse ülevaade: ühekordset sisselogimist võimaldavad autentimisviisid, OpenID, ID-kaart
- Plone sisuhaldussüsteemi OpenID lahenduse uurimine
- OpenID autentimise realiseerimine Meenutusteportaalis

Magistritöö struktuur on esitatud joonisel 1, kus on näidatud peatükkide ülesehitus ja omavahelised seosed.



Joonis 1. Magistritöö struktuur

Magistritöö esimeses peatükis antakse ülevaadet ühekordse sisselogimise põhimõtetest ning selle võimaldavate autentimisviiside tööpõhimõtetest ja spetsifikatsioonidest.

Teises peatükis antakse ülevaadet OpenID protokolli põhimõtetest ning spetsifikatsioonidest. Räägitakse Eestis laialt kasutatud ID-kaardist, uuest OpenID.ee Identiteedi pakkujast ja Sertifitseerimiskeskusest.

Kolmandas peatükis antakse ülevaadet Meenutusteportaali projektist ja selle Plone põhisest veebirakendusest.

Neljandas peatükis uuritakse Plone jaoks olemasolevat OpenID lahendust ning selle vastavust spetsifikatsioonidele ja Meenutusteportaali vajadustele. Kaardistatakse Meenutusteportaali vajadusi kasutajate autentimise suhtes ning luuakse OpenID lahendus, mis vastab Meenutusteportaali poolt püstitatud kriteeriumitele.

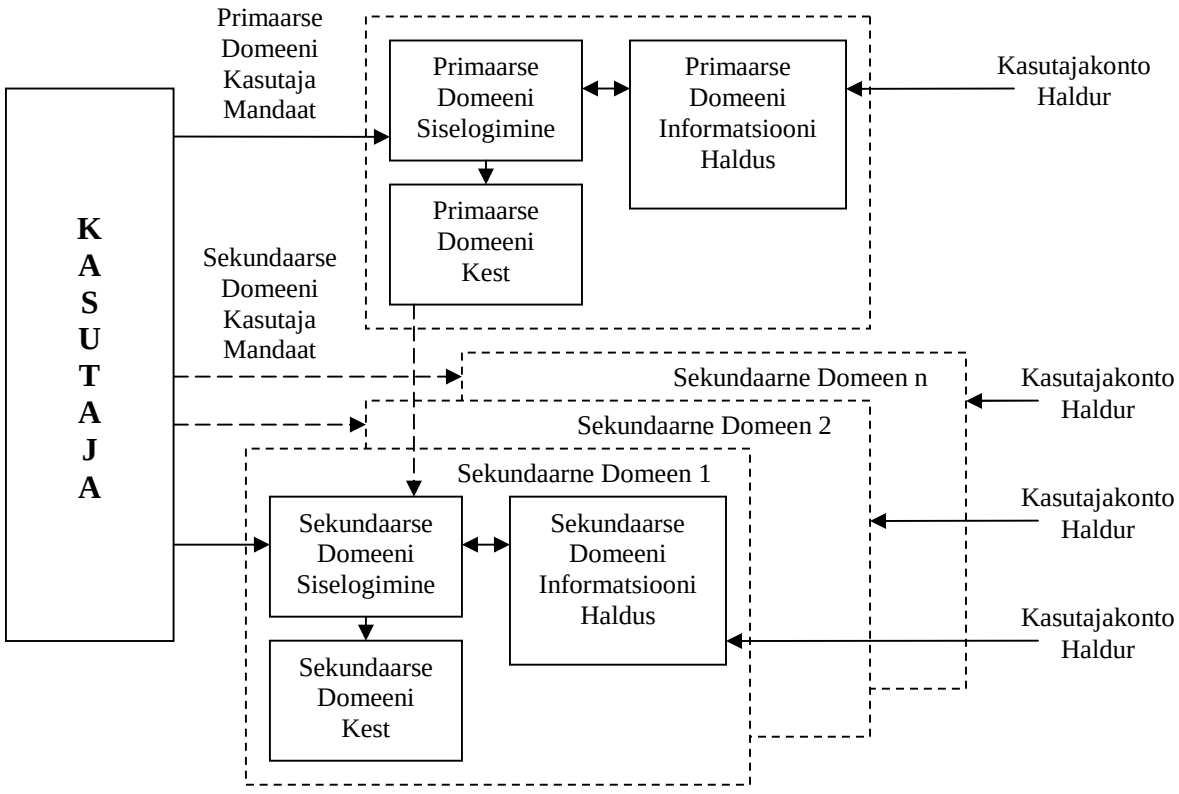
Tuginedes uuringu tulemustele ning OpenID lahenduse realiseerimise käigus saadud kogemusele kirjutatakse ka üldist kokkuvõtet OpenID tehnoloogia rakendatavuse kohta.

Magistritöö tulemusena valmib Meenutusteportaali vajadusele vastav OpenID tehnoloogial põhinev kasutajate autentimise rakendus.

1. Veebirakenduste ühekordse sisselogimise tehnoloogiad

1.1. Ühekordne Sisselogimine ehk Single Sign-On

IT süsteemid hakkavad aina rohkem toetama ettevõte äriprotsessi. Selle tagajärjel suureneb ka protsessi edukaks toimimiseks vajalikke süsteemide keerukustase, mis kindlasti teeb kasutajatele ja süsteemi administraatoritele nendega hakkama saamist palju keerukamaks. Tavaliselt peavad kasutajad sisenema mitmesse süsteemi, igas süsteemis võib olla kasutusel teistsugune autentimise informatsioon. Süsteemi administraatorid peavad tegelema kasutajakontode haldamisega igas ühes neist süsteemidest, ning tagama olemasoleva turvalisuspoliitika kasutamist igal pool terve süsteemi tervikluse säilitamiseks. Selline pärand-lähenemine, mis nõuab kasutajalt mitmesse süsteemi sisse logimist on näidatud Joonisel 2.



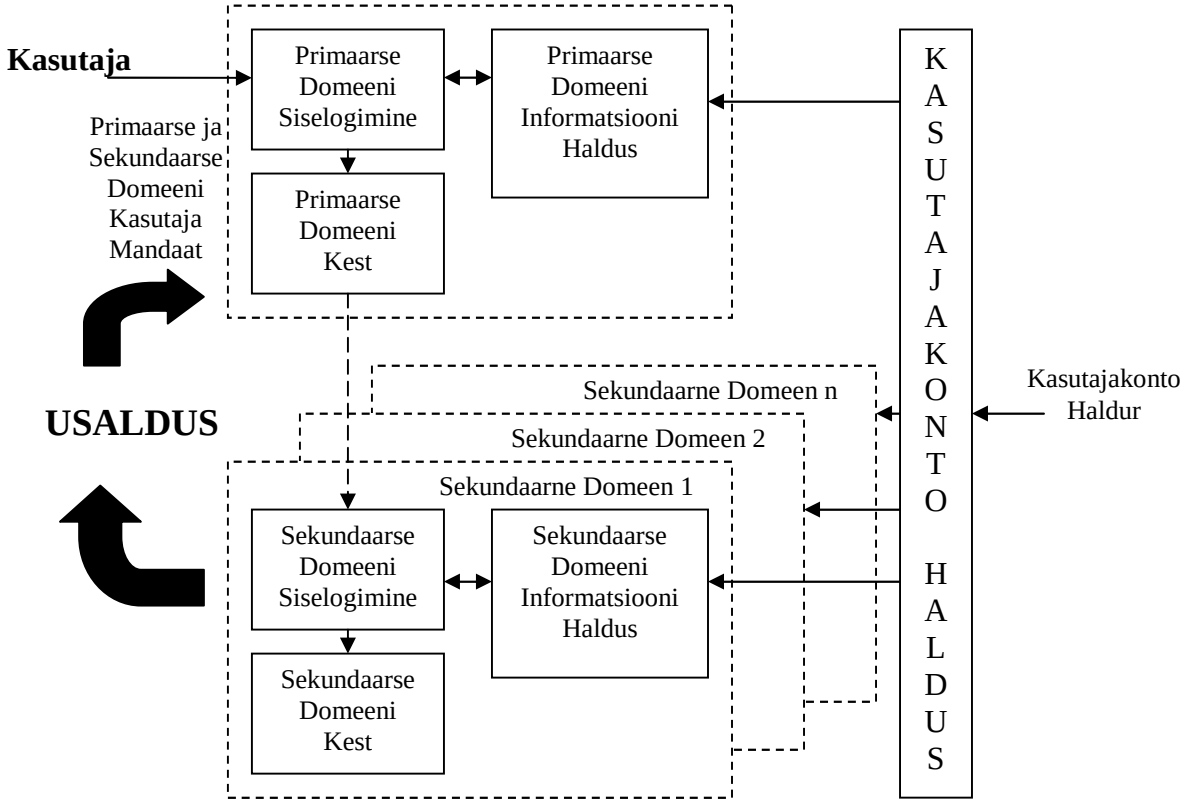
Joonis 2. Pärand-lähenemine Kasutaja Sisselogimiseks Mitmesse Süsteemi (The Open Group, Introduction To Single Sing-On)

Ajalooliselt koosnes hajus arhitektuuriga süsteem komponentidest, mis tegutsevad nagu sõltumatud turvalisusdomeenid. Need komponendid sisaldavad individuaalseid platvorme koos seotud opsüsteemide ja rakendustega.

Kõik komponendid käituvad nagu iseseisvad domeenid selles mõttes, et lõppkasutaja peab ennast identifitseerima ja autentima iga kasutatava domeeni jaoks. Selline stsenaarium on näidatud Joonisel 2. Esiteks peab kasutaja looma sessiooni Primaarse Domeeniga. Selle jaoks on kasutajal vaja Primaarse Domeeni sisenemiseks saatma domeenis kehtivat isikutunnistust, selleks võivad olla kasutajatunnus ja salasõna. Üldiselt on Primaarse Domeeni sessiooniks tööjaamas täidetav ja kasutajat esindav opsüsteemi sessiooni kest (näiteks: protsessi omadused, keskkonna muutujad ja kodukaust). Selle primaarse domeeni abil saab kasutaja käivitada teiste domeenide teenuseid, nagu platvormid ja rakendused.

Sekundaarse domeeni teenuste käivitamiseks peab kasutaja läbima vastava domeeni autentimise protsessi. Selleks on vaja saata veel ühte, nüüd aga teises domeenis kehtivat isikutunnistust. Iga kasutusele võetava sekundaarse domeeni jaoks on kasutajal vaja ennast uuest autentida. Tavaliselt eksisteerib kasutajat esindav komponent ka sekundaarses süsteemis. Haldamisperspektiivist nõuab taoline lähenemine iga olemasoleva domeeni eraldiseisvat haldamist ja liidest, mis võimaldaks mitmete kasutajakontode haldamist. Nii kasutatavus, kui ka turvalisus nõuavad, et erinevates domeenides kasutusel olevaid sisselogimis- ning kasutajakonto haldamisfunktsioone oleks vaja korrastada ja võimalusel integreerida. Kõike seda võimaldav teenus annab ettevõttele kulu vähendamise võimalusi:

- vähendades kasutajate poolset ajakulu erinevatesse domeenidesse sisenemisel, kaasaarvatud taoliste operatsioonide ebaõnnestumise võimaluse vähendamist.
- parem turvalisus, kuna kasutajal ei ole vaja mälus hoida palju erinevaid kasutajatunnuseid ja salasõnu.
- süsteemi administraatorid saavad kiiremini lisada ja kustutada kasutajaid või muuta nende ligipääsuõigusi.
- parem turvalisus, kuna administraatorid saavad paremini säilitada süsteemi terviklust, sealhulgas ühtselt peatada või eemaldada mingi kasutaja juurdepääsu kõigile süsteemi ressurssidele.



Joonis 3. Kasutaja Ühekordne Sisselogimine Mitmesse Süsteemi (The Open Group, Introduction To Single Sing-On)

Selline teenus sai nimeks **Ühekordne Sisselogimine (Single Sign-On, SSO). Ühekordne Sisselogimine** on kasutaja autentimise protsess, mille abil kasutaja saab, sisestades ühe kasutajanime ja parooli, ligipääsu mitmele rakendusele. Sellisel viisil saab kasutaja ligipääsu nendele rakendustele, kuhu on kasutajal õigus siseneda. Konkreetse sessiooni jooksul ei pea kasutaja enam rakenduste vahetamisel oma identiteedi tõestama.

Sellist lähenemist demonstreerib Joonis 3. Ühekordset Sisselogimist kasutatava lähenemise juures esmakordsel sisselogimisel sisestatakse ka kogu edasiseks teistes domeenides autentimiseks vajalikku informatsiooni. Primaarses domeenis kasutaja poolt sisestatud informatsioon on kasutatud Ühekordse Sisselogimisteenuse poolt selleks, et tegeleda kasutaja poolt kasutusele võetavates sekundaarsetes domeenides autentimisega.

Primaarse domeeni sisenemisel kasutaja poolt antud informatsiooni saab teiste sekundaarsete domeenidega autentimiseks mitmel viisil kasutada:

- Otse, kasutaja poolt antud informatsiooni antakse sekundaarsele domeenile uue sisselogimise osana.

- Kaudselt, kasutaja poolt antud informatsiooni kasutatakse ülejäänud autentimiseks vajalikku informatsiooni kätte saamiseks, mis asub ühekordse sisselogimisteenuse käes. Kättesaadud informatsiooni kasutatakse sekundaarse domeeni sisselogimise aluseks.
- Viivitamatult, sekundaarse domeeniga sessiooni loomiseks esmase sessiooni loomise osana. Eeldatakse et iga rakenduse kliendid on automaatselt aktiviseeritud ja side on loodud juba esmase sisenemise ajal.
- Ajutiselt salvestatud või vahemällu paigutatud ning kasutatud teise domeeni teenuse kasutamise päringu tegemisel kasutaja poolt.

Ühekordse Sisselogimise mudeli tähtsateks aspektideks on:

- sekundaarsed domeenid peaksid usaldama primaarset selles, et ta:
    - õieti kinnitab isiksust ja saadab autentimise isikutunnistust kasutaja jaoks
    - kaitsta autentimise isikutunnust kasutaja isiksuse kindlaks tegemiseks sekundaarses domeenis
- autentimise isikutunnistus peab olema kaitstud primaarse ja sekundaarse domeenide vahel edastamisel võimalikke rünnakute eest.

Ühekordse sisselogimise mudelil on mitu eelist võrreldes pärand-lähenemisega. Kuid selle heal tasemel teostamiseks on vaja standarte ning tehnoloogiaid, mis reglementeeriksid kogu hajutatud arhitektuuriga süsteemi toimimist. (The Open Group, Introduction To Single Sing-On)

1.2. Lihtsustatud Kataloogisirvimise Protokoll

Mis on kataloog ja kataloogiteenus

Kataloog on spetsiaalne andmebaas, mis on optimeeritud lugemiseks, sirvimiseks ja otsimiseks. Kataloogid omavad suunda sisaldama kirjeldavat, omaduse-põhist informatsiooni ja toetama keerulisi filtreerimise võimalusi. Tavaliselt kataloogid ei toeta keerulisi toiminguid või andmete esialgsele kujule taastamisvõimalusi, mida leidub keerulisi massilisi uuendusi toetavates andmebaaside haldamissüsteemides. Kataloogide uuendused on tavaliselt lihtsad **kõik-või-mitte-midagi** muudatused, kui need on üldse lubatud. Kataloogid on häälestatud andma kiiret vastust massilistele otsingu päringutele. Neil võib olla võime laialt dubleerida informatsiooni suurema kättesaadavuse ja töökindluse saavutamiseks, samal ajal vähendades vastuse andmiseks vajalikku aega. Kataloogi dubleerimise käigus võivad tekkida ajutised ebakõlad dublikaatide vahel. See on normaalne juhul, kui nad lõpuks sünkroniseeritud saavad.

Kataloogi teenuse pakkumiseks on mitu erinevat viisi. Erinevad meetodid võimaldavad hoida kataloogis erinevat tüüpi informatsiooni, püstitavad erinevaid nõudeid olemasoleva informatsioonile viitamise, pärimise, uuendamise, ligipääsu volitamise ja muude operatsioonide kohta. Mõned kataloogid on **lokaalsed**, võimaldades kasutada teenust ainult piiratud kontekstis. Teised kataloogid on **globaalsed**, võimaldades kasutada teenust palju laiemas kontekstis (näiteks: Internet). Globaalsed teenused on tavaliselt jaotatud mitme masina/serveri vahel, kõik need masinad teevad koostööd teenuse pakkumiseks. Tüüpiliselt globaalne teenus defineerib **nimeruumi**, mis annab täpselt samasuguse andmete vaade, kus tahes klient ka poleks andmete suhtes. Üheks globaalselt levinud kataloogiteenuseks on **Domeeninimede Süsteem (Internet Domain Name System, DNS)**, mis tõlgib kasutajatele mugavad domeeninimed IP aadressideks. (OpenLDAP Project, Introduction to OpenLDAP Directory Services)

LDAP

Lihtsustatud Kataloogisirvimise Protokolli (Lightweight Directory Access Protocol, LDAP) loomisel võeti aluseks **International Telekommunikatsioonide liidu (Telecommunication Union, ITU)** poolt välja töötatud X.500 sarja soovitusi kataloogide kohta. Seoses sellega omavad X.500 ja LDAP kataloogid väga sarnast struktuuri. LDAP kataloogid on sageli ka X.500 omadega ühilduvad, on palju nende kataloogide koostöö näiteid. Üks LDAP tehnoloogia rajajaid oli **Michigani Ülikool (University of Michigan)**, nende veebis saab ka praegu leida tasuta näiteid, dokumentatsiooni, lähtekoodi ja teisi ressursse.

LDAP on defineeritud avaldatud Interneti standardite komplekti kujul, tavaliselt viidatakse nende **Kommentaarinõue (Request For Comment, RFC)** numbrile avaldatud IETF lehel aadressil http://www.ietf.org. **Internetiehituse töörühm (Internet Engineering Task Force, IETF)** aitab hallata ranget eelnõu protsessi, mille käigus ideedest koosnevate mustandite arutamise protsessis saadakse avaldamiseks valmis Interneti standard. Viimane LDAP versioon 3 (v3) on defineeritud üheksa RFC dokumendi abil. RFC 2251 kuni 2256 annavad põhilisi detaile, hiljem neile järgnesid RFC 2829 ja 2830. Viimaks lasti välja RFC 3377, kus seotakse kõik eelmised kokku ametlikuks LDAP v3 standardiks. (Arkills, 2003, lk 17 - 18)

Järgnevalt vaadeldakse nelja põhilist komponenti:

- **Nimeruum** (namespace)
- **Kliendi operatsioonid** (client operations)
- **Skeem** (schema)
- **Haldus** (management) (Arkills, 2003, lk 19)

Nimeruum

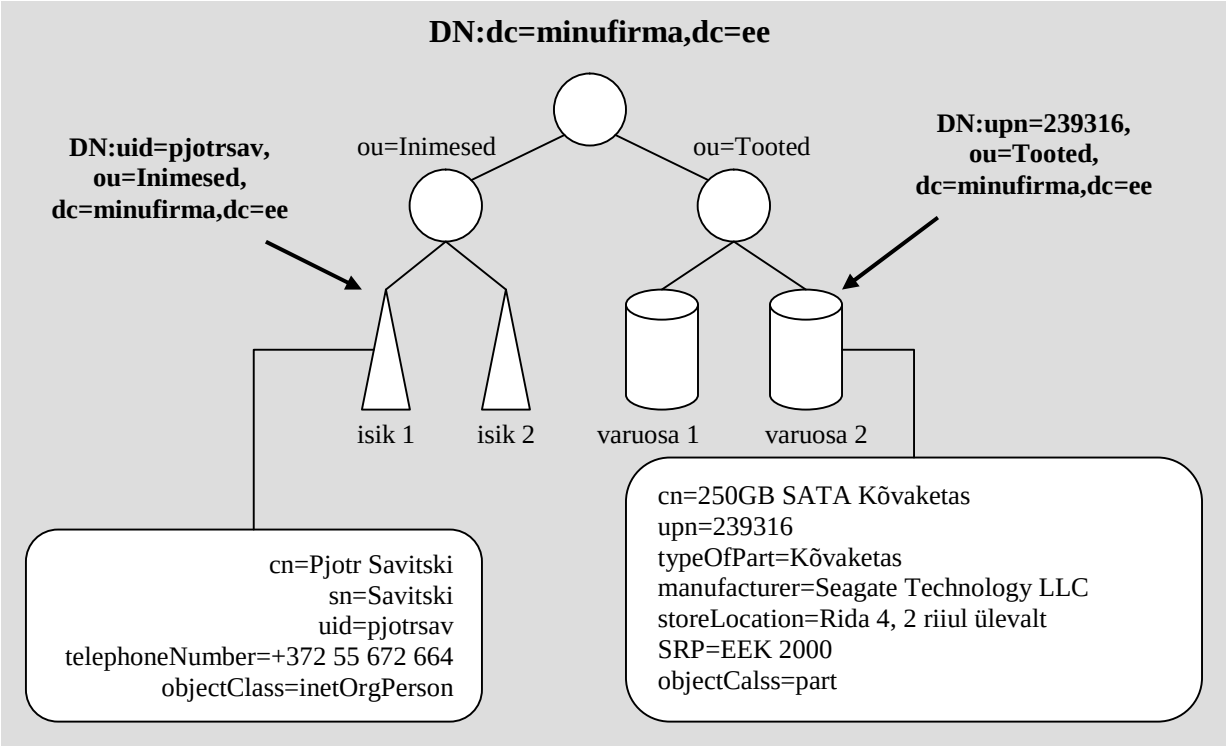
Iga kataloog vajab nimeruumi. Eelkõige viitab nimeruum sellele kuidas sissekandeid nimetatakse. Samas nimeruum võib vihjata kataloogis olevate sissekannete organisatoorsele struktuurile. Juhuslikult, saab mõistet **nimeruum** kasutada ka üldises tähenduses viidates kõigile teatud konteineris asuvatele objektidele.

Üldiselt, LDAP nimeruum on kataloogis asuvatele objektidele viitamiseks kasutatav süsteem. Igal objektil peaks olema nimi, mida kasutatakse kahel eesmärgil. Esiteks, annab see võimalust objektile viidata. Teiseks, see annab võimalust organiseerida objekte loogilisesse struktuuri. Nimeruumist arusaamine on kataloogist arusaamise võtmeks.

Iga kataloogis olev sissekanne vajab nime selleks, et sellele saaks viidata. Need nimed peaksid olema LDAP kataloogis unikaalsed, et oleks võimalik märgistada teatud sissekannet. Igale sissekandele unikaalse nime omastamise asemel läheb nimeruum ühe sammu võrra edasi ja määrab kuhu kohta kataloogi organisatoorses struktuuris iga sissekanne kuulub. Teades sissekande nime saab eeldada kus kohas kataloogi struktuuris see paikneb.

Nimeruumi hierarhilise struktuuri tõttu saab haldamise juhtimist delegeerida mitmes hierarhilise struktuuri punktis. Mis kindlustab mugavaid vahendeid halduse ühisdelegeerimiseks. See on üks LDAP tähtsaid eeliseid andmebaaside üle. Samas on see ka üheks põhilisi faktoreid kataloogis andmete organiseerimise viisi valimiseks.

Mitu kataloogi saavad jagada ühist nimeruumi, milleks on Interneti standard **Domeeninimede Süsteem (Domain Name System, DNS)**. Üheks DNS kasutamise näiteks on e-posti aadresside struktuur (keegi@nimeruum.com). DNS tagab nimede unikaalsuse. LDAP ja DNS nimeruumide hierarhiline struktuur annab võimaluse suurte globaalsete kataloogide realiseerimiseks. (Arkills, 2003, lk 19 - 21)



Joonis 4. DSN nimeruumiga integreeritud LDAP kataloog (Arkills, 2003, lk 24)

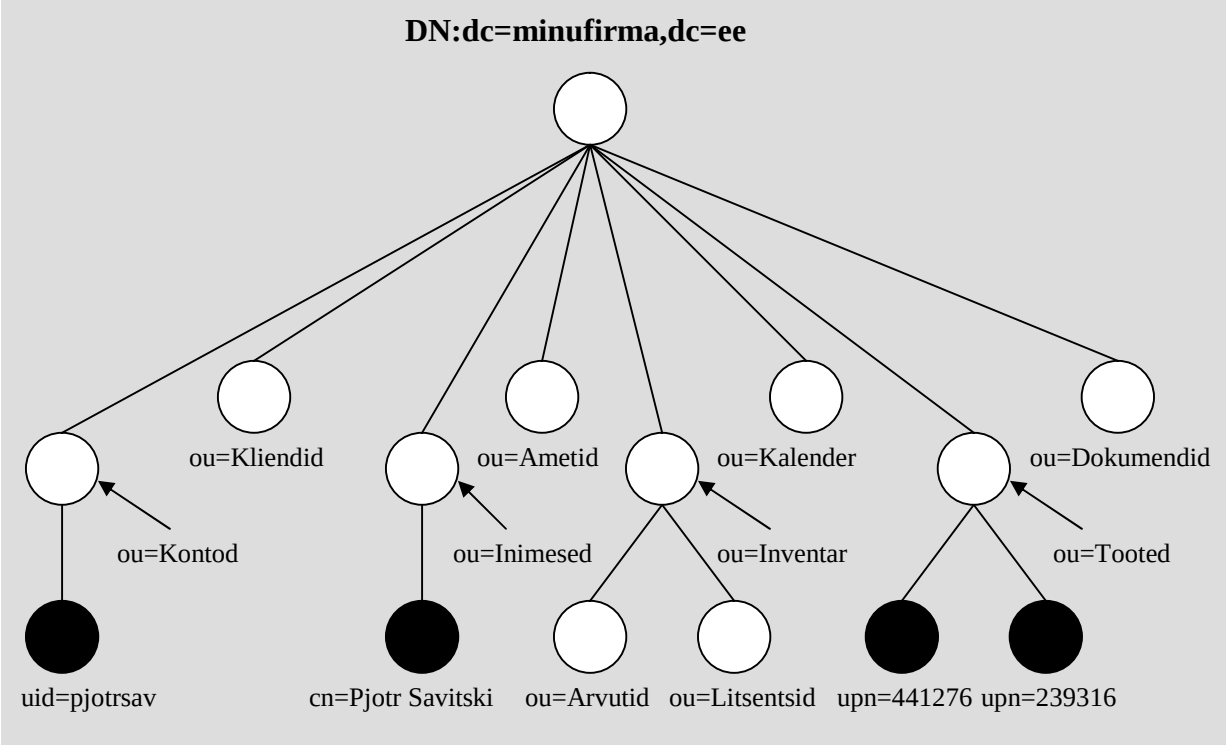
Joonisel 4 on näidatud lihtne kataloog. Kataloogi juure nimi on kataloogi põhja või aluse **eraldusnimi (distinguished name, DN)**. Kataloogi juureks ei pea ilmtingimata olema kataloogi sissekanne. Tavaliselt serveri põhi DN on samasugune nagu serveri DNS nimi ja kasutab **domeeni komponente (dc)** tunnuseid DNS tsoonide esitamiseks. Samas, serveri põhi DN ei pea ühilduma serveri DNS nimega, sellega abil on saavutatud mitut serverit kasutava kataloogi paindlikkus. Nimeruumi abil hajus arhitektuuriga LDAP kataloogi loomine on üks eeliseid andmebaasi ees.

Igal sissekannel on olemas unikaalne nimi, mida kutsutakse eraldusnimeks. Lisaks sellele on igal sissekandel ka lokaalne mini vahetu konteineri suhtes, seda kutsutakse **suhteliseks eraldusnimeks (relative distinguished name, RDN)**. RDN on unikaalne selles konteineris olevate sissekannete seas. Iga sissekande eraldusnime pannakse kokku sissekande suhtelisest eraldusnimest ja kõigi kataloogi juureni olevate konteinerite suhtelistest eraldusnimedest (neid kõiki eraldatakse komaga). Ei DN, ega ka RDN ei ole sissekande omadused/atribuudid, vaid RDN koosneb ühest või enamast sissekande omadusest. Suhteline eraldusnimi või RDN on omaduse tüübist ja väärtusest koosnev paar. RDN ei pea olema unikaalne terve kataloogi ulatuses, vaid konkreetse konteineri ulatuses.

Kasutatud eraldusnime asemel **uid=pjotrsav,ou=Inimesed,dc=minufirma,dc=ee** võiks kasutada ka midagi muud. Näiteks: **cn=Pjotr Savitski,ou=Inimesed,dc=minufirma,dc=ee**. Tuleb panna tähele, et RDN komponendi sees on mõlemad atribuudi tüüp **cn** ja atribuudi väärtus **Pjotr Savitski**. Ainuüksi atribuudi väärtusest ei piisaks, kuna siis poleks teada mis atribuudi tüüpiga see seotud on. Kuna eesnimi ja perekonnanimi ei pruugi olla unikaalsed, siis on parem kasutada mingit unikaalset identifikaatorit (nagu kasutajanimi).

Joonisel 5 on näidatud lihtsa kataloogi nimeruumi skeem. Iga konteineri (valge ring) sees peaksid olema sissekanded (must ring) ja võimalikult ka teised konteinerid, mis veelgi rohkem täpsustaksid struktuuri. Näiteks: konteiner Inimesed võiks olla jagatud osakondade järgi. Joonisel 5 oleva diagrammi elementide paigutus võiks olla teistsugune, samas võiks ka selline lahendus esitatud nõudeid täita.

LDAP nimeruum annab mõningaid olulisi eeliseid. Esiteks, sellega kaasneb sissekandeid unikaalselt identifitseeriv mudel, mis on väga paindlik - rohkem kui üks nimi võib sobida. Teiseks, on nimeruum loomupäraselt hierarhiline. Mis võimaldab samanimelise atribuutidega sissekannete eksisteerimist erinevates konteinerites. Kolmandaks, tavaliselt kasutatakse nimeruumi koos DNS süsteemiga, mis võimaldab teiste tehnoloogiatega integreerimist ning teenuse aadressiteisendust igalt poolt. Neljandaks, nimeruumi abil saab kasutada mitmes serveris paikneva hajus arhitektuuriga kataloogi. (Arkills, 2003, lk 21 - 25)



Joonis 5. Kataloogi nimeruum (Arkills, 2003, lk 26)

Protokoll

LDAP tuumas on defineeritud komplekt operatsioone (kataloogi sirvimise protokolle), mida kasutatakse kataloogis salvestatud andmete käsitlemiseks.

Klient-Server Mudel

Protokollina kasutab LDAP sidevahendiks Interneti **TCP/IP protokollistiku (Transmission Control Protocol/Internet Protocol, Edastusohje Protokollistik Internetiprotokolli Peal, Internetiprotokollistik)**. LDAP kataloogiga ühenduse loomiseks on kliendil vaja avada TCP/IP sessiooni selle LDAP serveriga. LDAP minimiseerib sessiooni loomise kulusid, lubades sooritada mitu operatsiooni ühe kliendi sessiooni käigus. Lisaks, saab vähendada liiklust efektiivselt kasutades kompressiooni, kuna suurem osa kataloogis salvestatud andmetest on diskreetse tekstipõhise informatsiooni kujul. LDAP kasutab andmete kodeerimisel üleliigselt keerukat kodeeringut, mis on üle võetud X.500 standardist.

Kuna LDAP poolt määratud operatsioonide komplekt vastab üks ühele erinevate programmeerimiskeelte **standardsetele rakendusliidestele (Application Programming Interface, API)**, siis iga LDAP klient on võimeline suhtlema iga LDAP serveriga. (Arkills, 2003, lk 26)

Klient

LDAP kliendiks võib olla kas eraldiseisev tarkvara, kus kasutaja kirjutab nõuetele vastavat süntaksit, või integreeritud tarkvara, kus suurem osa toimingutest on automatiseeritud ja kasutajal ei ole vaja süntaksist midagi teada. Suurem osa veebisirvijatest toetab LDAP protokolli ja võivad olla täisfunktsionaalseteks LDAP serverite klientideks. Integreerimise paindlikkus on üks tähtsamaid põhjusi LDAP protokolli kasutamiseks paljude ettevõtete poolt.

LDAP on avatud standard, seega iga klient või rakendus saab suhelda iga LDAP serveriga, hoolimata kliendi või serveri opsüsteemist. LDAP on keeruka, mittehomogeense opsüsteemi keskkonnas palju lihtsamini rakendatav kui mingi teine tehnoloogia. (Arkills, 2003, lk 27)

Operatsioonid

LDAP võimaldab teostada kümme erinevat operatsiooni. Piiratud operatsioonide arv on väga tähtis, kuna see võimaldab luua lihtsamaid kataloogiga suhtlevaid klient-programme. Neid

operatsioone saab grupeerida kolmesse põhilise kategooriasse ühe erandiga, nagu näidatud Tabelis 1. (Arkills, 2003, lk 28)

Kategooria	**LDAP Operatsioonid**
Kliendi Sessiooni Operatsioonid	Sidumine, lahti sidumine ja hülgamine
Päringu ja Otsingu Operatsioonid	Otsing ja võrdlemine
Muutmisoperatsioonid	Lisamine, muutmine, RDN-muutmine ja kustutamine
Laiendatud	Laiendatud

Tabel 1. LDAP operatsioonid (Arkills, 2003, lk 28)

Laiendatud operatsioon on unikaalne ja on kohatäide spetsiifiliste kataloogide teostusteks vajalikku protokolli funktsionaalsuse laiendamiseks, aga mis ikkagi omavad selleks eeldefineeritud süntaksit.

Kliendi sessiooni operatsioonid aitavad reguleerida klient-server sessiooni konteksti kõikide edasiste LDAP operatsioonide päringute jaoks sellelt kliendilt. Sidumise ja lahti sidumise operatsioonid võimaldavad kliendil luua kataloogiga isiksust. Seda isiksust saab kataloog hiljem kasutada teiste operatsioonide sooritamise jaoks vajalikku volituse kindlaks tegemiseks, sellega saab reguleerida ligipääsu kataloogi informatsioonile. Hülgamise operatsioon võimaldab kliendil tühistada veel täitmata olev operatsiooni päring.

Päringu operatsioonid võimaldavad kliendile kataloogis informatsiooni otsimist. Otsing on kõige sagedamini kasutatav operatsioon, ning selle kasutamise oskus saab olema korduvalt väärtuslik. Otsingul on rohkem parameetreid kui mingil teisel operatsioonil. Kuid selline keerukus tasub ennast ära, sest annab kasutajale võimaluse määrama peenemaid päringuid kataloogis otsingu sooritamiseks. Võrdlemist kasutatakse sissekandega seonduva informatsiooni kindlaks tegemiseks (verifitseerimiseks). Klient saadab sissekande eeldatava sisu väärtust (väärtusi), server vastab kas võrdlemise protseduur õnnestus või mitte.

Muutmisoperatsioonid võimaldavad kliendil muuta kataloogis olevat informatsiooni. Mõnedes kataloogide eksemplarides vastavad operatsioonid võivad olla keelatud. Näiteks: avaliku kirjutuskaitstud (ainult lugemiseks mõeldud) kataloogi puhul. RND-muutmise operatsioon võimaldab kliendil sissekande nime muuta ja teisaldada sissekannet mingi muu konteineri sisse.

LDAP protokollil on veel kaks märkimisväärset omadust: suunamine ja Unicode UTF-8 tugi. Suunamine võimaldab LDAP serveril kliendi poolt nõutavate andmete leidmiseks suunata klienti teise LDAP serveri juurde. Selline funktsionaalsus võimaldab kataloogiserverite ja isegi eraldiseisvate kataloogide vahelist integreerimist ja koostööd. **Unikood (Unicode**) on spetsiifiline andmete esitamisviis, mille abil saab esitada ükskõik mis kirjakeelt. Unikoodi tugi võimaldab LDAP kasutatamist peaaegu iga keele kontekstis, tehes seda globaalseks lahenduseks. (Arkills, 2003, lk 29 - 30)

Skeem

Kataloogis võimalikke sissekannete liikide määratlemiseks kasutatakse skeemiks kutsutava reeglite komplekti. Kui mingit üksiku objektiklassi ei ole skeemis, siis ei saa selle objektiklassiga ka sissekannet luua. Uute objektiklasside või mittekohustuslikke omaduste lisamiseks olemasolevale objektiklassile tuleb skeemi laiendada. Edaspidi skeem määrab reegleid nagu: mis tüüpi väärtust saab omadusse paigutada, mis tehteid/operaatorid kehtivad nendele omadustele. Kataloog kasutab **operaatoreid** omaduse väärtuse ja teise väärtuse võrdlemiseks. Suurem kui, vähem kui ja võrdsus on harilikud andmete operaatorid. (Arkills, 2003, lk 30)

Skeemi kontrollimine

Iga uue sissekande lisamisel käivitub skeemi kontrollimise protsess. Juhul kui mingi andmete osa ei vasta esitatavatele kriteeriumitele, siis ebaõnnestub terve sissekande lisamine. Mõningad LDAP teostused võimaldavad skeemi kontrollimist välja lülitada, kuid seda ei tasuks teha. Sellisel juhul võivad kataloogis olevad andmed oma ühtlust kaotada. (Arkills, 2003, lk 31)

Vaikimisi skeem

Minimaalne LDAP standardi poolt nõutud skeemi objektide komplekt on defineeritud RFC 2252 ja 2256 poolt. LDAP standardi minimaalne skeem on suures osas tehtud X.500 standardi poolt defineeritud skeemi objektidest ning järgib X.500 skeemi põhireegleid. Sellepärast paljud LDAP produktid ongi X.500 omadega ühilduvad. Kataloogide loojad tegelevad selle minimaalse komplekti teostamisega. Suurem osa tarkvara loojatest leiavad, et taolisest minimaalsest komplektist ei piisa ja laiendavad skeemi vastavalt oma enda vajadustele. (Arkills, 2003, lk 31)

Skeemi laiendamine

Kuigi oma süntaksi tõttu on skeemi väga raske lugeda, on see samal ajal suure paindlikkuse allikaks. Skeemi laiendamisega saab teostada kõikvõimalikke andmetüüpide kaasamist. Lisaks sellele annab skeem võimaluse määratleda uusi kataloogiga ja andmetega töötamisviise.

LDAP avalikustab kataloogi skeemi selleks, et iga klient saaks välja selgitada mis definitsioone ja reegleid server kasutab. Skeemi avaldamise koha informatsioon on salvestatud igasse sissekandesse. Suurem osa kataloogidest omavad iga sissekande jaoks kehtiva skeemi, seega on skeemi avalikustamise koht kõikjal sama. Mõned LDAP serverid võimaldavad määrata kataloogi erinevatele osadele unikaalseid skeeme. (Arkills, 2003, lk 31)

Isik (person) klassi skeemi defineerimise näide:

```
person OBJECT-CLASS ::= {
   SUBCLASS OF { top }
   KIND abstract
   MUST CONTAIN { sn, | cn}
   MAY CONTAIN { userPassword | telephoneNumber |
      seeAlso | description }
   ID 2.5.6.6}
```

(Arkills, 2003, lk 32)

Haldus

LDAP kataloogide haldamise võimalus on väga tähtis, see peaks olema lihtne, varustatud integreerimist lihtsustavate vahenditega. Mingi ükski osa kataloogi haldusfunktsionaalsusest ei ole standardi poolt sätestatud. Näiteks: andmete salvestamise ja välja otsimise viisid (tavaliselt kasutatakse spetsiaalset andmebaasi). (Arkills, 2003, lk 32)

Hajus arhitektuuriga kataloog

Kataloogi rikkekindlus on esmatähtis, sest sageli see võib mängida organisatsiooni äriprotsessiga seonduvalt keskset rolli. Suurem osa kataloogitarkvara loojatest on rakendanud oma produktides mingit andmete kopeerimise võimalust selleks, et teatud andmeid saaks kopeerida mitmesse LDAP serverisse. Kopeerimise kasutamisel teostatav jaotus annab mitu eelist, nende seas on: koormuse jaotamine ja kaitse andmete kaotamise vastu. Kuigi kopeerimine ei ole ainus kataloogi jaotamise viis. Erinevad LDAP serverid võivad hoida kataloogi nimeruumi erinevaid osi, omades viiteid teistele LDAP serveritele. Nimeruumi saab jagada ükskõik mis moodi. (Arkills, 2003, lk 33)

Turvalisus

LDAP versioon 3 omab:

- Tugevat autentimise ja andmete kaitsmise teenust **Lihtsa Autentimise ja Turvalisuse Kihi (Simple Authentication and Security Layer, SASL)** abil
- Sertifikaadipõhise autentimise ja andmete kaitsmise teenust **Transpordikihi Turbeprotokolli (Transport Layer Security, TLS)** ning **Turvasoklite Kihti (Secure Socket Layer, SSL)** abil (Arkills, 2003, lk 34)

Active Directory

Üheks LDAP protokolli Maailmas laialt kasutatud näiteks on Microsoft Corporation poolt kasutusel olev Active Directory hajus arhitektuuriga teenus. Seda teenust kasutatakse Microsoft Windows Server 2000 ja 2003 opsüsteemides. Active Directory võimaldab terve võrgu tsentraliseeritult ja turvaliselt hallata. Active Directory teenus võib olla teostatud hoone, linna või erinevates maailma kohtades olevate süsteemide sidumiseks.
(Microsoft Corporation, 2003, Active Directory Collection)

1.3. Turvalisuse tõendamise märgistuskeel

Turvalisuse Tõendamise Märgistuskeel (Security Assertion Markup Language, SAML) on XML-põhine raamistik kasutaja autentimise, õiguste ja atribuutide informatsiooni edastamiseks. SAML oli välja töötatud ja on ka praegu arendamisel avatud standardite konsortsiumi **Tehnilise Turvateenuste Komisjoni (Security Services Technical Committee)** poolt, **OASIS (Organization for the Advancement of Structured Information Standards)**. SAML võimaldab teatud majandusüksustel kinnitada teistele üksustele, nagu partnerfirma või teise ettevõte rakendus, subjekti (tavaliselt on selleks inimkasutaja) identiteeti, atribuute ja õigusi. Enne SAML standardi loomist ei eksisteerinud XML-põhist standardit, mis võimaldaks turvasüsteemil edastada turvalisusinformatsiooni rakendusele, mis usaldab seda turvasüsteemi. SAML võimaldab informatsiooni kirjeldamist tüüpilisel XML standardile vastaval kujul ja võimalusi selle vahetamiseks ja hankimiseks. (Geyer, 2007, About SAML)

SAML versioon 1.0 sai OASIS standardiks 2002. aasta Novembris. SAML 1.1 järgnes 2003. aasta Septembris ning saavutas märkimisväärse edu, saades võetud kasutusele finantsteenuste, kõrghariduse, valitsuse ja teistes majandusharu segmentides. Tuntud tarkvara arendusfirmad hakkasid kasutama SAML keelt oma rakendusserverites. Paljud nendest teostustest näitasid erinevate ettevõtete ja isegi valitsuse poolt arendatud rakenduste koostöövõimet, mille aluseks sai SAML keele kasutuselevõtt. SAML 2.0 tuli välja 2005. aasta Märtsis ja tõi endaga kaasa

palju uut funktsionaalsust. SAML oli loodud teistes standardites kasutamiseks: **Liberty Alliance** aadressil http://www.projectliberty.org/, **Shibboleth** aadressil http://shibboleth.internet2.edu/ ja OASIS Web Services Security aadressil http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss. Kõik need projektid baseeruvad oma tehnoloogiaid SAML keele erinevale tasemele adopteerimisel. (Geyer, 2007, History of SAML)

SAML 2.0 ühendab kokku SAML V1.1 poolt pakutavaid ehitusplokke koos kõrghariduse Shibboleth initsiatiivi ja Liberty Alliance **Liitidentiteedi Raamistikuga (Identity Federation Framework, Liberty ID-FF)**. Esialgu Liberty Alliance defineeris ID-FF kui laiendust SAML 1.0 (hiljem ka SAML 1.1) standardile. Need laiendused said nüüd lisatud SAML 2.0 standardisse. Edaspidi on SAML 2.0 standardiks, mille baasil hakkab Liberty Alliance edaspidi looma identiteete ühendavaid rakendusi (federated identity applications). (Madsen, 2005)

SAML arhitektuuris kasutatakse järgmiseid standarte:

- **Hüperteksti Edastusprotokoll (Hypertext Transfer Protocol, HTTP)**
- **Laiendatav Märgistuskeel (Extensible Markup Language, XML)**
- **XML Skeem (XML Schema)**
- **XML Signatuur (XML Signature)**
- **Lihtne Objektipöördusprotokoll (Simple Object Access Protocol, SOAP)**

Liitidentiteedi Haldus

Kuigi SAML 1.0 ja SAML 1.1 sätestasid Ühekordse Sisselogimise ilmnemist läbi kasutaja identifikaatori kandva **Autentimise Lause** abil ühenduse loomise. Teatud kasutaja jaoks kasutatava identifikaatori valimise mehhanism ei olnud aga määratletud. Eeldati et identifikaator, olgu see e-posti aadress või midagi muud, saab valitud ja kokku lepitud kasutades mingit teist eraldiseisvat andmevahetust. SAML 2.0 aga juba täpselt sätestab kuidas kaks osapoolt saavad, kasutaja osalemisel, teha kindlaks identifikaatori (või mitu identifikaatorit) selle kasutaja jaoks. Lisaks sellele SAML 2.0 defineerib mehhanisme, mille abil võivad mõlemad osapooled kokku lepitud identiteete hallata. Näiteks: uuendada, tühistada. (Madsen, 2005)

Privaatsuse mehhanismid

Esimesed SAML keele versioonid ei olnud privaatsuse tagamisele optimeeritud. SAML 2.0 omab mitmeid tunnuseid, mis tagavad heal tasemel privaatsuse saavutamist. Märkimisväärne on **pseudonüümse identifikaatori** formaadi määratlus, mille abil kaks osapoolt saavad viidata üksikisikutele. Selline lähenemine kaitseb üksikisiku privaatsust, keelates erinevatele osapooltele

mitmete samasuguste koopiate tekitamist (nagu on võimalik globaalse identifikaatori puhul, üheks selliseks võib olla e-posti aadress).

Lisaks sisaldab SAML 2.0 mehhanisme, mis võimaldavad osapooltel privaatsuse poliitikat/seadeid üks teisega vahetada. Näiteks: Kasutaja nõusolek mõnda tegevuse läbiviimiseks võib olla saadud ühe rakenduse poolel, ning nõusoleku andmise fakt võib olla SAML tõendite ja protokollide abil edastatud teisele rakendusele. (Madsen, 2005)

Sessiooni Haldus

SAML 2.0 võimaldab lisaks Ühekordsele Sisselogimisele ka **Ühekordse Väljalogimise (Single Logout)** funktsiooni, mis oskab automaatselt lõpetada mitmeid erinevaid sessioone, mis on loodud erinevate rakenduste poolt. Näiteks, kui kasutaja, peale SAML autentimise protsessi läbimist, lõi sessioone mitmesse erinevasse kohta ühekordse sisselogimise mehhanismi abil, siis ühest neist sessioonidest välja logimine võib põhjustada kõikide teiste sessioonide lõpetamist (seda määratakse mõlema kasutaja seadete ja erinevate rakenduste poliitikate poolt). (Madsen, 2005)

SAML 2.0 Komponendid

Selles osas vaadeldakse SAML standardi poolt defineeritud komponente milleks on: tõendite, sidumiste ja profiilide kontseptsioon.

SAML 2.0 Komponendid: Tõendid

Tõendiks on informatsiooni pakett, mille sees on üks või mitu SAML keskuse poolt edastatud lauset. SAML keel defineerib kolm erinevat SAML keskuse poolt edastatava lause tüüpi:

- **Autentimine:** Teatud kasutaja oli autenditud teatud viisil ning teatud ajal.
- **Atribuut:** Teatud isik on edastatavate atribuutidega seostatud.
- **Volitamisotsus:** Teatud isiku teatud ressursile juurdepääsu saamise päring sai positiivse või negatiivse vastuse.

SAML 2.0 Komponendid: Protokollid

SAML määrab mitu erinevat üldistatud päringu esitamise ja vastuse andmise protokolle. Nendeks on:

- **Autentimispäringu Protokoll (Authentication Request Protocol):** Võimaldab üksikisikul (või isiku nimel tegutseval agendil) küsida autentimislauseid ja atribuute sisaldavaid tõendeid.

- **Ühekordse Väljalogimise Protokoll (Single Logout Protocol):** Võimaldab peaaegu samaaegset üksikisikuga seonduvate aktiivsete sessioonide lõpetamist. Väljalogimine võib olla initsialiseeritud kasutaja, keskuse või rakenduse poolt.
- **Tõendite Pärimise Protokoll (Assertion Query and Request Protocol):** Määrab päringute komplekti, mis võimaldab SAML tõendeid kätte saada. Tõendi kättesaamise päringus võib identifikaatori abil saada kätte olemasolevat tõendit. Lisaks määratakse ka tõendite pärimise korda, kasutades mingit kriteeriumit.
- **Tehisese Teisenduse Protokoll (Artifact Resolution Protocol):** Määrab viisi, mille abil SAML protokolli teateid saab edastada viidates väikesele, teatud pikkusega väärtust - tehiseset (artifact). Selle tehisese abil saab vastuvõtja küsida teate looja käest protokolli teadet ennast. Neid erinevaid objekte saadetakse erinevate edastuskanalite kaudu.
- **Nime Identifikaatori Haldamise Protokoll (Name Identifier Management Protocol):** Võimaldab muuta isiku identifikaatori väärtust või vormingut. Päringu väljaandjaks võib olla kas teenusepakkuja või identifikaatorite keskus. Lisaks sellele võimaldab protokoll kustutada identifikaatori assotsiatsiooni identifikaatorite keskuse ja teenusepakkuju vahel.
- **Nime Identifikaatori Vastenduse Protokoll (Name Identifier Mapping Protocol):** Võimaldab vastandada ühe SAML identifikaatori teisele, pärast vastavaid kontrolle. Näiteks, võib üks teenusepakkuja küsida identifikaatorite keskuse käest identifikaatorit teatud kasutaja jaoks. seda identifikaatorit saab teenusepakkuja kasutada teise teenusepakkuju juures, rakenduste integreerimise stsenaariumi puhul.

SAML 2.0 Komponendid: Sidumised

SAML protokollid on abstraktselt defineeritud - nende abstraktsete struktuuride vastendused reaalselt eksisteerivatele protokollidele kutsutakse SAML protokolli sidumisteks.

SAML 2.0 Komponendid: Profiilid

SAML põhispetsifikatsioon annab märkimisväärset paindlikkust mingi konkreetse teate koostamiseks. Kuigi selline paindlikkus sobib SAML raamistikule endale, ei aita see aga koostalitusvõime saavutamisel erinevate osapoolte vahel. SAML profiilid tegelevadki selle probleemi lahendamisega. Tavaliselt SAML profiil määrab kitsendusi ja/või laiendusi põhiliste protokollide ja tõendite jaoks, mida kasutatakse konkreetses rakenduses SAML protokolli toetamiseks. Leppides kokku mingi konkreetse profiili kasutamisel, saavutavad SAML teateid vahetatavad osapooled koostalitusvõimet palju lihtsamal viisil. SAML profiilid sätestatud avaldused/laused edastatakse kasutades sobilikke protokolli teateid üle spetsiifilisi sidumisi.

Turvalisus

Lihtsalt tõendite saatmisest ei pruugi piisata heal tasemel turvalisuse saavutamiseks. Võimalikke rünnakute avastamiseks ja nende eest kaitsmiseks defineerib SAML erinevaid turvalisuse mehhanisme. Põhiliseks mehhanismiks on loomine identiteedi pakkuja ja teenusepakkuja vahel eelnevalt usaldust, tavaliselt selleks kasutatakse **Avaliku Võtme Infrastruktuuri (Publik Key Infrastructure, PKI)**.

Soovitavalt tuleb konfidentsiaalse informatsiooni või tõendite saatmisel võtta kasutusele SSL 3.0 või TLS 1.0. On kohustuslik, et tõendit kandev sõnum oleks digitaalselt allkirjastatud. (Lockhart et al., 2008)

XACML

Laiendatav Pääsu Reguleerimise Märgistuskeel (eXtensible Access Control Markup Language, XACML) on XML-põhine pääsu reguleerimise keel.

XACML keelel on kaks erinevat komponenti: pääsu reguleerimise poliitika keel ja päring/vastus keel. Poliitika keelt kasutatakse pääsu reguleerimise poliitika väljendamiseks (kes millal ja mida teha saab). Päringu/vastuse keele abil kirjeldatakse päringuid (kas ligipääs teatud ressursile peaks olema lubatud) ja nendele päringutele antavaid vastuseid.

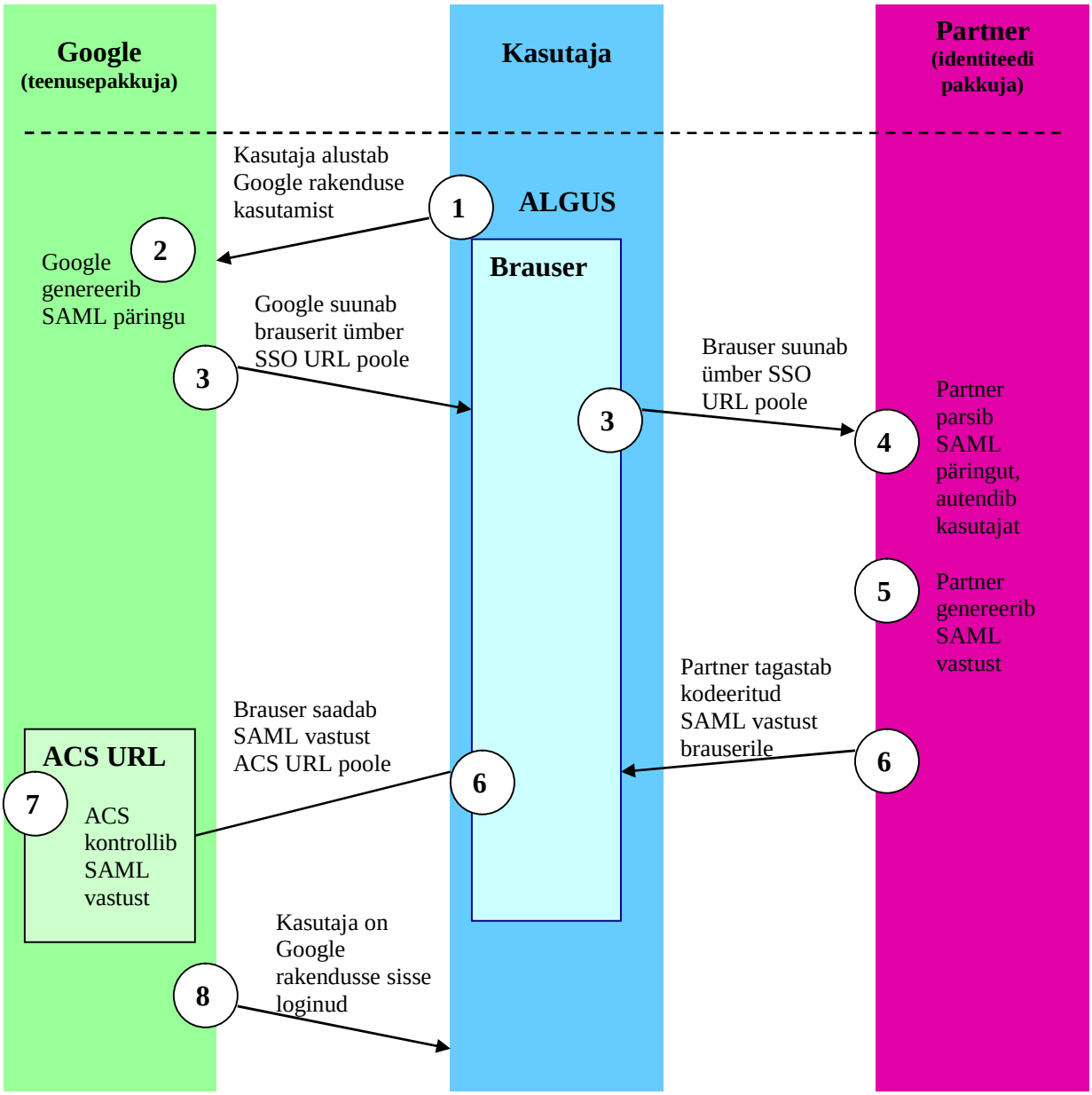
Uuemad XACML ja SAML keelte versioonid on loodud teineteise täiendamiseks. Näiteks: XACML poliitika võib täpselt määratleda mida peaks tegema pakkuja SAML tõendi saamise puhul, ning XACML atribuute saab SAML abil edastada (väljendada). (Geyer, 2007, XACML OASIS Standard)

SAML-põhine Ühekordne Sisseloginime Google Apps Rakenduse Näitel

Joonisel 6 näidatakse kasutaja sisse logimist Google Apps rakendusse, selleks kasutatakse partneri poort hallatavat SAML-põhist Ühekordse Sisselogimise (SSO) teenust.

Märge: Selle protsessi toimumiseks peab Google saama partneti käest viidet (URL) partneri SSO teenusele ja avalikku võtit, mille abil Google saaks kontrollida SAML vastuseid.

SAML Tehingu Sammud



Joonis 6. SAML abil Google Apps rakendusse sisse logimine (Google, 2007, SAML Single Sign-On (SSO) Service for Google Apps)

1. Kasutaja alustab Google poolt pakutava rakenduse kasutamist, selliseks võib olla Gmail või mõni teine teenus.
2. Google genereerib SAML autentimispäringu. SAML päring on kodeeritud ning manustatud partneri SSO teenuse poole suunatud viitesse. RelayState nimelist parameetrit lisatakse ka SSO viitesse, selle parameetri sees asub kasutaja poolt kasutusele võetava Google rakenduse viide. RelayState parameeter mängib identifikaatori rolli, seda antakse muutumata kujul tagasi.

3. Google saadab kasutaja brauserile ümbersuunamise. Ümbersuunamise viide sisaldab kodeeritud SAML päringut, mida tuleb edastada partneri SSO teenusele.
4. Partner dekodeerib SAML päringut ja eraldab välja mõlema **Kinnituse Tarbimiskeskuse (Assertion Consumer Service, ACS)** ja kasutaja sihtpunkti (RelayState parameeter) aadresse. Pärast seda toimub kasutaja autentimine. Partnerid saavad kasutajaid autentida, küsides kehtiva kasutaja mandaati või kontrollides kehtiva sessiooni küpsise olemasolu.
5. Partner genereerib SAML vastust, mis sisaldab autenditud kasutaja kasutajanime. Vastavalt SAML 2.0 spetsifikatsioonile, vastust allkirjastatakse partneri avaliku ja privaatse võtmetega.
6. Partner kodeerib SAML vastust ja RelayState parameetri ja tagastab informatsiooni kasutaja brauserile. Partner pakub mehhanismi, et brauser saaks informatsiooni Google Kinnituse Tarbimiskeskuse (ACS) poole edasi saata.
7. Google Kinnituse Tarbimiskeskus kontrollib SAML vastust, selleks kasutatakse partneri avalikku võtit. Kui vastust on edukalt kontrollitud, siis suunatakse kasutajat sihtpunkti viitele.
8. Kasutajat suunatakse sihtpunkti ja logitakse sisse Google Apps rakendusse. (Google, 2007, SAML Single Sign-On (SSO) Service for Google Apps)

Google'i poolt pakutavad teenused on laialt kasutatud, selle firma poolt SAML keel kasutusele võtmine on suureks edusammuks. See tõestab, et SAML keele abil on võimalik ehitada heal tasemel Ühekordset sisselogimist võimaldavaid lahendusi.

Eelised ja puudused

Igal tehnoloogial ja lahendusel on oma eelised ja puudused, järgnevalt on välja toodud SAML keele eelised ja puudused:

+ Võimaldab hästi toimivate Ühekordset sisselogimist võimaldavate süsteemide ehitamist
+ Põhineb olemasolevatel Interneti standartidel
+ Võimaldab kasutada pseudonüümseid identifikaatoreid, garanteerides kasutaja privaatsust
+ Liitidentiteedi raamistik ja haldamise võimalus
+ Ühekordse väljalogimise võimalus
+ Profiilide kasutamine aitab saavutada osapoolte vahelist koostalitusvõimet lihtsamal viisil
+ SSL või TLS kasutamine turvalisuse saavutamiseks, aitab kaitsta võimalikke rünnakute eest
+ Allkirjastamine ja Avaliku Võtme Infrastruktuur
+ Atribuutide vahetus

+ Theisese (artifact) kasutamine protokolli teadetele viitamiseks, võimaldab suuremahuliste sõnumite edastamist teiste edastuskanalite kaudu (kiirendab süsteemi toimimist)

– Suhteliselt keeruline ja mahukas protokoll (võrreldes OpenID protokolliga)
– Tavaliselt kasutatakse süsteemides, millega on mingil teenusepakkujal on vaja eelnevalt liituda (sellisel viisil saab luua süsteemi osapoolte vahel Usaldust, võtmete vahetus)
– Vähestel juhtumitel võib omada nõrkusi mõnedele rünnakute tüüpidele
– Protokolli realiseerimine mõnes süsteemis võib olla suhteliselt raske (kui tegemist ei ole suure äriettevõte või riigi sektori lahendustega)
– Koostalituse saavutamiseks peavad süsteemid kasutama samasuguseid profiile, eelnevalt on vaja profiilide kasutamisel kokku leppida

SAML on tõepoolest väga hea protokoll, mille abil saab erinevate rakenduste jaoks teostada Ühekordset sisselogimist. Tegemist on hästi dokumenteeritud tehnoloogiaga, mis on juba kõvasti arenenud. Samas tuleb tõdeda, et rakendamisel on tavaliselt vaja saavutada osapoolte vahelist usaldust. Lisaks sellel on vaja eelnevalt kokku leppida mingi konkreetse profiili kasutamist. Suures osas on selline tehnoloogia mõeldud suurematele tegijatele (ettevõtted, riigi süsteemid ja muud), kuna selle rakendamine ei saa olla väga lihtne.

1.4. Shibboleth

Shibboleth on samanimelise projekti raames arendatav ja põhiliselt teadusasutustes kasutatav avatud standardil põhinev autentimissüsteem. Shibboleth autentimissüsteem võimaldab luua erinevate piirkondade vahel Ühekordse sisselogimise ja kasutaja volitamise lubavat süsteemi (edastades kasutaja kohta käivaid atribuute). Autentimissüsteem omab turvalist raamistiku, mille abil saab lokaalsetele või eemalasuvatele ressurssidele edastada informatsiooni neid kasutatava isiku kohta. Liitidentiteedi kasutamine võimaldab, juhul kui isik tahab kasutada mõnda Shibboleth süsteemi poolt kaitstud ressurssi, selle isiku enda turvadomeenil saata vajalikku informatsiooni. Selle informatsiooni põhjal saab otsustada, kas isik saab loa selle ressursi kasutamiseks või mitte. Kasutajale võib olla lubatud otsustada kas väljastada teatud atribuute mingisugustele rakendustele või mitte. Selleks on vaja teostada isiklikke **Atribuutide Väljastamise Reegleid (Attribute Release Policies, ARP's)**, säilitades privaatsust ning samas saades sissepääsu usaldusväärse informatsiooni põhjal.

Shibboleth võimaldab kasutada ühele identiteedile vastastikku viitamist, ilma selle identiteeti paljastamata. Seega võib teenusepakkuja teada kasutajat ka ainult läbi juhuslikult genereeritava

ajutise identifikaatoriviide. Sellisel viisil, teades kasutaja volitusi, ei pruugi teenusepakkuja kasutaja enda identiteeti teadagi.

Shibboleth liit tagab arhitektuuri toimimiseks vajalikku usalduse osa. Liitu kuuluvad paljud ülikoolid, korporatsioonid, sisutarnijad ja teised, kes ühiselt vahetavad atribuute kasutades andmete edastamisel SAML/Shibboleth protokollidele kehtivat ühist reeglite ja tavade komplekti. Liitu kuulumine ei ole Shibboleth Süsteemi toimimiseks vajalik, aga see lihtsustab mitmete identiteedi pakkujate ja teenusepakkujate koostalitust. (Shibboleth Project, About)

Shibboleth Arhitektuur laiendab SAML keele ühekordse sisselogimise ja atribuutide vahetamise mehhanisme täpselt määrates SSO profiile ja kasutaja privaatsuse võimalusi.

Shibboleth Arhitektuur on ehitatud järgmiste standardite põhjal:

- **Hüperteksti Edastusprotokoll (Hypertext Transfer Protocol, HTTP)**
- **Laiendatav Märgistuskeel (Extensible Markup Language, XML)**
- **XML Skeem (XML Schema)**
- **XML Signatuur (XML Signature)**
- **Lihtne Objektipöördusprotokoll (Simple Object Access Protocol, SOAP)**
- **Turvalisuse Tõendamise Märgistuskeel (Security Assertion Markup Language, SAML)**

Shibboleth süsteemi komponendid

Shibboleth standardile vastava süsteemi põhikomponentideks on: identiteedi pakkuja, teenusepakkuja, mittekohustuslik „**Kust te pärit olete?“ (Where are you from?, WAYF)** teenus ning mõned muud alamkomponendid.

Identiteedi Pakkuja (Identity Provider, IdP) hooldab kasutajate mandaate ja atribuute. Saadab autentimistõendeid ja atribuute vastuseks teenusepakkujate päringutele. Selle alamkomponentideks on:

- **Autentimiskeskus (Authentication Authority)**, on integreeritud IdP autentimisteenusega ning väljastab autentimislauseid teistele komponentidele.
- **Ühekordse sisselogimise (Single sign-on, SSO)** teenus initsialiseerib autentimise protsessi ja suunab klienti ümber **Sisemisele Teisaldusteenusele (Inter-Site Transfer Service)**, mis suhtleb taustal Autentimiskeskusega vajalikku tõendi tekitamiseks. Tavaliselt on see SSO teenusega integreeritud.

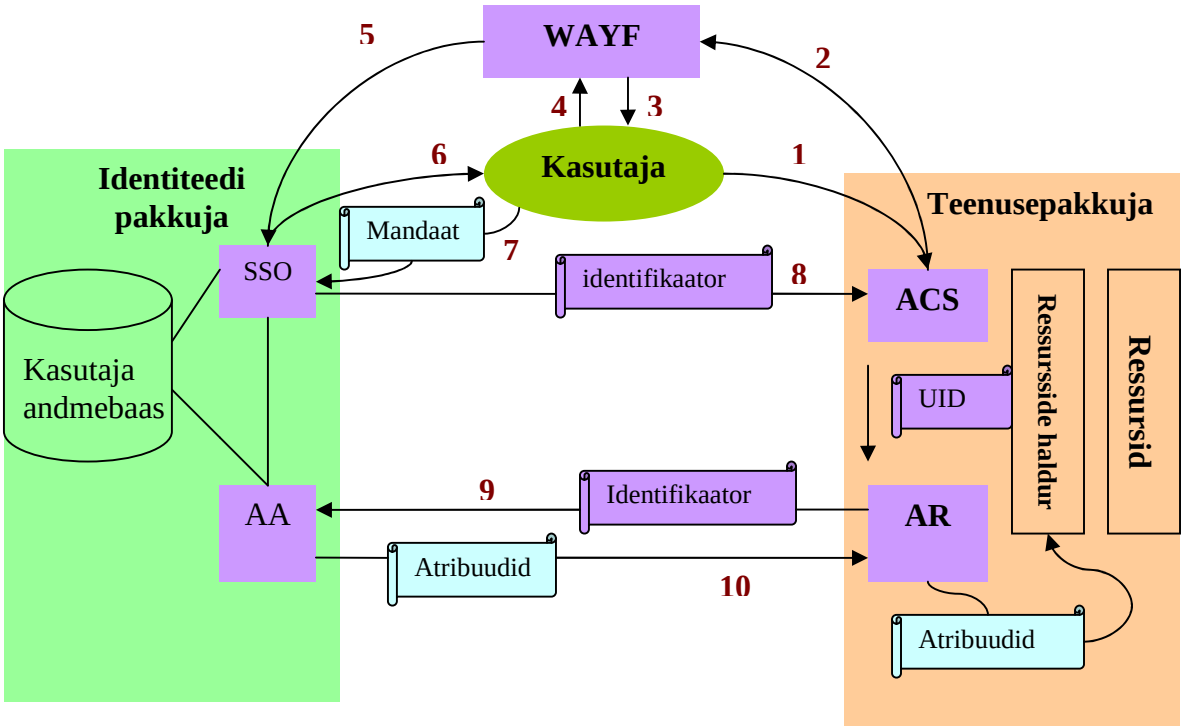
- **Tehisese Teisenduse Teenus (Artifact Resolution Service) -** kui kasutatakse vastavat profiili, siis IdP saadab teenuspakkujale reaalse tõendi asemel tehiseset (artifact). Selle viitena toimiva objekti abil saab teenusepakkuja reaalset tõendit, aga juba teise edastuskanali kaudu.
- **Atribuutide Keskus (Attribute Authority)** töötleb kõiki atribuutide päringuid, väljastab atribuutide tõendeid.

Teenusepakkuja (Service Provider) on kaitstud ressursside hoidla. Annab kasutajale ligipääsu identiteedi pakkuja käest saadud tõendite põhjal. Selle alamkomponentideks on:

- **Kinnituste Tarbimiskeskus (Assertion Consumer Service)**, mis töötleb identiteedi pakkuja poolt tagastatavaid tõendeid, algatab vajalikku atribuudi päringu tegemist, loob turvakonteksti ja suunab klienti ümber vajalikku ressurssi juurde.
- **Atribuutide Nõudja (Attribute Requester) -** teenusepakkuja ja atribuutide keskuse identiteedi pakkuja saavad vahetada atribuute teise kanali kaudu (ilma brauseri abita), sellisel juhul peab turvakontekst olema juba eelnevalt loodud.
- **WAYF** kesksus töötab väljaspool teenusepakkujat ja identiteedi pakkujat. Selle abil saab teha kindlaks kasutaja identiteedi pakkujat, kas kasutaja enda abil või automaatselt. (Cantor et al., 2005)

Shibboleth põhine autentimine

Alljärgneval Joonisel 7 on toodud „täielikku“ Shibboleth-toega autentimise näide, kus kasutaja poolt kasutatav brauser satub Teenusepakkuja juurde ilma brauseri sessiooni olemasoluta. Lisaks sellele ei ole ka mingit informatsiooni Identiteedi pakkuja kohta.



Joonis 7. Shibboleth autentimine. (Shibboleth Project, Shibboleth technical introduction)

1. Kasutaja proovib pöörduda teenusepakkuja serveris oleva Shibboleth poolt kaitstud ressursi poole.
2. Teenusepakkuja poolne Kinnituse Tarbimiskeskus (ACS) saadab kasutajat WAYF serveri poole.
3. WAYF server küsib kasutaja käest tema Identiteedi pakkujat (IdP).
4. Kasutaja täpsustab oma IdP serverit.
5. Kasutajat suunatakse ümber Identiteedi pakkuja SSO teenuse poole.
6. Identiteedi pakkuja küsib kasutaja käest sisselogimiseks vajalikku informatsiooni.
7. Kasutaja logib sisse oma lokaalse mandaatiga.
8. SSO teenus genereerib unikaalse Identifikaatori (UID) ja suunab kasutajat Teenusepakkuja Kinnituse Tarbimiskeskuse poole. Kinnituse Tarbimiskeskus kontrollib edastatud tõendit, loob sessiooni ja edastab andmeid Atribuutide Nõudja (AR) poole.
9. Atribuutide Nõudja kasutab Identifikaatorit Identiteedi pakkuja Atribuutide Keskuse (AA) käest atribuutide pärimiseks.
10. Atribuutide Keskus saadab vastuseks atribuute (lähtudes kehtivatest Atribuutide Väljastamise Reeglitest). Teenusepakkuja kasutab saadud atribuute pääsu reguleerimisel ja teiste rakenduse-poolsete otsuste juures. (Shibboleth Project, Shibboleth technical introduction)

Joonisel 7 välja toodud diagramm on suures osas eespoolt toodud Google Apps autentimise diagrammiga. Selle põhjuseks on kindlasti see, et Shibboleth on ehitatud SAML baasil.

Eelised ja puudused

Kuna Shibboleth on ehitatud SAML baasil, siis omab see ka kõiki selle eeliseid. Kuid tegemist ei ole lihtsa laiendusega. Shibboleth süsteemis on kasutatud ka omapäraseid komponente.
Shibboleth ei ole ainult standard, vaid tegemist on ka reaalse süsteemiga, mida saab kasutada.
Kindlasti on vaja seda eksisteerivate rakendustega integreerida. Shibboleth süsteemi põhilisteks eelisteks ja puudusteks on:

+ Põhineb SAML standardil, omab kõiki selle eeliseid
+ Avatud lähtekoodiga
+ Projekti raames on arendatud valmis tarkvara rakendus, mille abil saab seda juurutada
+ Võib olla kasutatud Sisevõrgu (Intranet) loomiseks
+ Annab heal tasemel kaitset
+ Võimaldab tuvastada, kas kasutajal on õigus ressurssi kasutada, ilma kasutaja identiteedi paljastamata (privaatsus)
+ Võimaldab WAYF teenuse kasutamist

– Keeruline ning mahukas
– Suhteliselt raske rakendada
– Kasutatakse kinniste süsteemide puhul, millega on vaja eelnevalt liituda

Shibboleth on hea süsteem, mis aga juba oma loomise käigus oli suunatud teatud valdkondades ja kohtades kasutamisele. Selle tulemusena on valminud väga turvaline ning usaldusväärne lahendus. Kui selle lahenduse kasutamisele võtmine on suhteliselt raske, kuna integreerimine olemasolevatesse süsteemidesse on päris keeruline.

1.5. Windows CardSpace

Windows CardSpace on tarkvaraklient, mille abil kasutajad saavad anda veebiteenustele digitaalset identiteeti lihtsal, turvalisel ja usaldusväärsel viisil. Seda nimetatakse **identiteedi valijaks (identity selector)**. Kui kasutajal on vaja teatud veebiteenusega autentida, siis CardSpace avab spetsiaalse hästi kaitstud ja mugava graafilise liidese. Selles graafilises liideses näidatakse kaarte, nende seast saab kasutaja endale sobiva valida. Iga kaardiga on seotud identiteediandmed, samas need ei paikne kaardi enda sees, vaid olid antud kasutajale mõne identiteedi pakkuja poolt või lõi kasutaja neid ise. Kuigi see võib väga veidrana tunduda (kasutaja mängib identiteedi pakkuja rolli), samas teevad kasutajad seda iga kord kui nad mingis

veebiteenuses kasutajakonto loovad. Selliste **Personaalsete kaartidega (Personal cards)** saab seostada piiratud identiteedi andmete kogust. CardSpace graafiline liides võimaldab kasutajatel importima **Hallatud kaarte (Managed cards)** teiste identiteedi pakkujate käest. Kui kasutaja valib mõnda kaarti, siis kaardiga seotud identiteedi pakkuja genereerib allkirjastatud ja krüpteeritud turvaluba (security token). Seejärel otsustab kasutaja, kas anda seda informatsiooni veebiteenusele üle või mitte. Kui kasutaja annab oma luba, siis saadetakse vastav info veebiteenusele töötlemiseks ja identiteedi ekstraktimiseks.

CardSpace on identiteedi valijaks Microsoft Windows süsteemide jaoks. Teised opsüsteemid omavad teisi identiteedi valijate teostusi (näiteks: DigitalMe Mac ja Linux süsteemide jaoks). Subjekte, identiteedi pakkujaid ja teenusepakkujaid koos nimetatakse Identiteedi Metasüsteemiks (Identity Metasystem) - arhitektuur millel baseerub CardSpace teenus. CardSpace ei ole ainult Microsofti algatus, vaid pigem jagatud visioon tänapäeva Interneti identiteedi väljakutsete lahendamiseks. (Microsoft Corporation, What is Windows CardSpace?)

1.6. Kokkuvõte

Selles osas vaadeldi Ühekordse Sisselogimise põhimõtete rakendamist võimaldavaid ning tänapäevaks juba laialt kasutust leidnud tehnoloogiaid. Alguses kirjutati Ühekordse Sisselogimise põhimõtetest ning erinevustest võrreldes pärand-lähenemisega, mis nõudis kasutajalt iga uue süsteemis kasutamise alustamisel sisselogimise protsessi läbimist. Tihtipeale võisid kasutajal erinevates süsteemi komponentides olla erinevad kasutajatunnused ja paroolid, mis ei olnud väga kasutajasõbralik ja mugav lahendus. Tutvustati Liitidentiteeti mõistet, mis omab Ühekordset Sisselogimist lubavate süsteemide kontekstis väga suurt tähtsust.

Vaadeldi ning uuriti mitut erinevat tehnoloogiat, mida tänapäeval kasutatakse paljudes süsteemides. Tutvustati LDAP, SAML protokollide ja SAML standardi baasil tehtud Shibboleth autentimissüsteemi tööpõhimõtteid ning ülesehitust. Toodi välja erinevate tehnoloogiate eeliseid ja puudusi. Tutvustati erinevaid lahendusi kasutatavate süsteemide kasutaja autentimise käiku ning joonistati selle kohta diagrammid. Lühidalt tutvustati ka Windows CardSpace tehnoloogiat.

2. Ühekordne sisselogimine OpenID ja ID-kaardi abil

2.1. OpenID

Mis on OpenID?

OpenID kõrvaldab erinevates veebirakendustes mitme erineva kasutajanime kasutamist, seeläbi lihtsustades kasutajal igapäevast Interneti kasutamist.

Iga kasutaja saab ise valida kõige usaldusväärsema ja sobivama OpenID pakkuja olemasolevate hulgast. OpenID Identiteedi pakkuja muutmisel võib olemasolev identifikaator jääda kasutajale. Lisaks sellele on OpenID iseenesest täielikult vaba tehnoloogia, mis ei ole mingi äriettevõte oma. Ettevõtetele tähendab see väiksema kasutajakontode haldamise maksumust. OpenID pakub kasutajatele suuremat kindlustunnet, kuna iga kasutaja saab oma sisselogimist kontrollida.

OpenID on avatud, hajutatud, tasuta raamistik kasutaja-keskse digitaalse identiteedi võimaldamiseks. OpenID kasutab olemasolevaid Interneti tehnoloogiaid (URI, HTTP, SSL, Diffie-Hellman) ja tajub, et inimesed juba praegu loovad endale identiteete kas blogi, albumi, profiililehe või mingil muul kujul. OpenID tehnoloogia kasutamisel saab lihtsal viisil transformeerida ühte neist universaalsetest ressursiidentifikaatoritest kasutajakontoks, mida saab hiljem kasutada OpenID sisselogimist võimaldavates veebirakendustes.

OpenID on hetkel veel omaksvõtu faasis ning saavutab aina rohkem populaarsust, kuna suured organisatsioonid nagu AOL, Microsoft, Novell ja teised hakkavad kasutama OpenID tehnoloogiat. Hetkeseisuga eksisteerib üle 160 miljoni OpenID võimelist universaalset ressursiidentifikaatorit koos ligi kümne tuhande OpenID sisselogimist võimaldavate veebiteenustega. (OpenID.net, What is OpeID?)

Kes omab kontrolli OpenID üle?

OpenID sai algatatud avatud lähtekoodi kogukonna poolt selliste probleemide lahendamiseks, mida ei saanud juba olemasolevate tehnoloogiate abil lahendada. OpenID on lihtne indiviidide identifitseerimise meetod, mis kasutab veebisaitide identifitseerimise tehnoloogilist raamistiku. Iseenesest ei ole OpenID kellegi omand, ning ta kunagi ei peakski olema. Tänapäeval võib igaüks saada OpenID kasutajaks või OpenID Identiteeditеenuse pakkujaks. Selleks ei ole vaja

kuskil registreerida ega saada mingi organisatsiooni heakskiidu. (OpenID.net, Who Owns or Controls OpenID?)

„Keegi ei saa seda omada. Kellegil ei ole plaanis sellega raha teenida. Eesmärgiks on iga selle osa avalikustamine kõige liberaalsema litsentsi alusel, et mängu ei tuleks raha, litsentseerimine või registreerimine. Sellise asja olemasolu toob kasu tervele kogukonnale, ja kõik me oleme kogukonna liikmeteks.“ (Brad Fitzpatrick, OpenID looja)

OpenID Foundation (OIDF) loodi 2007. aasta Juunis OpenID tehnoloogiate ja kogukonna edutamiseks, kaitsmiseks ja juurutamiseks. OIDF ei määra OpenID tehnilist suunda. Selle asemel OIDF juurutab ja kaitseb kõike, mis on kogukonna poolt loodud. (OpenID.net, OpenID Foundation)

OpenID protokoll

OpenID spetsifikatsioonid arendatakse kogukonna poolt. Kogukonna liikmed teevad kindlaks, et iga mustandi staatuses olev ettepanek (draft proposal) on vastavuses OpenID arengu üldprintsiipidega: mitte üleliigselt keeruline, modulaarne, tasuta, mitte üleliigselt koormatud ning laiendatav.

OpenID on toetatud mitmete programmeerimiskeelte poolt ning nende jaoks leidub ka valmis tehtud teeke (libraries): Java, PHP, Perl, Ruby, Python. Rohkem informatsiooni võib leida aadressil http://wiki.openid.net/Libraries.

Hetkeseisuga on ametliku spetsifikatsiooni staatuseni jõudnud:

- **OpenID Autentimine 2.0 (OpenID Authentication 2.0)**
- **OpenID Atribuutide Vahetus 1.0 (OpenID Attribute Exchange 1.0)** - OpenID teenuse laiend, võimaldab lõpp-punktide vahelist identiteedi informatsiooni vahetamist.
- **OpenID Autentimine 1.1 (OpenID Authentication 1.1)**
- **OpenID Lihtsa Registreerimise Laiend 1.0 (OpenID Simple Registration Extension 1.0)** - OpenID protokolli laiend, võimaldab väga kerget profiili vahetust. Selle abil saab edastada kaheksa üldkasutatavat parameetrit, kui kasutaja registreerib endale uue konto mingi veebiteenuse juures. Sellisteks üldkasutatavateks parameetriteks on: Täisnimi (fullname), Hüüdnimi (nickname), E-post (email), Sünnikuupäev (dob), Kasutaja sugu (gender), Kasutaja keel (language), Riik (Country), Ajavöönd (timezone).

- **Yardis Avastuse Protocoll (Yardis discovery protocol**); Arendatud eraldi projektis, seda kasutatakse OpenID 2.0 versioonis. (OpenID.net, Read the Specifications)

OpenID 1.1 ja 2.0 peamised erinevused

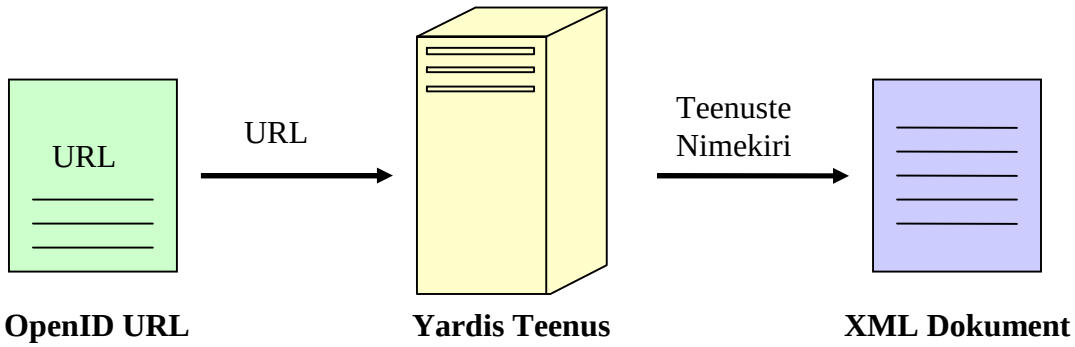
OpenID spetsifikatsioonid eksisteerivad kahes erinevas versioonis: 1.1 ja 2.0. Nende versioonide vahel on olemas mõningaid erinevusi. Versiooni 2.0 saab kasutada versiooniga 1.1 tagasiühilduval viisil. Versioonide 1.1 ja 2.0 põhilisteks erinevusteks on:

- Yardis protokolli kasutamine teenuse leidmiseks
- XRD dokumentide tugi
- Turvalisuse parandamiseks lisati positiivsete tõendite sisse spetsiaalseid väärtusi (nonce), korduva väärtusega positiivset tõendit vastu ei võeta. Sellisel viisil saab kaitset kordusrünnete (relay attack) vastu.
- Tugi DH-SHA256 võtmete vahetamiseks ja HMAC-SHA256 tugevamate krüpteerimiste jaoks. (Rehman, 2008, lk 73)

Yardis

Yardis on lihtne protokoll XML keele baasil. Selle abil saab Teenusepakkuja avastada nii autentimist, kui ka teisi konkreetsel URL aadressi poolt pakutavaid teenuseid. Kuna URL aadressi saab kasutada mitmete süsteemide poolt, siis saab Yardis protokolli abil tuvastada teenuse tüüp ja identifitseerimise mehhanism. Vastavalt hetkel olevatele spetsifikatsioonidele töötab Yardis üle HTTP protokolli. Vastuseks päringule saadetakse tavaliselt **Laiendatava Ressursikirjelduse (eXtensible Resource Descriptor, XRD**) vormingus XML dokument. (Rehman, 2008, lk 53)

Joonisel 8 on näidatud Yardis teenus, mis võtab sisendiks URL aadressi ning väljastab XML dokumenti. Seejärel Teenusepakkuja ise interpreteerib XML dokumenti ja saab olemasolevaid teenuseid kasutada. Yardis soodustab erinevate Identiteedi teenuste vahel koostöö tegemist.



Joonis 8. Yardis teenuse sisend ja väljund. (Rehman, 2008, lk 55)

OpenID süsteemi komponentide koostöö

OpenID süsteem koosneb kolmest põhikomponendist: Teenusepakkuja (Tarbija), Identiteedi pakkuja ja kasutajaagent (teisi sõnu veebibrauser). Autentimise protsessi käigus suhtlevad need komponendid teineteisega.

- Teenusepakkuja ehk Tarbija on veebiteenus, kuhu kasutaja proovib sisse logida, suhtleb Identiteedi pakkujaga ja Kasutajaagendiga. Lõppkasutaja proovib teenusepakkuja veebiteenusesse OpenID abil sisse logida. Autentimisprotsessi käigus saadab Tarbija mitu sõnumit nii otse Identiteedi pakkujale, kui ka läbi Kasutajaagenti (kasutades selleks HTTP ümbersuunamissõnumeid).
- Identiteedi pakkuja on OpenID server, kus paikneb Lõppkasutaja mandaat (credentials). Identiteedi pakkuja valideerib antud identiteedi URL aadressi ning saadab tarbijale vastuse.
- Lõppkasutaja suhtleb Tarbijaga ja Identiteedi pakkujaga kasutajaagendi abil.

Autentimisprotsessi käigus mängib veebibrauser sõnumite vahendaja rolli Identiteedi pakkuja ja Tarbija vahel. Tavaliselt Tarbija suhtleb veebibrauseriga autentimisprotsessi jooksul nagu ka Identiteedi pakkuja. Kuid mõnedel juhtudel võib Tarbija kasutada vahemällu salvestatud (cached) võtmeid, sellisel viisil saab kasutajat autentida ilma otsese suhtlemise Identiteedi pakkujaga.

Kuna kasutaja omab kontrolli oma URI üle, siis see võib paikneda kas Identiteedi pakkuja juures või kuskil mujal. Kui kasutaja on oma URI omanik, siis ta saab ta kasutada teist OpenID serverit ning tema identiteet jääb samaks. Sellisel juhul hangib Identiteedi tarbija URI OpenID süsteemis ja ükski teine osapool ei pea seda enam tegema. Lisaks sellele saab kasutada ka oma

veebibrauserit OpenID Identiteedi pakkujana, sellisel juhul osalevad infovahetuses ainult kaks osapoolt. (Rehman, 2008, lk 59)

Otsene ja Kaudne Infovahetus (suhtlus)

Eksisteerib kaks üldist infovahetuse meetodit OpenID süsteemi komponentide vahel: **Otsene Infovahetus (Direct Communicatiob)** ja **Kaudne Infovahetus (Indirect Communication)**.

Otseses Infovahetuses kaks olemit suhtlevad üksteisega HTTP protokolli abil, kasutades selleks HTTP POST meetodit.

Kaudse Infovahetuse puhul kaks olemit suhtlevad üksteisega mingi kolmanda olemi kaudu. Tavaliselt on selleks kolmandaks olemiks veebibrauser. Kaudne infovahetus (HTTP GET meetodi abil) võib toimida **HTTP Ümbersuunamise (HTTP Redirect)** või **HTML Vormi (HTML Form)** ümbersuunamise kaudu. (Rehman, 2008, lk 63)

OpenID Identiteedi URL Leht

Kuna kasutaja kontrollib ise oma identiteeti, siis ta saab panna oma OpenID URL aadressi ükskõik mis serverile (ei ole vajadust paigutada seda Identiteedi Pakkuja juurde). Tavaliselt on vaja luua HTML dokument, kust saab leida vajaliku informatsiooni. Selle dokumendi URL ongi kasutaja Identifikaator. Kui mõlemad Identiteedi pakkuja ja Tarbija toetavad 2.0 versiooni, siis saab kasutada ka XRD dokumenti. All on toodud võimaliku HTML lehe näide. (Rehman, 2008, lk 71)

```
<html>
 <head>
  <link rel="openid.server" href="http://someopenid.com/server">
  <link rel="openid.delegate" href="http://idp.somserver.com/?user=someuser">
 </head>
 <body>
  <h3>OpenID Identity Page</h3>
  <p>
  This is the identity page for the user <strong>someuser</strong>.
  </p>
</body>
</html>
```

(Rehman, 2008, lk 72)

Näides kasutataval lehel on **openid.server** võtmesõnaks ning peaks olema just sellisel kujul, **href** osa võib aga muutuda vastavalt sellele mis Identiteedi pakkujat kasutatakse (vastavalt Identiteedi pakkuja sättimistele võib alguses olla HTTP või HTTPS). Vastav rida näites seletab Tarbijale mis OpenID serveriga on vaja ühendust luua kasutaja autentimiseks. **openid.delegate** reast saab välja lugeda OpenID URI. Tuleb märkida, et **delegate** võtmesõna kasutatakse juhtudel, kui URI asub väljaspool serverit. (Rehman, 2008, lk 72)

OpenID Turvalisus

OpenID protokolli kasutamisel tuleks kaaluda võimalikke turvalisuse riske ning ehitada rakendatavat süsteemi nii, et see tagaks heal tasemel turvalisust.

Võimalikud rünnakute liigid:

- **Kordusrünne (relay attack)** - selliste rünnakute tõenäosust vähendati spetsiaalsete **nonce** väärtuste lisamisega OpenID sõnumitesse. Kui aga Tarbija ei tegele aktiivselt nonce väärtuste salvestamisega või võimaldab liiga vana ajatempli kasutamist, siis muutub ta seda tüüpi rünnakutele haavatavaks. Kaks sammu peaks aitama nende rünnakute ärahoidmiseks:
    - Kõik tarbijad ja Identiteedi pakkujad peaksid kasutama **Võrguaja Protokolli (Notwork Time Protocol, NTP)** oma kellade sünkroniseerimiseks ajaserveriga.
    - Tarbijad peaksid ignoreerima neid sõnumeid, kus vahe praeguse aja ja ajatempli vahel on piisavalt suur.
- **Õngevõtmine/õngitsemine (phishing attack)** - selle rünnakuga hakkama saamiseks on vaja kasutada turvalisi andmete edastamise viise (eriti autentimise saavutamisel). Lisaks sellele arendatakse erinevaid laiendeid, mis aitaksid selle probleemi lahendamisel. (Rehman, 2008, lk 213)

OpenID süsteemi jaoks on SSL kasutamine väga oluline. SSL krüpteerib kõiki andmeid transpordi tasemel ning on väga laialt kasutatud turvameetmeks veebibrauseri ja serveri vahel. On väga soovitatav krüpteerida kogu OpenID protokolli liiklust Teenusepakkuja, Identiteedi pakkuja ja Kasutaja veebibrauseri vahel.

Veel üheks potentsiaalseks probleemiks võib olla Veebibrauseri Ajalugu. Kuna mõningaid OpenID sõnumeid saadetakse HTTP GET meetodiga, siis võib veebibrauser neid salvestada. Kui ründaja saab arvutile ligi, siis võivad need sõnumid anda talle väärtuslikku informatsiooni. Eriti kriitiliseks võib see muutuda avaliku kasutuse arvuti puhul, kus mitu erinevat inimest saavad

ligipääsu veebibrauseri ajaloo juurde. Selle probleemi vältimiseks on kasutajal vaja arvutiga töö lõpetamisel veebibrauseri kasutusajaloo kustutada.

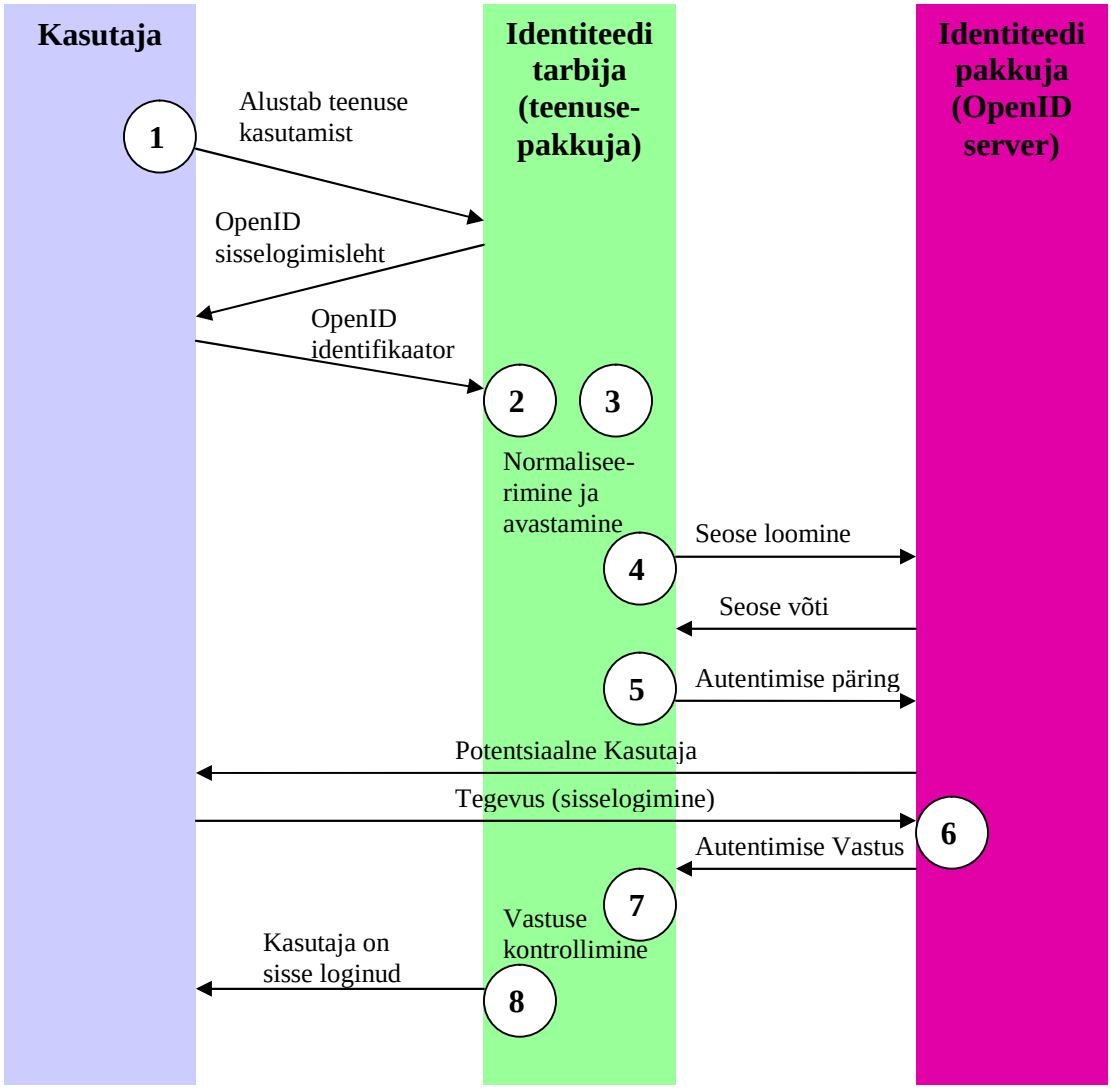
Identiteedi pakkuja saab oma kasutajate kohta palju informatsiooni, nagu kasutaja poolt külastatavate veebiteenuste infot. Selle informatsiooni abil saab luua identiteedi omaniku veebiteenuste kasutuse profiili. Lisaks sellele paiknevad Identiteedi pakkuja juures kõik kasutaja tõendid teiste teenuste kasutamiseks. Seega kasutajal oleks vaja valida endale usaldusväärne ja heade kaitsemehhanismidega Identiteedi pakkujat, et maandada võimalikke riske. (Rehman, 2008, lk 214)

OpenID ja Windows CardSpace

OpenID ja CardSpace integratsiooni puhul eksisteerib kasutaja OpenID URL "kaardi" kujul, mida saab kasutada CardSpace tehnoloogiat toetavatesse veebirakendustesse sisenemisel. Sellisel viisil töötab OpenID identiteet mõlema OpenID ja CardSpace teenust kasutatavate veebirakendustega. (Rehman, 2008, lk 217)

OpenID põhine sisselogimine

Joonisel 9 näidatakse OpenID põhist kasutaja autentimist.



Joonis 9. OpenID abil autentimine. (Stepka, 2007)

1. Kasutaja läheb Teenusepakkuja (identiteedi tarbija) juurde ning sisestab vastavasse kohta oma OpenID identifikaatorit. Näiteks: http://minunimi.identiteedipakkuja.com.
2. Teenusepakkuja käivitab normaliseerimise protsessi (tuvastatakse kas tegemist on URL või XRI tüüpi identifikaatoriga, siis viiakse seda vastavusse protokolli poolt esitatavate nõuetega).
3. Normaliseeritud identifikaatori abil otsitakse vajalikku informatsiooni edasiste päringute tegemiseks. Sellisel viisil saadakse teada kasutaja Identiteedi pakkujat ja muud vajalikku informatsiooni.
4. Teenusepakkuja loob Identiteedi pakkujaga võtmete abil seost (mittekohustuslik). Seda võtit kasutatakse edaspidi sõnumite allkirjastamiseks. Sellisel viisil võib saavutada paremat turvalisust.

5. Teenusepakkuja esitab päringu kasutaja autentimiseks. Päringut ei esitata otse Identiteedi pakkujale, vaid ümbersuunamise kasutamisel suunatakse kasutajat Identiteedi pakkuja juurde. Sellisel viisil ei saa teenusepakkuja autentimise protsessis kasutatavat informatsiooni.
6. OpenID server vastab autentimispäringule. Kuna Identiteedi pakkuja saab autentimispäringu läbi kasutaja, siis on tal võimalus teha mitmeid interaktioone kasutajaga selle protsessi käigus. Sellisel viisil saab kasutaja ise valida, kas lubada autentimist või mitte.
7. Teenusepakkuja kontrollib saabunud vastust/tõendit. Selle kontrolli käigus tehakse kindlaks: et ümbersuunamise aadress klapib kasutaja esialgse aadressiga, avastatud informatsioon on sama mis tõendis olev, kontrollitakse spetsiaalse unikaalse (nonce) atribuudi väärtust, kontrollitakse allkirjastamise võtit.
8. Kui vastuse/tõendi kontrollimine oli edukas, siis on kasutajal õnnestunud sisse logida. (Stepka, 2007)

Eelised ja puudused

Nagu ka teistel tehnoloogiatel ja lahendustel, on OpenID kasutusel oma eelised ja puudused:

+ Võimaldab Ühekordset sisselogimist
+ Tasuta ning kõigile avatud
+ Lihtne rakendada juba olemasoleva süsteemi kontekstis
+ Laiendatav standardsete laiendite abil
+ Kasutab ära olemasolevaid Interneti tehnoloogiaid
+ Lihtsa Registreerimise laiend defineerib 8 üldkasutatavat parameetrit, mida saab Identiteedi pakkuja edastada Identiteedi tarbijale
+ Teekid (libraries) erinevate programmeerimiskeelte jaoks
+ Võimaldab luua tõepoolest avatud süsteeme
+ Oskab kasutada võtmeid, krüpteerimist ja teisi turvamehhanisme (SSL)
+ Teenusepakkuja avastamise mehhanismid (Yardis)
+ Võimaldab valida endale sobivat identiteeti
+ Kasutaja omab kontrolli identiteedi üle
+ Lihtsal viisil saab luua oma Identiteedi pakkuja serverit

− Võib olla haavatav mõnede rünnakute liikidele
− Identiteedi pakkuja kaitsemehhanismide tase peab olema kõrge, sest seal hoitakse kasutaja tõendeid ning ka kasutatavate teenuste statistikat

- Identiteedi pakkuja usaldusväärsus probleem

OpenID on väga lihtne ning mugav tehnoloogia, mille realiseerimist olemasolevates rakendustes saab teostada praktiliselt igaüks. OpenID sisselogimise realiseerimisel ei ole vaja mõelda mingite teatud profiilide kasutusele võtmisest. Võimalikud laiendid toovad endaga kaasa pigem lisafunktsionaalsust. Kui üks osapooltest seda laiendit ei toeta, siis ei sega see kuidagi OpenID autentimise toimimist. Esimeste versioonide turvaprobleemid on juba suures osas lahendatud.

2.2. ID-kaart

ID-kaart on uue aja isikuttõendav dokument, mida saab kasutada ka Internetis oma identiteedi tõestamiseks. Tegemist on mugava ning võltsimisekindla dokumendiga, millel on juba praegu palju kasutamisviise ja neid tuleb aina juurde. Kaardi ennast valmistab Šveitsi firma Trüb AG, isikuandmeid aga trükitakse kaardile Eestis. Selle protsessi valvamiseks kasutatakse väga tõsiseid turvameetmeid. (Martens, 2002)

ID-kaardi ajalugu

Kõik algas 2001 aasta veebruaris, millal Hansapanga, SEB Eesti Ühispanga, Elioni ja EMT poolt sai loodud aktsiaselts Sertifitseerimiskeskus (SK). SK loomise eelduseks oli 2000. aastal jõustunud digitaalallkirja seadus. Kevadel võitis Sertifitseerimiskeskus Siseministeeriumi riigihanget Eesti ID-kaartide sertifitseerimisteenuse pakkumiseks. 2002. aasta jaanuaris jõudsid esimesed ID-kaardid omanikeni. Eesti president Arnold Rüütel ja tema naine olid esimesed inimesed, kes said endale uue aja isikutunnistust. Sellega algas ID-kaardi tee Eesti ühiskonda. (Martens, 2002)

ID-kaardi kasutamisvõimalused ja eelised

ID-kaart ei ole ainuüksi väike ja mugav plastikust tehtud isikuttõendav dokument, mida saab Eesti siseselt kasutada. Vaid sellega saab ka reisida Euroopa Liidus, Euroopa Majanduspiirkonna liikmesriikides ning Šveitsis. Lisaks sellele on võimalik ID-kaardi abil anda **digitaalseid allkirju**, mille abil saab teostada digitaalset elektroonsete dokumentide ringlust.

Viimasel ajal on arvutitehnoloogiad kiiresti arenenud, mis toob endaga kaasa nii head, kui ka halba. Kiire Interneti areng on toonud endaga kaasa palju uusi võimalusi, mida inimesed kasutavad ka oma igapäevases elus ja tööülesannete täitmisel. Ka siin saab ID-kaart toeks olla. Praegusel hetkel saab suurema osa riigi veebiteenustest ning ka mõnede ettevõtete veebiteenustest kasutada ID-kaardi abil. Mis teatud raames realiseerib **Ühekordse Sisselogimise** süsteemi. Üheks tüüpiliseks näiteks võib olla sisenemine Ühte veebiteenusesse läbi mõnda teist

veebiteenust. Tavaliseks juhtumiks võib olla mõne Internetipanga portaali kasutamisel sisse logimine mõnda riigi või teise ettevõte portaali (Maksu- ja Tolliamet, EMT iseteenindus, Eesti Energia).

Veel üheks ID-kaardi heaks iseloomujooneks võib nimetada **turvalisust**. ID-kaardil on palju keerukaid füüsilisi turvaelemente. Kaardi elektrooniliseks kasutamiseks on vaja teada PIN koode, PIN1 on kasutatud kasutaja identifitseerimiseks ja PIN2 on kasutatud digitaalse allkirja andmiseks. PUK koodi abil (see on neist kolmest kõige keerukam) saab vajadusel muuta oma PIN1 ja PIN2 koode. Digitaalse allkirja ehtsust ja sertifikaadi kehtivust kontrollib Sertifitseerimiskeskus AS, kes tegeleb ka peatatud ja tühistatud sertifikaatide nimekirja haldamisega. Identiteedi informatsiooni vahetamisel kasutatakse krüpteerimist ning teisi turvatehnoloogiaid. Mis teeb ID-kaardist ühe väga usaldusväärse elektroonilise Identiteedi tõestamise allika. ID-kaardi kasutamise turvanõuetega saab tutvuda aadressil http://www.id.ee/10358?id=10521.

Üks levinumaid ID-kaardi kasutamisviise on **ID-pilet**. Iga kaardi omanik saab osta endale digitaalset piletit, sellise pileti olemasolu saab kontrollida ID-kaardi abil.
Iga kaardi omanik saab endale isikliku **@eesti.ee e-posti aadressi**. Selle aadressi abil saab toimida riigi ja isiku vaheline suhtlus, kuhu saadetakse ametlikke teateid ja isikut puudutavat personaalset infot. Samas saab isik seda aadressi kasutada ka oma isikluks otstarbeks. (Sertifitseerimiskeskus, id.ee, 2008, ID-kaart - uue aja isikutunnistus)

Mobiil-ID

Üheks viimasel ajal tekkinud uueks võimaluseks on Mobiil-ID. Mobiil-ID on telefoni SIM-kaart, mis sisaldab lisaks tavalise SIM-kaardi funktsioonidele ka mobiilset identiteeti. Mobiilse identiteedi abil saavad internetiteenuste pakkujad kasutajat tuvastada, samuti on võimalik kasutajal oma digitaalset allkirja anda. Mobiil-ID abil saab teha samu e-toiminguid, nagu ka oma ID-kaardiga. Mobiil-ID tuleb enne kasutamist oma ID-kaardiga aktiveerida. Mobiil-ID sertifikaadid kehtivad 5 aasta jooksul, pärast seda tuleb vana SIM-kaart uue vastu vahetada. Mobiil-ID omab ka mitu eelist: enam ei ole vajadust kaardilugejate kasutamiseks, ei mingit lisatarkvara paigaldamist. Mobiil-ID on universaalne.(Keskel, 2008)

OpenID.ee

Ideelabor arendab viimasel ajal uut teenust, mis võimaldab kasutada OpenID tehnoloogiat käsikäes Mobiil-ID ja Eesti ID-kaardiga. Teenuse kohta saab mõningat informatsiooni veebilehel http://openid.ee. (Ideelabor, Mis on OpenID.ee?)

Hetkeseisuga ei veel tegemist täisfunktsionaalsuse ning lõpetatud teenusega, vaid versiooni tähiseks on **beta2**. Üheks lihtsaks näiteks on kasutaja identiteedi leht (URL). Ainsaks lehe külastajale näidatavaks informatsiooniks on teade, et tegemist on OpenID identifikaatoriga. Mingit informatsiooni selle omaniku kohta pole võimalik leida. Teenusesse ID-kaardi abil sisse logitud kasutajale näidatakse ainult informatsiooni tema OpenID identiteedi (identifikaatori) kohta, ei ole võimalik valida lehe külastajatele kuvatavat informatsiooni. Omavahel saab võrrelda järgmiseid lehti: https://openid.ee/pjotr.savitski ja http://pjotr.savitski.myopenid.com/.
Praegusel hetkel OpenID.ee teenus toetab OpenID **Autentimise versiooni 2.0** ja **Lihtsa Registreerimise Laiendi versiooni 1.1 mustandit** (Simple Registration 1.1 draft 1). Kui kasutaja otsustab oma andmeid mingile teenusele edastada, siis kontrollitud ja tõeste andmetega on tegemist järgmiste väljade puhul: **nimi** (fullname), **sugu** (gender), **sünnikuupäev** (dob) ja kasutaja **@eesti.ee e-posti aadress** (e-mail). (Paljak, 2008, Ideelabori OpenID serveri (openid.ee) kasutusjuhend arendajale)

Sertifitseerimisekekus

Sertifitseerimiskeskus tegeleb ID-kaardile elektrooniliste sertifikaatide väljastamisega ja hoolitseb rakenduse arendamise ja leviku eest. ID-kaarte väljastatakse koostöös **Kodakondsus- ja Migratsiooniametiga**, kes võtab vastu kaarditaotleja info ja kontrollib selle õigsust. (Sertifitseerimiskeskus, ID-kaart)

On kahte liiki sertifikaate:

- sertifikaat isiku digitaalseks tuvastamiseks, e-posti signeerimiseks ja krüpteerimiseks
- sertifikaat digitaalseks allkirjastamiseks, millega saab sertifikaadi omanik anda digitaalallkirja.

Igasse sertifikaati peavad olema sisse kantud järgmised kohustuslikud andmed: sertifikaadi väljaandja andmed, sertifikaadi omaniku andmed, sertifikaadi kehtivusandmed, sertifikaadipõhised andmed.
Igal sertifikaadil on olemas kehtivusaeg, mis on sertifikaatidesse kantud. Selle aja jooksul on garanteeritud sertifikaadi kehtivusinfo levitamine. Sertifikaadi kehtimahakkamise ajaks on konkreetse sertifikaadi moodustamise kuupäevast järgmine kuupäev ja kellaaeg 00:00. Kehtivuse

lõppemise kuupäevaks on 1100 päeva (umbes 3 aastat) sertifikaadi kehtimahakkamise päevast hilisem kuupäev ja kellaaeg või isikutunnistuse kehtivuse lõpptähtaeg, kui see on varasem. (Sertifitseerimiskeskus, 2004, Sertifikaadid Eesti Vabariigi isikutunnistusel, lk 5)

ID-kaardi sertifikaatide kehtivust saab kontrollida ja vajadusel uuendada koduleheküljel http://www.sk.ee/id-kontroll/. ID-kaardi enda kehtivust saab kontrollida Kodakondsus- ja Migratsiooniameti koduleheküljel http://www.mig.ee/index.php/mg/webquery/queryresults/RpcWebQuery/1373.

Esialgsed sertifikaadid on igale ID-kaardile kantud juba selle tootmise käigus, sertifikaatide aegumisel tuleb neid kaardi omanikul uuendada. Aegunud sertifikaatide uuendamise eest maksab Eesti riik (2004. aasta 3. detsembril Siseministeeriumi ja AS Sertifitseerimiskeskuse vahel sõlmitud lepingu alusel). Seega on ID-kaardi sertifikaatide uuendamine kaardiomanikule tasuta. (Sertifitseerimiskeskus, Sertifikaatide uuendamine)

2.3. Kokkuvõte

Selles osas vaadeldi Ühekordset sisselogimist OpenID ja ID-kaardi abil. Tutvustati OpenID protokolli tööpõhimõtteid ning ülesehitust. Toodi välja OpenID tehnoloogia eeliseid ja puudusi. Tutvustati OpenID kasutaja autentimise käiku ning joonistati selle kohta diagramm.

Mainiti ning lühidalt tutvustati ka Eestis laialt kasutatud ID-kaarti ning sellega seonduvat lisateenust OpenID identiteedi saamiseks ja kasutamiseks. Leidub ka muid Ühekordse Sisselogimise võimaldamiseks ja Liitidentiteedi kasutamiseks suunatud initsiatiive ja projekte. Sellisteks on Bandit aadressil http://www.bandit-project.org/, Higgins aadressil http://www.eclipse.org/higgins/, LID aadressil http://lid.netmesh.org ja kindlasti ka paljud teised. Suures osas on need kas alles algusfaasis, või ei ole neid veel laialt kasutusele võetud.

Kui võrrelda omavahel erinevaid Ühekordset Sisselogimist võimaldavaid tehnoloogiaid, tuleb tõdeda, et suures osas kasutavad need samu Interneti standarte, ning nende toimimispõhimõtted on ka päris sarnased. Suurem erinevus seisneb aga nende tehnoloogia keerukuse tasemetes, mõningaid tehnoloogiaid saab lihtsamalt rakendada. Lisaks sellele omavad erinevad tehnoloogiad natuke erinevat suunda. Mõned on suunatud ettevõtete ja nende partnerite poolt pakutavate teenuste ühendamiseks, sellisel juhul on tavaliselt vaja neid teenuseid eelnevalt omavahel siduda (Ühekordse Sisselogimise võimaldamiseks on vaja süsteemide vahelist usaldust). Need süsteemid omavad head turvalisuse taset, kuid ka teised rohkem avatumad

lahendused võivad saavutata samalaadset turvalisuse taset. Tihipeale saavad taolised süsteemid pakkuda mitte ainult Ühekordset Sisselogimist, vaid ka mõningaid muid võimalusi. Üheks selliseid on kõigist praegusel hetkel kasutatavatest süsteemi teenustest Ühekordse Väljalogimise võimalus, seda on võimalik realiseerida SAML keele tehnoloogiate kasutamisel. Teised süsteemid on aga kohe algusest peale suunatud mitte ainult suhteliselt kinnistes ettevõtete ja nende partnerite lahendustes kasutamiseks, vaid pigem võimalikult laiale kasutajate hulgale. Üheks selliseks lahenduseks on OpenID, mille arendamisega tegeleb uutele liikmetele avatud kogukond.

Tuleb tõdeda, et mõningaid tehnoloogiaid saab üksteisega koos kasutada. Näiteks: CardSpace ja OpenID. Lisaks sellele on SAML ja OpenID standardid, mis sätestavad informatsiooni edastamist Ühekordset Sisselogimist lubava süsteemi komponentide vahel. Nende toimimiseks on vaja olemasolevat Autentimiskeskust, selleks võib olla kasutatud mõni LDAP tehnoloogial baseeruv lahendus. Juba praegugi mõnede suuremate ettevõtete süsteemid oskavad kasutada mitut erinevat tehnoloogiat korraga. Tulevikus on kindlasti oodata komplektseid lahendusi, mis toetavad suure hulga olemasolevaid standarte.

3. Meenutusteportaali teostamine Plone sisuhaldussüsteemi baasil

3.1. Meenutusteportaali projektist

Arvutite ja Interneti kasutamine on saanud paljude inimeste igapäevaelu märkimisväärseks osaks, kus nad teevad tööd, suhtlevad, otsivad vajalikku informatsiooni jne. Interneti avarustes on võimalik peaaegu igaühele leida endale mingit huvitavat tegevust, selle jaoks on olemas palju erinevaid veebiteenuseid ja veebikeskkondi. Kuid mitte kõigi jaoks ei ole lihtne selgeks õppida arvutite ja Interneti kasutamist. Eriti raskeks võib see osutuda just vanematele inimestele. Selle olukorra parandamiseks on valminud mitu projekti eakatele arvutikursuste organiseerimiseks. Üheks huvitavaks initsiatiiviks võib pidada projekti **Grandparents & Grandsons,** mille raames kaasatakse eakate inimeste õpetamisele noori. Projektiga saab lähemalt tutvuda ametlikus veebis aadressil http://www.geengee.eu. Sellised initsiatiivid on olukorda märkimisväärselt parandanud. Selleks, et eakad inimesed hakkaksid oma uusi teadmisi praktikas kasutama, on vaja pakkuda neile ka mingeid huvitavaid kohti Interneti ruumis. Üheks selliseks huvitavaks ressursiks võib saada Meenutusteportaali projekti raames arendatav ning just eakate inimeste jaoks mõeldud veebiteenus.

Meenutusteportaali projekti teostatakse **Spinno programmi** raames, lisainformatsiooni saab aadressil http://www.tlu.ee/?LangID=1&CatID=2929. Meenutusteportaali projekti raames tahetakse luua veebiportaal, kus kasutajad saaksid oma mälestusi sisestada ning ka teiste mälestustega tutvuda. Teiste inimeste mälestuste otsimiseks luuakse kasutajasõbralik otsing, mille abil saab lihtsal ning mugaval viisil otsida teiste kasutajate jagatud meenutusi vastavalt valitud kriteeriumitele. Lisaks sellele peaks kasutajatel olema võimalik teineteisega suhtlemiseks ning süsteemi kuulutuste lisamiseks.

Meenutusteportaali projekti partneriteks on nii Tallinna Ülikooli struktuurüksused ja töötajad, kui ka teised organisatsioonid. Partnerid Tallinna Ülikoolis: TLÜ Sotsiaaltöö Instituut (prof. Taimi Tulva, Vaike Salveste) , TLÜ Infoteaduste Instituut, TLÜ Ajaloo Instituut, TLÜ Informaatika Instituut, TLÜ Infotehnoloogia osakond. Teised partnerorganisatsioonid ja võimalikud partnerid: Eakate Päevakodud (Poska tn), Eesti Kirjandusmuuseum, Eesti Rahva Muuseum ja nende korrespondentide võrk, Ajalooõpetajate Selts, Piirkondlikud raamatukogud. (Tambaum, 2007)

Portaali eripära

Portaal eristub tavapärasest memuaaride kogumist sellega, et mälestusi sisestatakse lõikudena. Iga lõiguga on seotud ajatempel, kohatempel ja mõned märksõnad. Selle informatsiooni abil saab portaalis luua suure täpsusega päringute tegemise süsteemi, mis annaks häid ning täpseid tulemusi. Vajalikku informatsiooni kätte saamiseks ei ole kasutajal enam vaja läbi töötada sadu meenutusi sisaldavaid artikleid, vaid saab kohe alustada huvitava sisu lugemisega.

Mälestused omavad eaka inimese jaoks väga suurt tähtsust, ning on tema üks suurimaid varandusi ja elumootoreid. Nende esitamine on sellise inimese jaoks üks väga motiveeriv tegevus. Eakad on suures osas innukad oma mälestusi jagama. Kuigi meie kiires elus on tihtipeale probleemiks see, et vana inimese meenutuste vastu piisavalt huvi ei tunne.

Kõiki portaali kasutajaid saab jagada kaheks peamiseks grupiks: infot sisestavad registreeritud kasutajad (tavaliselt eakad) ja teised, kes saavad seda infot kasutada (anonüümsed ehk autoriseerimata kasutajad). Vajaduse korral peaks portaalis olema hulk kasutavaid, kes saaksid eakaid inimesi oma meenutuste sisestamisel aidata (tavaliselt nõuandega). Samas võiksid need kasutajad kontrollida et kõigis sisestatud meenutustes oleks konstruktiivne, faktiline ja huvitav info.

Projekti mõju

Projekt peaks omama mõju eestkätt eakatele inimestele, portaali kasutamise ning teistega suhtlemise protsessi käigus õpivad eakad inimesed arvutit kasutama või parandavad juba olemasolevaid teadmisi ja oskusi. Eakate portaali kasutamise protsessi tulemusena tekib ajaloolise info ja faktide kogu, mis on lihtsalt kasutatav ning kõigile kättesaadav. Eakatel suureneb sotsiaalse kaasatuse tunne, paraneb enesehinnang, suureneb sotsiaalne aktiivsus. Inimestel tekib võimalus üheskoos arutada sisestatud meenutusi ning võrrelda mitme erineva inimese mälestusi samade sündmuste kohta. Kuna ka noorema põlvkonna inimesed saavad sisestatud meenutustega tutvuda, siis peaks seeläbi vähenema põlvkondade vaheline lõhe. Veebis tekib eakate inimeste virtuaalne kogukond, kus nad saavad lisaks meenutuste sisestamisele ka omavahel suhelda, endale uusi tuttavaid ja sõpru leida. Tekkinud virtuaalne kogukond peaks kujunema kommunikatsiooniallikaks eakatega seotud huvigruppidele.

Projekti ettevalmistamise etapp

Projekti ettevalmistuse etapi käigus peeti läbirääkimisi võimalikke partneritega ja huvigruppidega. Portaali ülesehituse ning sisulise struktuuri väljatöötamisel kasutati tulevaste

portaali kasutajate seas läbiviidud intervjuude tulemusi. Kogutud informatsiooni põhjal koostati võimalikke riskide loetelu ning nende riskide maandamise võimalusi. Portaali prototüübi pilootkatsete käigus kogutakse eakate kasutajate käest tagasisidet, mille abil peaks olema võimalik portaali kasutajasõbralikumaks ja paremini kasutatavamaks muuta. (Tambaum, 2007)

3.2. Plone-põhine veebirakendus

Plone on avatud lähtekoodiga kiiresti arenev sisuhaldussüsteem, ametlik veeb asub aadressil http://plone.org/. Plone on loodud **Zope** rakendusena, ametlik veeb asub aadressil http://www.zope.org/. (Pelletier, Shariff, 2005) Zope on sisuhaldussüsteemide, sisevõrkude, portaalide ja teiste rakenduste loomiseks mõeldud avatud lähtekoodiga rakendusserver. Zope on põhiliselt kirjutatud **Python** programmeerimiskeele abil, ametlik veeb asub aadressil http://www.python.org/.

Plone sisuhaldussüsteemi lähtekood vastab **W3C konsortsiumi (World Wide Web consortium)** poolt kehtestatud standarditele. Plone sisuhaldussüsteemi ülesehitus on hästi läbi mõeldud ning funktsionaalsust saab laiendada lisaproduktide installimise kaudu. Vajaduse korral võib kirjutada lisaprodukti, mille abil saab lihtsal viisil Plone portaali välimust muuta. Lisaprodukti abil saab süsteemis olemasolevaid komponente laiendada või välja vahetada ning uusi komponente lisada, kohandades süsteemi vastavalt oma vajadustele. (Aspeli, 2007)

Meenutusteportaali projekti raames kavandatava pilootportaali arendamisega tegeleb Tallinna Ülikooli Haridustehnoloogia keskus. Portaali praegune testversioon on kõigile kättesaadav aadressil http://www.htk.tlu.ee/meenutused. Käesoleva töö autori ülesandeks oli vastavalt etteantud spetsifikatsioonidele programmeerida Meenutusteportaali rakendus. Rakenduse realiseerimise käigus tuli töö autoril tegeleda spetsifikatsioonide täpsustamisega ning vastava portaali struktuuri kavandamisega. Töö autori ülesannetesse ei kuulu Meenutusteportaali kujunduse väljatöötamine ja realiseerimine, sellega tegeleb Haridustehnoloogia keskuse veebidisainer Priit Tammets.

Praegusel hetkel ei ole veel Meenutusteportaali rakendus valmis saanud, sinna tehakse pidevalt muudatusi ja täiendusi. Lähiajal peaksid olema läbi viidud portaali kasutamise katsed eakate inimestega. Portaali arendajad osalevad testimisel ning analüüsivad selle protsessi käiku. Saadud tulemuste põhjal peaks olema võimalik teha portaali lihtsuse, mugavuse ja kasutatavuse kohta järeldusi. Vajaduse korral muudetakse portaali rakendust, et saavutada kõrget kasutajasõbralikkuse taset..

Platvormi valik

Meenutusteportaali projekti raames loodav portaali rakendus põhineb Plone avatud lähtekoodiga sisuhaldussüsteemil. Plone sisuhaldussüsteemi raamistik pakub palju erinevaid kasulikke komponente, mille baasil saab oma enda rakendust kiiresti ja mugavalt luua. Platvorm pakub heal tasemes kasutajate haldust, otsingute teostamise süsteemi ning otsingusüsteemi komponentide muutmise või laiendamise võimalust, lihtsate baaskomponentide põhjal oma enda sisutüüpide loomist (alussisutüüp on juba eelnevalt varustatud teatud metaandmetega), laiendatavaid katalooge (nende abil saab kiiresti teostada otsinguid ning tõsta süsteemi toimimise kiirust), paindlik ja lihtsal viisil laiendatav töövoode (workflow) süsteem, võimalus süsteemi sättimiste muutmiseks, tõlkimismehhanism koos tõlgetega mitmes erinevas keeles ning võimalus erinevate tõlkedomeenide kasutamisel oma enda tõlgete lisamiseks ja muid võimalusi.

Üks süsteemi eeliseid on mugav ning mitmetasemeline süsteemi administreerimise graafiline liides:

- tavaliseks igapäevaseks süsteemi haldamiseks saab kasutada Plone graafilise liidesega integreeritud administraatorite ja haldurite jaoks mõeldud lisafunktsionaalsust, mida on väga lihtne ja mugav kasutada; liides kasutab portaali keelt
- keerukamateks süsteemi haldamisülesanneteks saab kasutada **Zope Haldusliidest (Zope Management Interface, ZMI)**; ZMI liides on ingliskeelne ning pakub võimalust muuta peaaegu kõiki portaali sättimisi; vajaduse korral võib selle abil kiiresti muuta portaali visuaalse osa elementide koode ilma produkti enda koodi muutmata ja rakendusserveri taaskäivituseta.

Eelnevalt oli töö autoril juba kogemus Plone baasil suuremate ning väiksemate veebirakenduste loomisel. Üks huvitavaid ning praegu juba reaalselt kasutatavaid rakendusi on **LeMill** portaal, mis on avatud veebipõhine kogukond õpimaterjalide otsimiseks, loomiseks ja jagamiseks. LeMill portaaliga saab tutvuda aadressil http://lemill.net/. LeMill portaal on loodud **Calibrate** projekti raames, rohkem informatsiooni leidub ametlikust veebist aadressil http://calibrate.eun.org. Mõne veebipõhise materjali loomisel võivad osaleda mitu erinevat õpetajat, ning saadud ressurss on kõigile avatud kollektiivne looming. Selline lähenemine soodustab erinevate Euroopa Liidu riikide õpetajate koostööd. Teine huvitav näide on Õpetaja Professionaalse Arengu **ePortfoolio** lahendus. Lisainformatsiooni saab leida projekti veebist aadressil http://www.htk.tlu.ee/opah. Käesoleva töö autor on LeMill portaali arendajate meeskonna liige.

Veel üheks eeliseks oli Plone sisuhaldussüsteemi kolmanda põlvkonna poolt pakutav **OpenID** abil sisselogimise võimalus. OpenID sisselogimise võimaluse lisamise eest Plone sisuhaldussüsteemile on OpenID Fond (OpenID Foundation) selle sisuhaldussüsteemi arendajatele välja maksnud 5000 USA dollarit auhinnaraha. (OpenID.net, OpenID Foundation awards first code bounties.)

Portaali ülesehitus

Meenutusteportaali struktuuri kavandamisel lähtuti kasutajasõbralikkuse ning lihtsuse põhimõtetest, sest portaali kasutajateks peavad saama eakad inimesed. Portaali kasutamise alustamiseks oleks eakal inimesel vaja teada arvutikasutamise põhimõtteid ning osata Interneti kasutada. Lisaks sellele võiks teha kiiret sissejuhatavat kursust, mille jooksul saaks portaali funktsionaalsuse põhimõtteid selgeks teha ning kogu rühmaga proovida portaali funktsionaalsust kasutada.

Erinevad ülesehituse viisid

Iga rakenduse realiseerimiseks on mitu erinevat viisi. Ka Meenutusteportaali ülesehituse kavandamise puhul oli valida mitme erineva lahenduse seast, kaks võimalikku suunda olid:

- kõikide portaali lisatavate objektide hoidmine ühes või mitmes põhikaustas; vajalikke lisavõimaluste realiseerimisel kasutada tsentraliseeritud hoidlate süsteemi,
- igale portaali kasutajale luuakse kodukaust, kus hoitakse kõiki tema poolt lisatud objekte; lisavõimaluste realiseerimisel kasutatakse kasutaja kodukausta kogu vajalikku informatsiooni hoidmiseks.

Igal lähenemisel on omad head ja vead. Esimese tsentraliseeritud arhitektuuriga variandi puhul oleks võimalik vabaneda kasutajate kudukaustade süsteemist, selle abil võiks muuta tulevase portaali kasutamist lihtsamaks lõppkasutajate jaoks. Veel üheks eeliseks oleks võimalus kasutada Plone sisuhaldussüsteemi OpenID sisselogimise moodulit peaaegu muutmata kujul. Samal ajal muudaks see palju keerukamaks portaali realiseerimiseks vajalikku koodi taset. Kuid kõige tõsisemaks probleemiks oleks jõudlus. Kui ühes kohas hoitakse suure osa portaalis olevast sisust, siis suure hulga sisuobjektide tekkimisel hakkab see mõjutama kogu süsteemi toimimise kiirust. Selle variandi puhul oleks palju raskem teostada kasutajate poolt lisatud sisu haldamist, mis võiks tekitada palju probleeme süsteemi haldurite jaoks. OpenID standardlahenduse kasutamise puhul oleks selle abil sisseloginud kasutajate haldus praktiliselt võimatu.

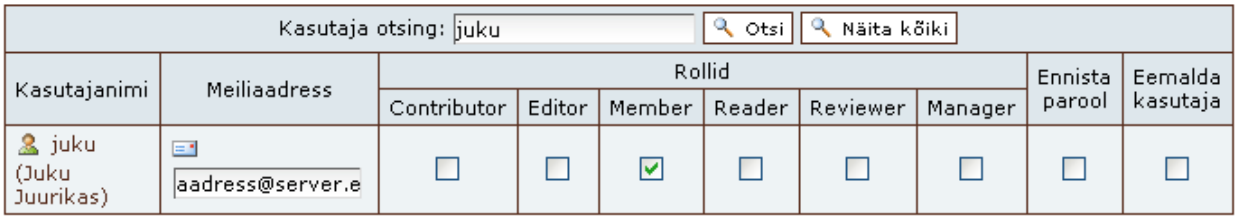
Teine variant võimaldaks mugava kasutajate haldamise süsteemi kasutamist, lihtsamat konkreetse kasutaja poolt lisatud sisu haldamist, vähendada jõudluse probleemide tekkimise tõenäosust. Samal ajal on aga vaja tulevastele portaali kasutajatele tutvustada kodukaustade

süsteemi. Lisaks sellele ei ole võimalik olemasoleva OpenID sisselogimise mooduli muutmata kujul kasutada, vaid tekib vajadus mooduli funktsionaalsuse muutmiseks ja laiendamiseks. Koodi keerukuse tase ei oleks selle teise variandi puhul palju madalam.

Otsuse langetamisel võttis antud töö autor arvesse kõik eelpool mainitud erinevate lähenemiste eeliseid ja puudusi ning arvestas ka eelneva taoliste portaalide loomise kogemusega. Meenutusteportaali realiseerimisel otsustati kasutada teist varianti, kus igal kasutajal on oma isiklik kodukaust.

Kasutajad

Portaalil on kaks põhilist kasutajate tüüpi **registreeritud kasutajad** ning **anonüümsed kasutajad**. Registreeritud kasutajatel on võimalus saada endale kodukausta ning osaleda portaali sisu loomisel. Anonüümsetel kasutajatel on võimalik tutvuda portaali sisuga, teostada otsinguid ning kasutada muud sisuga tutvumiseks mõeldud funktsionaalsust. Plone sisuhaldussüsteem pakub mugava ning lihtsa viisi olemasolevate kasutajate haldamiseks. Joonisel 10 on näidatud registreeritud kasutajate haldamise vorm.



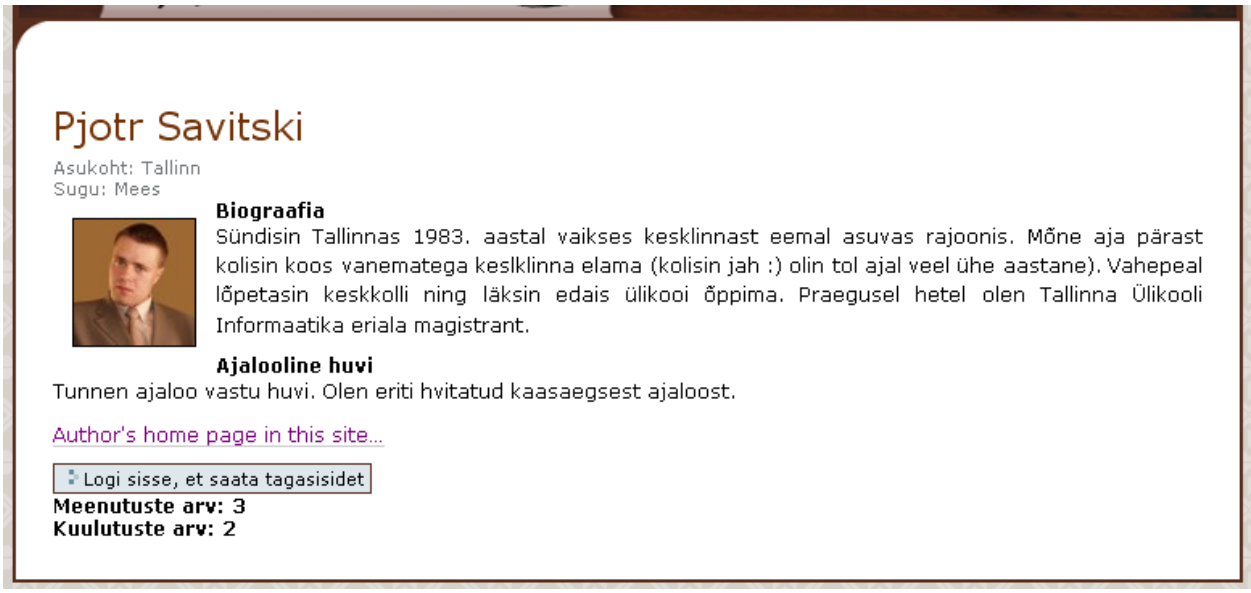
Joonis 10. Registreeritud kasutajate haldamine.

Kasutaja haldamisvormi abil saab teostada vajalikke kasutajate otsinguid kasutajanime järgi, näha kõiki portaalis registreeritud kasutajaid, anda teatud kasutajatele erinevaid rolle, eemaldada kasutajaid ning ennistada paroole. Joonisel 10 on näha, et igal registreeritud kasutajal võib olla mitu erinevat rolli. Iga portaali registreeritud kasutaja saab automaatselt portaali liikme (member) rolli. Selle rolli abil on tal õigus saada süsteemi poolt tekitatud kodukausta ning hiljem sinna midagi lisada. Veel üheks kasutaja rolliks on haldur (manager), selle rolli abil saab teatud kasutajale anda portaali haldamiseks vajalikke õigusi. Plone sisuhaldussüsteem annab võimaluse vajaduse korral uusi rolle lisada või muuta olemasolevate rollidega kaasnevaid portaali erinevate funktsionaalsuste kasutamise võimalusi. Hetkeseisuga kasutatakse Meenutusteportaalis ainult kahte rolli liige ja haldur.

Kasutaja profiil

Igal registreeritud kasutajal on portaalis võimalus täita oma isikliku kasutaja profiili. Profiilis sisestatud andmete abil luuakse kasutaja jaoks portaalis tema leht, kus kõik teised kasutajad

saavad seda informatsiooni lugeda. Joonisel 11 võib näha kuidas kuvatakse portaali kasutaja isiklikku lehte anonüümsele kasutajale.



Joonis 11. Portaali kasutaja isiklik leht.

Vajaduse korral saab üks portaali registreeritud kasutaja teise portaali registreeritud kasutajaga kontakteeruda, selleks kasutatakse kasutajalehel oleva vormi. Joonisel 11 on näha, et anonüümsel kasutajal ei ole võimalust selle funktsionaalsuse kasutamiseks. Vormi abil võib saata adressaadi e-posti aadressile kirja. Kasutaja profiilis saab sisestada oma isiklikke andmeid, kirjeldada oma biograafiat ja ajaloolist huvi. Lisaks sellele on olemas võimalus enda fotot üles laadida. Kasutaja profiil on tehtud Plone süsteemi poort pakutava vaikimisi profiili baasil, kuid seda on muudetud vastavalt Meenutusteportaali vajadustele.

Kasutaja kodukaust

Igal registreeritud kasutajal on Meenutusteportaalis olemas oma kodukaust (kasutaja kodukausta vaatega saab tutvuda joonisel 12). Plone kasutab selleks tavalist, kausta. Kuid vajalikku lisafunktsionaalsuse lisamiseks tuli antud töö autoril luua spetsiaalne objekti tüüp tavalise kausta sisutüübi baasil. Selles kasutas on kasutajal õigus sisestada kahte tüüpi sisu objekte, nendeks on: **Meenutused** ja **Kuulutused**. Mõlemad sisutüübid baseeruvad olemasolevatel sisutüüpidel, kuid on laiendatud vastavalt Meenutusteportaali nõuetele.

Meenutus on portaali sisutüüp, mille abil iga registreeritud kasutaja saab sisestada portaali oma mälestusi. Meenutusteportaali rakenduse kavandamise ja spetsifikatsioonide täpsustamise käigus tekkis vajadus visuaalse kaardirakenduse kasutamiseks. Aina populaarsemaks on saamas Google'i poolt pakutav Google Maps teenus (Google Maps ja Meenutused, lk 54). Kuna tegemist on tasuta, kvaliteetse ning hästi dokumenteeritud teenusega, siis langetati otsus selle

teenuse poolt pakutavaid võimalusi ära kasutada. Üheks Plone sisuhaldussüsteemi eeliseks on mitmete erinevate lisaproduktide olemasolu. Enne oma lahenduse tegema hakkamist otsustas töö autor eelnevalt uurida Google Maps kasutamist võimaldavaid produkte. Uuringu käigus selgus, et eksisteerib juba mitu erinevat produkti, mille abil saab Google Maps teenust Plone portaaliga integreerida. Nende produktide uurimisel selgus, et ainult üks neist pakub Meenutusteportaali kontekstiga sobilikke võimalusi. Selleks on **Florian Schulze** poolt loodud **Maps** produkt, Maps produkti kirjeldusega saab tutvuda aadressil http://plone.org/products/maps/. Kuna olemasolev Maps produkt ei vastanud täielikult uue portaali vajadustele, siis tuli seda muuta. Teised samas rakendusserveris olevad portaalid võivad olemasolevat Maps produkti kasutada, seega otsustas töö autor luua selle baasil uue **MapsMX** nimelise produkti. MapsMX produkt vastab täielikult Meenutusteportaali vajadustele ning on tihedalt integreeritud portaali funktsionaalsustega. Uues produktis on vähe muudetud Google Maps teenusega suhtlemiseks kasutatav koodi osa. MapsMX produktis kasutatakse oma enda tõlkimisdomeeni, kuvamis- ja muutmisvormide funktsionaalsus on laiendatud, Meenutuse sisutüübi (loodud GeoLocation sisutüübi baasil) ja muid Meenutusteportaali spetsiifilisi funktsionaalsusi. Meenutuse sisestusvormil on punaste ruudukestega näidatud sisestamiseks kohustuslikud väljad. Kui üks nendest väljadest on tühi, siis ei saa seda meenutust salvestada. Salvestusnuppu vajutamisel näidatakse kasutajale kohustuslikke välju, mida on tal veel vaja täita.

Igal meenutusel on teatud hulk välju:

- **Pealkiri** - meenutuse peakiri, kus kasutaja nimetab meenutuse teemat.
- **Kirjeldus** - piiratud pikkusega lühikirjeldus, mis peaks tutvutama meenutuse sisu tulevastele lugejatele.
- **Ajavahemik** - meenutuses kirjeldavate sündmuste toimumisaeg. Perioodid on näidatud kümne aasta kaupa.
- **Meenutuse autor** - täidetakse ainult sel juhul, kui tegemist on vahendatud meenutusega.
- **Koht** - kasutaja saab sisestada otsingusse meenutuse toimumiskohta. Seda näidatakse kaardil. Kui vajalikku kohta ei saa leida, siis tuleb sisestada lähima naaberasula nime. Pärast saab kaardil olevat sümbolit hiirega õigesse geograafilisse punkti nihutada. Selle funktsionaalsuse võimaldamiseks kasutatakse Google Maps kaarditeenust (Google Maps ja Meenutused, lk 54).
- **Etapitähis** - igat meenutust saab siduda oma elukaare etapi-tähisega. Sellisel juhul tähistatakse kaardil meenutusi erineva värvi sümbolitega. Erinevaid võimalikke etappe on viis: lapsepõlv, noorus, keskiga, pensionipõlv ja vahendatud meenutus.

- **Meenutuse tekst** - selle suurema tekstikasti saab kasutaja sisestada on meenutuse teksti. Meenutuse teksti saab otse veebilehel sisestama hakata, teksti küljendamise otstarbeks kasutatakse veebipõhist graafilist redaktorit.
- **Kategooriad** - igat meenutust saab siduda portaali loojate poolt pakutavate kategooriatega. Selleks on kasutajal vaja valida sobivad kategooriad pakutavate nimekirjast.
- **Seonduvad meenutused** - kasutaja saab valida teisi selle meenutusega seonduvaid meenutusi.
- **Asukoht** - kasutaja sisestab siia täpse asukoha nime.
- **Kommenteerimisluba** - kasutaja saab lubada kommenteerimist, vaikimisi on kommenteerimine keelatud.

Kuulutus on portaali sisutüüp, mille abil saavad portaali registreeritud kasutajad mingeid kuulutusi lisada. Kuulutusi saavad näha teised portaali kasutajad. Kuulutusel on ainult kaks välja: **Pealkiri** ja **Kuulutuse tekst**. Kuulutuse teksti pikkus on piiratud. Kõiki avalikustatud kuulutusi saab näha kuulutuste lehelt. Kasutaja saab oma kuulutusi hallata oma kasutaja kaustast.

Sõprade nimekiri

Iga registreeritud kasutaja saab moodustada teiste portaali registreeritud kasutajatest oma sõprade nimekirja. Kasutaja sõprade nimekirja saab näha joonisel 12. Nimekirja lisatud kasutajaid näidatakse kasutaja kodukausta vasakul olevas menüüs. Iga kasutaja täisnimi on viide selle kasutaja isiklikule lehele portaalis, kus saab tutvuda kasutaja poolt sisestatud informatsiooniga. Sõprade nimekirja haldamiseks saab kasutada allaolevat nuppu. Haldamine on väga lihtne ning intuitiivne. Nimekirja haldamisvormil näidatakse kõiki portaali kasutajaid, nimekirja lisatud kasutajad on märgistatud. Sõbra lisamiseks/eemaldamiseks piisab sellest, et kasutaja märgistab teatud kasutajat või eemaldab märgistuse teatud kasutaja nime eest. Sõpru võivad näha ka teised portaali kasutajad ja külastajad.

Sisutüüpide staatus

Portaali objektidele on rakendatud lihtne avalikustamise skeem, mille järgi igal portaali lisataval objektil võib olla kaks erinevat staatust: **avalik** ja **peidetud**. Iga objekt on esialgu peidetud, et kasutaja saaks vastavalt vajadusele oma Meenutust või Kuulutust täiendada. Kui objekt on valmis, siis saab kasutaja käivitada avalikustamise protsessi. Peaaegu kohe muutub objekti staatus avalikuks. Kõik avalikus staatuses objektid on igale portaali kasutajale nähtavad (kaasa arvatud anonüümsed kasutajad või külalised). Peidetud staatuses objektid on aga nähtavad ainult

objekti omanikule ja portaali administraatoritele. Vajaduse korral saab kasutaja oma meenutuse või kuulutuse staatust muuta jälle peidetuks.

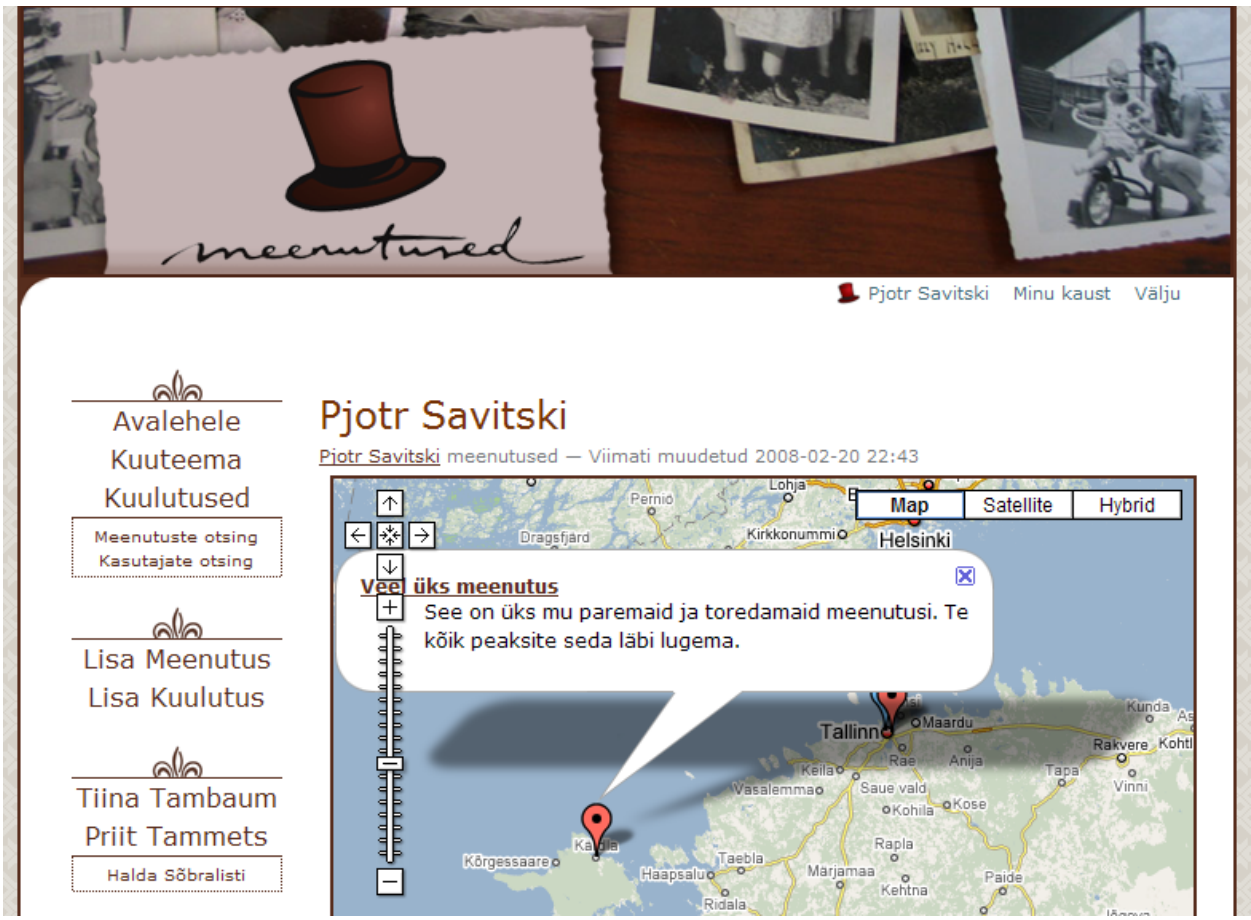
Google Maps ja Meenutused

Meenutusteportaalis kasutatakse Google Maps kaarditeenust. Teenusega saab tutvuda aadressil http://maps.google.com/. Tegemist on hästi dokumenteeritud ning tasuta teenusega, mida saab suhteliselt lihtsal ja mugaval viisil oma rakenduses ära kasutada. Teenuse kasutamise alustamiseks on vaja eelnevalt registreerida spetsiaalse võtme (API Key). Võti on seotud portaali veebiaadressiga (URL), ning selle võtme abil saab portaal Google Maps teenusega suhelda.

Seda teenust kasutatakse Meenutusteportaalis kahel viisil:

1. Iga kasutaja saab meenutuse sisestamisel otsida vastavat geograafilist punkti. Kui aga punkti otseselt leida ei õnnestu, siis saab kasutaja ise kaardil olevat sümbolit hiirega õigesse geograafilisse punkti nihutada. Hiljem näidatakse väikest kaardikest, mis annab inimestele lihtsamal viisil ettekujutuse mis kohaga tegemist, saab vaadata naabrust. Vajaduse korral on kaardi mastaapi võimalik suurendada või vähendada.
2. Iga kasutaja kausta vaates on näha suuremat kaarti (joonis 12), kus on vastavalt etapitähisele (erinevate värvidega) näidatud kõik selle kasutaja poolt lisatud meenutused. Kui meenutuse sümboli peal vajutada, siis kuvatakse selle meenutuse kohta pealkiri ja lühikirjelduse informatsiooniga element. Süsteem proovib kaarti nii mastaapida, et kõik meenutused mahuksid kaardil nähtava osa sisse.

Joonisel 12 võib näha ühe kasutaja kodukausta vaates oleva kaardi, kus näidatakse selle kasutaja poolt loodud meenutusi. Meenutuse ikoonile saab vajutada ning lugeda meenutust kirjeldava informatsiooni. Meenutuse pealkiri on viide täispikkuses meenutuse tekstile. Tulevikus on plaanis lisada portaali ühe üldise kaardi, kus näidatakse kõiki portaalis avaldatud meenutusi. Kaardi kasutamise lihtsustamiseks võimaldatakse vajalikke tulemuste filtreerimist.



Joonis 12. Kasutaja kodukausta vaade.

Meenutuste ja kasutajate otsing

Portaalis on olemas meenutuste ja kasutajate otsinguks mõeldud vormid, mille abil saab kiiresti ning mugavalt teostada täpseid otsinguid. Kasutajate otsinguvormi kasutatakse muutmata kujul. Meenutuste otsinguvorm on loodud töö autori poolt Plone standardse otsinguvormi baasil, kus on mõningaid kriteeriume muudetud ning mõningaid lisatud (ajavahemik, autori nimi).

Kasutajate otsinguvormil saab sisestada kolm erinevat kriteeriumit, nendeks on: **kasutajanimi**, **e-posti aadress** ning **täisnimi**. Otsingu tulemuseks on leht, kus kuvatakse ka kasutajate poolt lisatud pilte.

Meenutuste otsingu teostamisel saab kasutaja otsida mitmete kriteeriumite põhjal:

- **Otsi teksti** – vastavaid sõnu otsitakse objektide sisust, pealkirjast ning kirjeldusest. Mitme sõna otsingut saab kombineerida AND ja OR spetsiaalsete fraaside kasutamisel.
- **Pealkiri** – otsitakse vastava pealkirjaga objekte.
- **Ajavahemik** – otsitakse kõiki valitud ajavahemikuga seotud meenutusi. Vaikimisi otsitakse kõiki ajavahemikke.
- **Kategooriad** – otsitakse vastavate kategooriatega meenutusi. Saab valida kõikide portaalis olemasolevate kategooriate seast. Lisaks sellele saab märkida: vastab kõigile või vastab mõnele.

- **Autori nimi** – otsitakse mingi konkreetse autori poolt loodud meenutusi. Otsinguks saab kasutada eesnime, perekonnanime või täisnime.
- **Uued objektid alates** – otsitakse meenutusi, mis olid lodud teatud ajahetkest alates.

Otsingu tulemuste vormil kuvatakse kasutajale ka informatsiooni otsingus kasutatavate tunnuste väärtustega. Selle informatsiooni abil saab iga kasutaja näha otsingukriteeriume, millele vastavad leitud meenutused.

Portaali otsingute kiirendamiseks kasutatakse **Portaali Kataloogi (Portal Catalog)**. Tegemist on sisuhaldussüsteemi komponendiga, mis on ehitatud kataloogi põhimõtetel. Iga portaalis loodud sisuobjekti jaoks lisatakse selle kataloogi kirje, millega on seotud üldine info selle objekti kohta (näiteks: pealkiri, identifikaator, lühikirjeldus, loomise kuupäev, muutmise kuupäev, autor ja muu). Kataloogi lisatavat informatsiooni on võimalik süsteemi loojal mugavalt laiendada (nii koodi poole pealt, kui ka ZMI kaudu). Kataloogi laiendamisel tuleb silmas pidada, et kataloogi tohib lisada ainult piiratud mahuga informatsiooni. Vastasel korral ei pruugi kataloog hästi toimida ning võimaldada kiiret andmete tagastamist.
Meenutuste otsingu võimaldamiseks on kataloogi lisatud: ajavahemik ja autori täisnimi. Lisaks nendele lisas antud töö autor kataloogi ka mõningaid muid välju. Kataloogid võimaldavad kasutada mitu erinevat otsingukriteeriumit, mis võimaldab ka kõige keerukamate otsingute teostamist. Kataloogi abil on võimalik kiiresti saada teatud objekti kohta andmeid, mis on suure ja keeruka süsteemi puhul äärmiselt oluline.

4. OpenID põhise sisselogimise realiseerimine Meenutusteportaalis

4.1. OpenID Plone peal

Internetis on hetkel palju huvitavaid ning kasulikke veebiteenuseid, mida paljud inimesed aktiivselt kasutavad oma igapäevaelus. Suurem osa nendest süsteemidest nõuab inimeselt kasutajakonto loomist. Tihtipeale on igas süsteemis kasutajal oma kasutajatunnus ja salasõna, mida tuleb meeles pidada. Pikka aja jooksul tekib neid salasõnu ja paroole nii palju, et nende haldamine muutub inimese jaoks päris keeruliseks.

Kuna Meenutusteportaali peamisteks kasutajaskonnaks on eakad inimesed, siis nende jaoks võib muutuda mitmes kohas kasutajakontode haldamine tõsiseks probleemiks. Eestis on juba pikka aega kasutusel olnud ID-kaart ning tänapäeval selle kasutusevaldkond aina laieneb. Suurem osa Eesti elanikkonnast omavad juba ID-kaarte ning kasutavad neid riigi ja eraettevõtete veebiteenuste kasutamiseks. ID-kaart on väga turvaline identiteedi tõestamise viis, seega oleks mõistlik selle võimalusi Meenutusteportaalis kasutajate autentimisel ära kasutada.

Projekti autorid ning portaali loojad on arvestanud sellega, et mõnede eakate inimeste jaoks võib ID-kaardi kasutamise osutuda suhteliselt keerukaks. Võimalike probleemide vähendamise jaoks luuakse heal tasemel abimaterjale, kus lihtsal ja arusaadaval viisil seletatakse ID-kaardi kasutamisel sisselogimise protsessi. Vajaduse korral saab korraldada eakate inimeste jaoks kursuseid.

Ideelabor tegeleb juba mõnda aega OpenID.ee nimelise teenuse arendamisega, mis võimaldab kasutada OpenID tehnoloogiat käsikäes Mobiil-ID ja Eesti ID-kaardiga. Ühe eesti kodaniku OpenID tunnus võib olla koostatud sellisel kujul: **https://openid.ee/eesnimi.perekonnanimi**. Eesnimedes ja perenimedes olevaid täpitähti asendatakse nii, et saaks standardile vastava veebiaadressi moodustada. Oma OpenID.ee identifikaatori teada saamiseks on kõige lihtsam minna aadressile **https://openid.ee/auth/login,** ning sisse logida oma ID-kaardi või Modiil-ID abil. Siis saab iga inimene oma OpenID identiteedi tunnust näha ning edaspidi kasutama hakata.

Plone sisuhaldussüsteemi kolmanda põlvkonna (versioonid 3.x) rakendused võimaldavad OpenID kasutamist süsteemi sisse logimisel. (Aspeli, 2007) Olemasolev lahendus toetab OpenID Autentimise versiooni 2.0. Selleks vajalik Plone-poolne funktsionaalsus on loodud

sisuhaldussüsteemi arendajate meeskonna liikmete poolt. Kogu funktsionaalsus baseerub Python'i OpenID lisapakettidel. Neid saab leida sellelt aadressil http://www.openidenabled.com/python-openid/. Antud töö autor uuris Plone lahenduse võimalusi ning kasutatavust Meenutusteportaali kontekstis.

OpenID võimalusi kasutatava Plone portaali loomine on suhteliselt lihtne. Selleks on vaja järgida Plone sisuhaldussüsteemi lähtekoodi CMFPlone kataloogis INSTALL.txt failis olevaid käske. Plone sisuhaldussüsteemi saab alla laadida mitme erineva paketti kujul aadressil http://plone.org/products/plone. Mõned paketid paigaldavad nii Plone süsteemi ennast, kui ka kõiki selle töö käivitamise jaoks vajalikke lisakomponente. Teine võimalus on aga Iga platvormi jaoks sobiv lähtekoodiga pakett. Selle paketti kasutamiseks on juba eelnevalt vaja süsteemi paigaldada Python ja Zope (allalaadimisviite all olevast lühikirjeldusest saab leida vajalikke versioonide numbreid).

Kui kõik komponendid on paigaldatud ning Zope rakendusserver on käivitatud, saab ZMI liidese kaudu luua uue Plone portaali, mis kohe võimaldab OpenID sisselogimist (tuleb valida vastava profiili). Teiseks võimaluseks oleks juba olemasolevas Plone portaalis lisada OpenID produkt (laiend). Kui produkt on edukalt paigaldatud, siis lisaks olemasoleva portaali kasutajanime ja parooliga sisselogimisele saab nüüd portaali siseneda ka OpenID identiteedi abil. Joonisel 13 saab näha Plone portaali esilehele tekkinud OpenID sisselogimiseks kasutatava vormi.

Joonis 13. OpenID sisselogimisvorm.

Esialgu ei saa OpenID abil sisseloginud kasutajad mingeid lisavõimalusi juurde, sest need on **Autenditud (Authenticated)** virtuaalse gruppi liikmed. Selle gruppi liikmetel ei ole esialgu portaali liikme rolli. Autenditud grupile saab määrata teatud rolle, mille abil selle liikmed saavad võimaluse võtta osa portaalis käivatest diskussioonidest, lisada kommentaare või isegi sisu. Kõike seda saab lubada nendele kasutajatele kas globaalselt kogu portaalis, või lokaalselt mingis teatud kaustas ja selle kausta alamkaustades. (Vladimirskiy, 2007)

OpenID standardlahendus ja Meenutusteportaal

Hetkel olev OpenID lahendus ei vasta kõikidele Meenutusteportaali poolt esitatavatele nõuetele:

1. Hetkeseisuga ei saa võimaldada Plone portaali registreeritud kasutajatele siduda oma kasutaja profiiliga mitte ühtegi OpenID identifikaatorit. Sellisel viisil ei saa mingi registreeritud kasutaja teostada sisselogimist oma OpenID abil.
2. Vastavalt OpenID põhimõtetele saab praegu portaali sisselogimisel kasutada kõiki Identiteedi pakkujate OpenID identiteete. Pole võimalik piirata lubatud OpenID pakkujate hulka, mis on aga meenutusteportaali kontekstis vajalik.
3. Igal Meenutusteportaali registreeritud kasutajal peaks olema oma kodukaust. Katsete jooksul selgus, et hetkeseisuga olemasoleva süsteemi abil ei saa OpenID kasutaja jaoks kodukausta luua. OpenID identiteediga sisseloginud isiku kasutajatunnuseks on tema OpenID identiteedi URL. Sellest ei ole võimalik luua kasutaja kausta ID, mis vastab süsteemis kehtestatud reeglitele.
4. Kõiki OpenID abil sisseloginud kasutajaid ei saa mugavalt hallata, andes teatud kasutajale lisaõigusi. Vaid kõigi nende kasutajate privileegide ja õiguste haldamine toimub läbi Autenditud virtuaalse gruppi haldamist.

Läbiviidud uuringu tulemuste põhjal tegi antud töö autor järelduse, et olemasoleva Plone sisuhaldussüsteemi OpenID sisselogimist võimaldav laiendus ei vasta Meenutusteportaali vajadustele. Vajalikku tulemuse saamiseks on vaja olemasoleva OpenID sisselogimist võimaldava mooduli baasil luua Meenutusteportaali kriteeriumitele vastav lahendus.

4.2. Meenutusteportaali OpenID lahendus

Eelmises peatükis uuriti olemasoleva OpenID sisselogimist lubava Plone mooduli võimalusi. Uurimise käigus selgus, et olemasolev lahendus ei vasta Meenutusteportaali vajadustele. Töö autor otsustas, et olemasoleva OpenID sisselogimist võimaldava produkti baasil on vaja luua oma laiendatud võimalustega lahendus. Laienduse eesmärgiks on viia OpenID sisseloginime vastavusse Meenutusteportaali vajadustega, samal ajal pidades silmas kasutajasõbralikkuse ning lihtsuse põhimõtteid. Uues lahenduses saab ära kasutada juba toimivat OpenID Identiteedi pakkuja serveriga autentimise mehhanismi, mida pakub hetkel eksisteeriv lahendus. Nagu ka eksisteeriv Plone OpenID laiend, tugineb uus lahendus Python'i OpenID lisapakettidele.

OpenID lahenduse erinevad variandid

OpenID sisselogimise võimaldamiseks Meenutusteportaalis saaks kasutada mitu erinevat lahendust. Valitud lahenduse funktsionaalsus sõltub portaali poolt esitatud nõuetest, kuid oma rolli mängib ka portaali rakenduses kasutusele võetud ülesehitus (Erinevad ülesehituse viisid, lk 49). Töö autor on kaalunud Meenutusteportaali OpenID sisselogimise realiseerimise jaoks kahte võimalikku teed:

- Kasutada olemasolevat OpenID sisselogimise lahendust ning anda Autenditud gruppi kasutajatele liikme (member) rolli.
- Laiendada olemasoleva OpenID sisselogimise laiendi võimalusi, siduda OpenID identiteeti portaali registreeritud kasutajaga.

Esimese variandi realiseerimise jaoks oleks Meenutusteportaalis võimalik kasutada sellist ülesehitust, kus kogu portaali sisu lisatakse ühte kohta. Selline ülesehituse skeem ei osutunud kõige paremaks, ning töö autor valis teist teed. Selle variandi kasutamiseks on halduril vaja eelnevalt portaali vastavalt vajadustele seadistada. Erinevate kasutajakaustade süsteemiga poleks võimalik seda varianti kasutada, kuna hetkel olev süsteem ei võimalda OpenID abil sisseloginud kasutajaid hallata. Hästi toimiva süsteemi ülesehitamine oleks äärmiselt keeruline, kuna iga lisavõimaluse realiseerimise käigus oleks vaja lahendada ebamugava ülesehituse kitsendustest tulenevaid probleeme.

Teine võimalikku realiseerimise variant sobib hästi Meenutusteportaali jaoks valitud ülesehitusega. Kuna OpenID identiteet on seotud portaali kasutajaga, siis on võimalik ka lõppkasutajaid mugavalt hallata. Selle variandi realiseerimisel saab kasutada kahte erinevat kasutajatunnuse loomise viise:

- kasutaja identiteet on tavaliselt kujul **http://openid.ee/eesnimi.perenimi.** Kuna Plone sisuhaldussüsteem ei luba kasutada registreeritud kasutajate nimedes spetsiaalseid sümboleid, siis oleks võimalik viia identiteeti normaalsele kujule ning selle abil luua portaali kasutaja. Edaspidi on portaali kasutaja seotud vastava OpenID identiteediga.
- Koostada kasutajatunnus kasutaja enda eesnimest ja perenimest, vajaduse korral lisada unikaalsuse tagamiseks kasutajatunnuse lõppu numbrit. Kõik täpitähed muudetakse tavalisteks inglise tähestiku tähtedeks.

Esimese võimaluse puhul oleks võimalik tõlgendada OpenID identiteet kasutajatunnuseks ning kasutajatunnus identiteediks. Saadav identiteedi unikaalsus oleks tagatud, kuna OpenID identiteedid on unikaalsed. Plone sisuhaldussüsteemis kasutatakse kasutajatunnust kasutaja kodukausta identifikaatoriks ning mitmes muus kohas, seega ei ole sellisel viisil kasutajatunnuseid eriti mõistlik kasutada.

Teise võimaluse kasutamisel on süsteemi realiseerimine suhteliselt samalaadne. Üheks suureks vaheks on see, et kasutajatunnust luuakse teistmoodi (kasutades ees- ja perekonnanime).

Antud töö autor on valinud OpenID sisselogimise teostamise variandi, kus identiteedi seotakse portaali kasutajaga ning kasutajatunnuse loomisel kasutatakse täisnime.

Valitud variandi teostamine

Vastavalt spetsifikatsioonidele võimaldab Meenutusteportaali OpenID sisselogimise lahendus järgmist funktsionaalsust:

- Kasutaja poolt sisestatud OpenID identifikaatorit kontrollitakse enne autentimise protsessi käivitamist. Lubatakse ainult OpenID.ee poolt kasutavaid identifikaatoreid. Sellega tagatakse Identiteedi pakkuja usaldusväärsust ja heal tasemel turvalisust.
- Iga OpenID abil sisseloginud virtuaalne kasutaja (OpenID URL) on seotud portaali kasutajaga (member). Esmakordsel sisselogimisel süsteem käivitab kasutajakonto loomise protsessi ning seob seda OpenID identiteediga.
- Kuna iga OpenID abil sisseloginud virtuaalne kasutaja on seotud portaali kasutajaga, siis on võimalik kasutajate haldamisel ära kasutada sisushaldussüsteemis olemasolevaid kasutajate haldamise võimalusi.

OpenID identiteedi valiidsuse kontroll

Kuna Meenutusteportaali sisselogimiseks on lubatud kasutada ainult ühe kindla OpenID Identiteedi pakkuja poolt väljastatud OpenID identiteete, siis tekib vajadus sisselogimisprotsessi alguses kontrollida sisestatud identiteeti. Selle jaoks on loodud valiidsuse kontrollmehhanism, mis kontrollib kas sisestatud OpenID URL sisaldab **openid.ee/** elementi. Kui sisaldab, siis tegemist on lubatud identiteediga. Kui aga mitte, siis seda identiteeti Meenutusteportaalis kasutada ei saa. Portaal kuvab kasutajale vastava teade.

OpenID identifikaatori ja kasutaja sidumine

OpenID identifikaatori (virtuaalne kasutaja) ja kasutaja omavaheliseks sidumiseks on portaali kasutajatehaldus laiendatud lisamooduliga. Muudatusi tehakse kogu lisafunktsionaalsust kandva lahenduse portaali paigaldamisel. Kasutaja haldusesse lisatud moodul hoiab kõiki OpenID abil sisseloginud virtuaalsete kasutajate ja tavakasutajate vahelisi seoseid. Kuna OpenID identifikaator ja kasutajatunnus on mõlemad unikaalsed, siis saab mugaval viisil luua nende vahelist seost. Lisamoodul hoiab informatsiooni sõnastiku (dictionary) vormis, kus võtmeks on OpenID ja väärtuseks on kasutajatunnus:

{’https://openid.ee/pjotr.savitski’:’pjotrsavitski’, ’https://openid.ee/juku.juurikas’:’jukujuurikas’, ’https://openid.ee/mari.maasikas’:’marimaasikas2’, …}

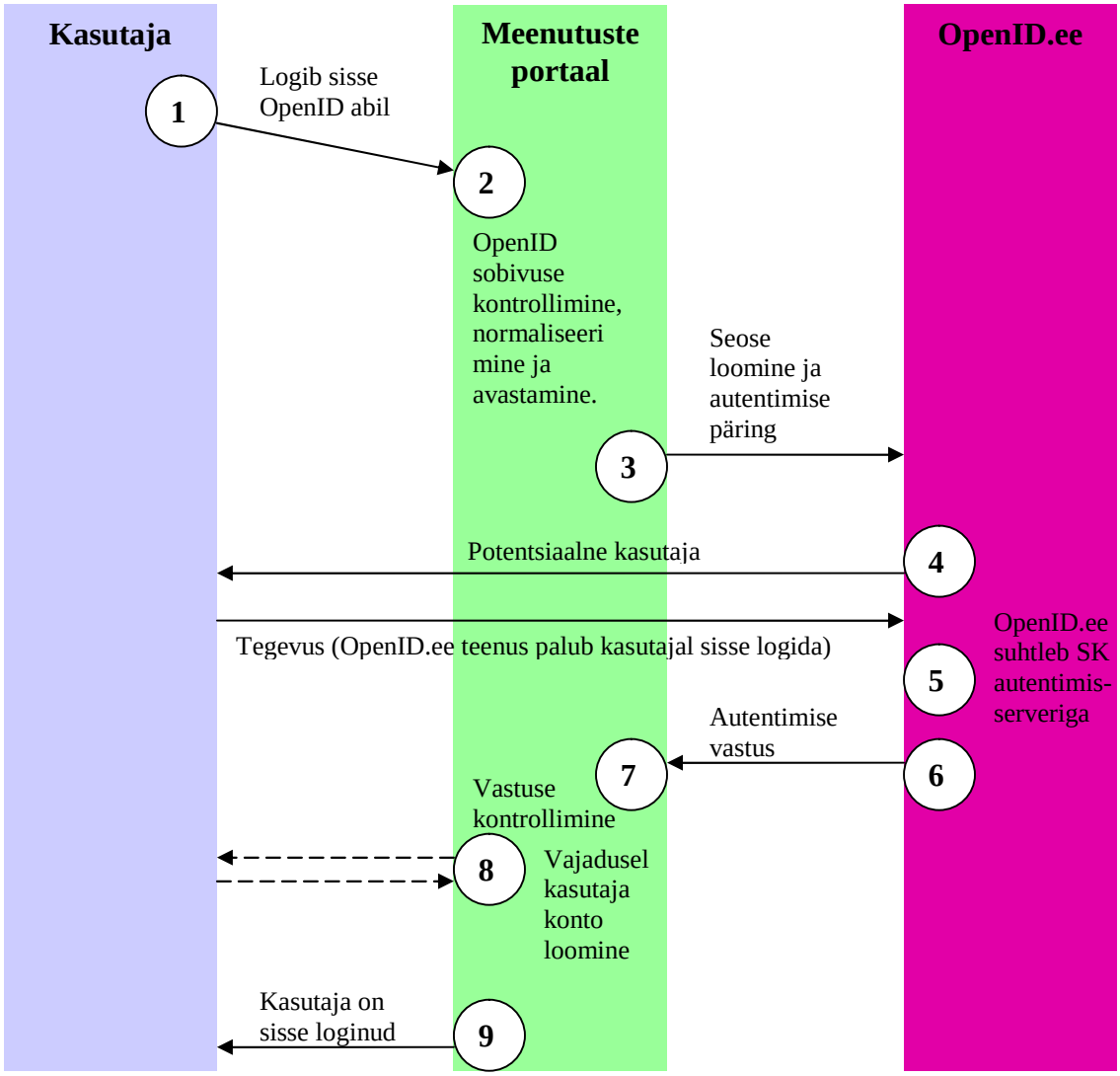
Sõnastiku kasutamisel on mitu eelist. Üheks töö autori poolt ärakasutatud eeliseks on kiire võtme abil vastava väärtuse kättesaamine. Teiseks, võimalus saada kõik selle sõnastiku võtmed korraga ning teostada nende seas otsingu. Seda funktsionaalsust kasutatakse esmakordselt sisseloginud

virtuaalse kasutaja äratundmiseks – kui konkreetset OpenID identifikaatorit ei ole võtmete seas, siis on tegemist esmakordse sisselogimisega.

Esmakordsel OpenID identifikaatoriga sisselogimisel suunatakse kasutajat registreerimisvormile. Registreerimisvormile pääsevad ligi ainult autenditud kasutajad ja ainult esmakordsel sisselogimisel, sellisel viisil on loodud kaitse selle funktsionaalsuse kuritarvitamise vastu. Kasutaja sisestab registreerimisvormile oma eesnime, perekonnanime ja e-posti aadressi. Nende andmete abil luuakse portaali kasutaja, kellega saab edaspidi seotud vastav OpenID. Kasutajanime pannakse tavaliselt kokku kasutaja ees- ja perekonnanimest (kõik täpitähed asendatakse nii, et kasutajatunnus vastab portaali kasutajatunnuse poliitika reeglitele). Kui on juba olemas kasutajad samalaadse ees ja perekonnanimega, siis lisatakse kasutajatunnuse lõppu number (sellisel viisil tagatakse kasutajatunnuse unikaalsust). Kui kasutajakonto loomise protsess on lõppenud, siis seotakse tekitatud kasutajatunnus kasutaja OpenID identifikaatoriga.

Kui uus kasutajakonto on loodud või oli juba eelnevalt selle OpenID identifikaatoriga seotud kasutaja olemas, siis käivitatakse sisselogimise protsessi viimase etapi. Selle etapi käigus vahetatakse OpenID abil sisseloginud virtuaalne kasutaja selle identiteediga seotud tavalise kasutaja vastu. Protsessi lõpus saab portaali kasutaja sisse logitud oma kasutajakontoga, sellel kasutajal on olemas kodukataloog (kasutaja kodukaust) ja võimalus kogu meenutusteportaali funktsionaalsust kasutamiseks. Seda kasutajat on nüüd võimalik mugaval viisil hallata, mõnedele kasutajatele saab vajaduse korral määrata halduri õigusi.

Joonisel 14 on näidatud diagramm, mis kajastab Meenutusteportaali spetsiifilise OpenID lahenduse poolt lisanduvaid sisselogimise protsessi iseärasusi.



Joonis 14. Meenutusteportaali OpenID sisselogimise lahendus.

1. Inimene siseneb Meenutusteportaali avalehele ning otsustab OpenID abil sisse logida.
2. Meenutusteportaal kontrollib kas sisestatud OpenID vastab portaali nõuetele. Portaali saab sisse logida ainult OpenID.ee Identiteedi pakkuja teenuse OpenID identiteetidega. Teostatakse ka sisestava identiteedi normaliseerimist ning avastatakse Identiteedi pakkuja aadressi.
3. Luuakse seost Identiteedi pakkuja teenusega ning saadetakse kasutaja autentimise päring.
4. Kasutajat suunatakse Identiteedi pakkuja poole (OpenID.ee teenus). Kasutajal on vaja teenuse kasutamiseks logida sisse ID-kaardi või Mobiil-ID abil.
5. OpenID.ee teenus suhtleb Sertifitseerimiskeskusega. Kui kasutaja on sisestanud õigeid autentimisandmeid, siis saab kasutaja alustada teenuse kasutamist.
6. Kasutaja peab otsustama, kas ta lubab Identiteedi pakkujal saata Meenutusteportaalile tõendit või mitte. Selle tõendi abil saab Meenutusteportaal kontrollida, kas kasutaja on

selle OpenID identiteedi omanik või mitte. Identiteedi pakkuja saadab Meenutusteportaali poolt esitatud päringule vastuse.

7. Meenutusteportaal kontrollib Identiteedi pakkuja poolt saadetud vastust. Positiivse vastuse korral saab virtuaalne kasutaja portaali oma identiteediga sisse logitud.
8. Meenutusteportaal kontrollib kas selline OpenID on seotud mõne portaalis olemasoleva kasutajakontoga. Kui kasutajakonto on juba olemas, siis logitakse kasutajat automaatselt sisse vastava kontoga. Kui see isik külastab portaali esmakordselt, siis suunatakse teda kasutajakonto loomise vormile (kasutajal on vaja sisestada oma täisnime ja e-posti aadressi). Sisestatud informatsiooni abil luuakse kasutajale portaalis kasutajakonto, kasutajanime genereerimisel kasutatakse täisnime, kasutajakontoga on seotud vastav OpenID. Virtuaalse gruppi kuuluv kasutaja logitakse välja ning toimub automaatne sisselogimine OpenID identifikaatoriga seotud kasutajakontoga. Esmakordsel sisselogimisel luuakse kasutajale kodukaust.
9. Isik on Meenutusteportaali edukalt sisse loginud.

Loodud OpenID sisselogimise mooduli laiendus lahendab eelmises peatükis välja toodud tavalise Plone lahenduse kitsendusi. Laiendus vastab Meenutusteportaali vajadustele, võimaldades kasutada OpenID.ee Identiteedi pakkuja poolt võimaldatud ID-kaardiga sisselogimist.

4.3. Järeldused

OpenID on väga võimas tehnoloogia, mida saab mugaval viisil kasutada Ühekordse sisselogimise realiseerimisel. Autentimise protsess on OpenID spetsifikatsioonide poolt reglementeeritud, seega suures osas on igal pool praktiliselt sama. Enamasti on vahet rakenduse poolsel lahendamisel, kuidas kokku sobitada OpenID abil sisseloginud kasutajad olemasoleva kasutajakontode ja kasutajate haldamise süsteemiga.

OpenID kasutamisel tuleb kindlasti rakendada kõikvõimalikke turvameetmeid ning kasutada viimase, 2.0 versiooni poolt pakutavaid lahendusi. Sellisel viisil saab lahendada võimalikke rünnakute probleeme. Koos OpenID tehnoloogiaga saab kasutada ka teisi. Eelnevalt mainitud lahenduses kasutati OpenID sisselogimise protsessi käigus ID-kaarti. Sellisel viisil realiseeriti väga lihtsal viisil ID-kaardi põhist autentimist üle OpenID.

Kuna OpenID sisselogimist saab teostada suhteliselt lihtsal ja mugaval viisil, siis tõenäoliselt hakatakse seda realiseerima ka teistes olemasolevates ja loodavates rakendustes.

Kokkuvõte

Magistritöö eesmärgiks oli kaardistada OpenID põhise autentimise eelised ja puudused võrreldes alternatiividega ja töötada välja toimiv rakendus Meenutusteportaali jaoks. Eesmärk oli tingitud sellega, et tänapäeval tekib aina suurem vajadus Ühekordset sisselogimist võimaldavate lahenduste juurutamiseks. Sellel põhimõttel baseeruvate tehnoloogiate abil saab kasutajate igapäevaelu lihtsustada, neil ei ole enam vaja mäletada palju erinevaid kasutajatunnuseid ja salasõnu erinevate veebirakenduste kasutamiseks. Taolise lähenemise puhul on tihtipeale ka süsteemi administraatoritel lihtsam teostada kasutajate haldust tsentraliseeritud lahenduse abiga.

OpenID on massiliseks kasutamiseks mõeldud tehnoloogia, mida on suhteliselt lihtne teostada juba olemasoleva rakenduse juures. Suurem osa alternatiividest on mõeldud kasutamiseks suhteliselt kinniste äriettevõtete ning nende partnerite süsteemide puhul. Taolised tehnoloogiad baseeruvad rakenduste või süsteemide vahelise usalduse loomisel, selle saavutamiseks on partneritel vaja eelnevalt oma süsteeme siduda. Mõningad võimalikud alternatiivsed tehnoloogiad on praegusel hetkel veel alles arenguetapis, neid ei ole veel laialt kasutusele võetud. OpenID ei pruugi pakkuda kõiki keerukamate alternatiivide juures olevaid lisavõimalusi, samas pakub see standardset ning iga rakenduse juures vabalt kasutusele võetavat autentimisviisi. OpenID on võimeline kasutama turvalisuse tagamiseks umbes samu mehhanisme, nagu ka teised süsteemid. OpenID on täiesti vaba ja avatud kogukonna poolt arendatav tehnoloogia, mis on tema suureks eeliseks paljude konkurentide ees. Igaüks saab lihtsal viisil luua mitte ainult OpenID identiteete tarbivat teenust, vaid ka identiteete pakkuvat teenust.

Meenutusteportaali jaoks sobiva lahenduse väljatöötamiseks uuriti Plone sisuhaldussüsteemi jaoks juba teostatud OpenID abil autentimist võimaldava laienduse tööpõhimõtteid. Tuli välja, et olemasolev lahendus ei vasta Meenutusteportaali kriteeriumitele ja ei sobi taolise ülesehitusega rakenduse jaoks. Uue lahenduse realiseerimise käigus lubati portaali OpenID abil sisselogimisel kasutada ainult OpenID.ee teenust, mis on usaldusväärne ning võimaldab ära kasutada Eestis laialt levinud ID-kaardi võimalusi. Meenutusteportaali OpenID laienduse näol on tegemist kontekstisse sobiva spetsiifilise realiseerimisviisiga, mille võimalusi saaks veelgi rohkem laiendada. Kasutades realiseeritud lahenduse põhimõtteid saaks luua üldisemat ning kõigi portaali kontekstiga sobivat lahendust, mis pakuks administraatoritele mugavaid haldamisviise.

Kasutatud kirjandus

Arkills, B. (2003). How LDAP Works. Viimati loetud internetis 03.05.2008. Aadress http://www.pearsonhighered.com/samplechapter/020178792X.pdf

Aspeli, M. (2007). Professional Plone Development. Packt Publishing.

Cantor, S., Carmody, S.,Erdos, M., Hazelton, K., Hoehn, W., Morgan, B., Scavo, T., Wasley, D. (2005). Shibboleth Architecture. Viimati loetud internetis 03.05.2008. Aadress http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-200509.pdf

Geyer, C. (2007). About SAML. Viimati loetud internetis 03.05.2008. Aadress http://saml.xml.org/about-saml

Geyer, C. (2007). History of SAML. Viimati loetud internetis 03.05.2008. Aadress http://saml.xml.org/history

Geyer, C. (2007). XACML OASIS Standard. Viimati loetud internetis 03.05.2008. Aadress http://saml.xml.org/xacml-oasis-standard

Google. (2007). SAML Single Sign-On (SSO) Service for Google Apps. Viimati loetud internetis 03.05.2008. Aadress http://code.google.com/apis/apps/sso/saml_reference_implementation.html

Ideelabor. Mis on OpenID.ee? Viimati loetud internetis 03.05.2008. Aadress http://openid.ee

Keskel, U. (2008). Mobile ID – Your New Key to Online Services. Viimati loetud internetis 03.05.2008. Aadress http://www.ebaltics.com/01005557?PHPSESSID=a81d374c2f6f8c0f1cf103f7b587ebbf

Lockhart, H., Campbell, B., Ragouzis, N., Hughes, J., Philpott, R., Maler, E., Madsen, P., Scavo, T.. (2008). Security Assertio Markup Language (SAML) V2.0 Technical Overview. Viimati loetud internetis 03.05.2008. Aadress http://www.oasis-open.org/apps/group_public/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

Madsen, P. (2005). SAML 2: The Building Blocks of Federated Identity. Viimati loetud internetis 03.05.2008. Aadress http://www.xml.com/lpt/a/1525

Martens, T. (2002). The Story of the Estonian ID Card. Viimati loetud internetis 03.05.2008. Aadress http://www.ebaltics.com/00605142?PHPSESSID=a81d374c2f6f8c0f1cf103f7b587ebbf

Microsoft Corporation. (2003). Active Directory Collection. Viimati loetud internetis 03.05.2008. Aadress http://technet2.microsoft.com/windowsserver/en/library/6f8a7c80-45fc-4916-80d9-16e6d46241f91033.mspx?mfr=true

Microsoft Corporation. What is Windows CardSpace? Viimati loetud internetis 03.05.2008. Aadress http://netfx3.com/content/WindowsCardspaceHome.aspx

OpenID.net. What is OpeID? Who Owns or Controls OpenID? Viimati loetud internetis 03.05.2008. Aadress http://openid.net/what/

OpenID.net. OpenID Foundation. Loetud Viimati loetud internetis 03.05.2008. Aadress http://openid.net/foundation/

OpenID.net. Read the Specifications. Viimati loetud internetis 03.05.2008. Aadress http://openid.net/developers/specs/

OpenID.net. OpenID Foundation awards first code bounties. Viimati loetud internetis 03.05.2008. Aadress http://openid.net/foundation/bounty/award1/

OpenLDAP Project. Introduction to OpenLDAP Directory Services. Viimati loetud internetis 03.05.2008. Aadress http://www.openldap.org/doc/admin23/intro.html

Paljak, M. (2008). Ideelabori OpenID serveri (openid.ee) kasutusjuhend arendajale. Viimati loetud internetis 03.05.2008 http://ideelabor.ee/opensource/wiki/OpenID

Pelletier M. and Shariff M. (2005). Plone Live. SourceBeat, LLC.

Rehman, R. (2008). Get Ready for OpenID. Conformix Technologies Inc.

Sertifitseerimiskeskus, id.ee. (2008). ID-kaart - uue aja isikutunnistus. Viimati loetud internetis 03.05.2008. Aadress http://www.id.ee/10358

Sertifitseerimiskeskus. ID-kaart. Viimati loetud internetis 03.05.2008. Aadress http://www.sk.ee/pages.php/02020401

Sertifitseerimiskeskus. Sertifikaatide uuendamine. Viimati loetud internetis 03.05.2008. Aadress http://www.sk.ee/pages.php/0202040102,674

Sertifitseerimiskeskus. (2004). Sertifikaadid Eesti Vabariigi isikutunnistusel. Viimati loetud internetis 03.05.2008. Aadress http://www.sk.ee/file.php?id=364

Shibboleth Project. About. Viimati loetud internetis 03.05.2008. Aadress http://shibboleth.internet2.edu/about.html

Shibboleth Project. Shibboleth technical introduction. Viimati loetud internetis 14.04.2008. Aadress http://shibboleth.internet2.edu/tech-intro.html

Stepka, J. (2007). Using OpenID. Viimati loetud internetis 03.05.2008. Aadress http://www.theserverside.com/tt/articles/article.tss?l=OpenID

Tambaum, T. (2007). Memuaarikogumise portaal (projekt).

The Open Group. Introduction To Single Sing-On. Viimati loetud internetis 03.05.2008. Aadress http://www.opengroup.org/security/sso/sso_intro.htm

Vladimirskiy, A. (2007). OpenID support. Viimati loetud internetis 03.05.2008. Aadress http://plone.org/documentation/how-to/openid-support/

SUMMARY

Title: OpenID-based Authentication in Web Applications - the Case of Meenutused Portal
Keywords: Single Sign-On, OpenID.

The master thesis focuses on the issues of Single Sign-On authentication implementation for usage in multiple systems. Single Sign-On is nowadays implemented by many big players like Google to enable convenient the usage of their services and services by their partners. Even now there are many technologies that define standards and protocols for building Single Sign-On implementations. Some of these are harder and some easier to implement. Many of these are meant to be used as enterprise solutions by large companies. Some are meant to be used globally, in context of almost every system. One of these technologies is OpenID. OpenID is meant to eliminate the need for multiple usernames across different websites, simplifying the online experience for users.

The main goal of the thesis was to study OpenID technology and to evaluate its benefits and shortcomings compared to the competitors. Using the knowledge gained during that analysis, author then implemented an OpenID authentication module for the Memories Portal (Meenutusteportaal), a memories-sharing portal for elderly people based on Plone content management system. The Memories Portal‘s specific OpenID implementation is largely based on the existing OpenID extension for Plone, but the author of this thesis has made an adaptation of this extension that connects the OpenID identifier with the portal member account. The solution will allow the usage of OpenID.ee as the only trusted Identity Provider. Benefit of limiting OpenID providers to this one allows (and actually, forces) the users to authenticate themselves with Estonian ID card.

The length of the thesis is 65 pages, with 14 figures and 1 table included in the text. The list of references contains 32 items of literature and Web resources. The thesis is written in Estonian.